Harnessing QD-PUFs for Secure Authentication via Fuzzy Fingerprint Generation

Kieran D. Longmate

This thesis is submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

Department of Physics
Lancaster University
26th of September 2022

Preface

This thesis is the result of work which I performed at Lancaster University, between October 2018 and September 2022. Except where otherwise stated the contents of this thesis are the results of my own work, and is not the same as any others I have already submitted, or in the process of submitting, for any degree at any university or institution. The word count on this thesis does not exceed the maximum limit of 80,000 words.

Kieran D. Longmate

Acknowledgements

This is dedicated to my companion on this journey, my guiding light and the one without whom none of this would have been possible.
Lulu Healey

"But then science is nothing but a series of questions that lead to more questions, which is just as well, or it wouldn't be much of a career path, would it?" - Sir Terry Pratchett

List of Publications

Kieran Longmate, Elliott Ball, Edward Dable-Heath, and Robert Young. "Signing information in the quantum era". *AVS Quantum Sci* 2(4), 2020.

Kieran D Longmate, Nema M Abdelazim, Elliott M Ball, Joonas Majaniemi, and Robert J Young. "Improving the longevity of optically-read quantum dot physical unclonable functions". *Sci Rep*, 11(10999), 2021.

Matthew Fong, Chris Woodhead, Nema Abdelazim, Daniel Abreu, Angelo Lamantia, Elliott Ball, Kieran Longmate, David Howarth, Benjamin Robinson, Robert Young and Phillip Speed. "Using intrinsic properties of quantum dots to increase security when uniquely identifying devices". *Sci Rep*, 12(1) 2022.

Elliott M. Ball, Kieran Longmate, Joonas Majaniemi, Angelo Lamantia, Daniel Abreu, Matthew J. Fong, and Robert J. Young. "Smartphone-based fingerprint extraction from quantum-optical pufs". *Awaiting Publication*, 2022.

Abstract

The field of security technology is an eternal race. For every step forwards that is made in producing technology to help secure something it is not long behind it that those who seek to attack it make one also. Cryptography is one key example, even as encryption algorithms get more advanced so too do the computers that can be used to brute force them. Anti-counterfeiting is another. For each new complex watermark or hologram to prove authenticity there shortly follows better production techniques that aid in replicating them.

There is a solution to this within the concept of Quantum Dot Physically Unclonable Functions (QD-PUFs). Underpinned by the laws of quantum physics rather than mathematically hard problems they are, as their name suggests, impossible to replicate. Providing an extremely appealing solution to security concerns where authentication and identification are required.

There are several matters however that prevent QD-PUFs from being used in a much more wide spread manner. The aim of this thesis is therefore to address these in order to move QD-PUFs closer to being widely available. The foremost of these issues is a way to digitise the output of QD-PUFs. This forms the bulk of this thesis in detailing, analysing and discussing the fingerprinting algorithms designed to perform this task. As well as this the stability of the QD-PUFs, how to hide the information within fingerprints and the influence of varying incident wavelengths are covered. All to provide a comprehensive discussion on QD-PUFs and their fingerprints.

Contents

Chapter 1

Introduction

Although many may not realise it, uniqueness plays a key role in underpinning many aspects of security in our modern world. One of its primary uses is in verifying authenticity. Luxury goods may have a holographic tag to show they are the genuine article. Official documents such as passports bear complex watermarks and are made of a secret selection of materials. Digital authentication requires a digital signature unique to the sender and kept secret from an attacker for fear of imposter attacks.

The weakness with these and the myriad of other wide ranging examples however is the same in each case. They rely on it being difficult to replicate whatever unique feature is used for authentication. Difficult but not impossible. With improvements and the greater accessibility to technology a grave threat is posed to the assumption that such authentication tokens rely on[1][2]. Improvements and down scaling in manufacturing technology mean that holographic tags can be created far easier[3]. More advanced chemical analysis can better identify the materials used in passports. The advent of more powerful computers (not to mention the threat posed by quantum computing) drastically reduces the time to crack the difficult maths problems that keep digital signatures secure[4]. This leads to a metaphorical arms race. Those that wish to protect their security developing techniques that are more and more difficult to replicate or crack. On the other side of the coin are those that wish to attack such security, creating ever more advanced methods to do so.

With this in mind it is therefore obvious as to why Physically Unclonable Functions or PUFs would be such an area of interest for research. The innate physical properties of these are impossible, not just difficult, to replicate[1][5]. Thus, it would appear, providing a light at the end of the tunnel for the authentication arms race. Such a useful item could be embedded into a luxury good or passport, its unique output them registered with whoever produced the object. Any that allow for a digital output would mean that one could carry a digital signature in physical form. There are however two major problems with most PUFs that prevent more widespread use. The first is the authenticating of them, many still require specialised equipment[5]. The second is simulation attacks. An attacker may record the possible outputs of a PUF and then use it to mimic the PUF and fool authentication protocols[2]. Thus, most PUFs require a secondary verification to ensure no simulation occurs.

Both of these issues can be solved with a novel variation of PUFs known as Quantum Dot Physically Unclonable Functions or QD-PUFs[5]. Using the quantum mechanical

properties of quantum dots, these PUFs produce an unclonable output that a user can verify by themselves is not a simulation. They also can be challenged using nothing more than a camera and bright light in the visible spectrum[6][7]. Something that most members of the public posses at all times in modern phones. Thus, removing the need for specialised equipment. Such a concept has a wide range of applications in solving the issues of authentication already discussed.

On their own however, QD-PUFs are not of much use. As their output is a complex optical pattern, in order to harness them we require some method of digitisation so they can be quantitatively analysed[5]. The harnessing of QD-PUFs is therefore what we will focus on here. One cannot simply just compare two photographs of a QD-PUF to give secure authentication. Image noise, varying ambient lighting conditions and too great a bit depth prevent this. Instead one must generate a noise resistant binary fingerprint from the QD-PUF. This allows for the harnessing of QD-PUFs in authentication. The development and the understanding of such fingerprints are discussed in the following pages.

To open with, chapter 2 covers the necessary theoretical background that will form the bedrock of the discussion in later chapters. It covers what a PUF is in greater deal and what the properties of quantum dots that we use in QD-PUFs are. Although further proof of this is beyond the scope of the discussion here this chapter also discusses the simulation attack prevention inherent to QD-PUFs that sets them apart from other PUFs.

After the theoretical groundwork has been laid, chapter 3 covers the common methods used throughout the experiments in the following chapters. This includes an overview of how QD-PUFs are created and the process by which they are challenged in the laboratory. We then discuss the fingerprinting algorithms themselves, detailing how they encode the brightness texture of the QD-PUFs, how we quantitatively analyse the fingerprints as well as the authentication process for them. Any methods that are unique to the experiments in a chapter are detailed in the chapter they are relevant to.

Chapter 4 forms the first of the experimental chapters and lays the groundwork for those following it. The purpose of this chapter is to develop understanding of the behaviour of the fingerprinting algorithms. Three of which are novel in design and provide noise resistant alternatives to techniques such as Gabor filters for encoding texture information as a binary output. Each will be tested first in comparison to each other over three different QD-PUFs. Then the focus moves to how well the algorithms can handle damage to the input image, a key issue when QD-PUFs are moved to use outside of the laboratory.

As discussed there is a constant arms race to try and break security measures. Chapter 5 discusses the security of the fingerprints themselves from the viewpoint of an attacker using them as a point of attack in the QD-PUF authentication process. It details potential weaknesses and how they can be overcome. Completing the image of the strengths and weaknesses of the fingerprints generated from QD-PUFs. To further expand upon this a unique approach to obscuring structural information and debiasing 2D binary matrices is also proposed and its performance analysed.

QD-PUFs will be in use for prolonged periods in practical settings. They do experience degradation over time. This is a factor that must be considered when discussing

how best to harness them for use. As such chapter 6 covers this issue. Detailing the effects of QD-PUF degradation on their brightness and their fingerprints, alongside how this can be counteracted. Thus, progressing insight into the link between the polymer matrices that quantum dots are suspended within and their rate of degradation.

Finally we have chapter 7. The aim of this chapter is to expand upon the work covered in the rest of the chapters. Each of the preceding chapters test QD-PUFs under one incident wavelength of light. Here we look at their behaviour when the wavelength of the incident light is varied. This covers the effect it has on the quantum dot pattern and the possibility of creating multiple fingerprints from a single QD-PUF. As well as this it details a novel method of analysing the photoluminesence excitation spectrum of quantum dots that are deposited onto a substrate.

Chapter 2

Theoretical Background

The useful feature of Quantum Dot Physically Unclonable Functions (QD-PUFs) is their unique optical pattern when excited with incident light. This is formed by colloidal quantum dots (CQDs) that have been deposited onto a substrate whilst suspended in a solvent or a lacquer. An example of a QD-PUF with its central quantum dot pattern can be seen in figure 2.1. Whilst the creation of QD-PUFs will be detailed in chapter 3 this section will instead cover the theoretical background that underpins their usefulness. Much of this will be referenced back to in later chapters. We begin with the theoretical background of quantum dots with section 2.1.2 by covering what exactly a quantum dot is and why they form unique optical patterns. Then will be covered the non-linearity of their emission and how this can be harnessed as an important additional layer of security. Following on from this, is the effects of oxidation on the emission intensity of quantum dots in section 2.1.3, such that we can better understand the hurdles to the long term use of QD-PUFs. Finally for quantum dots the variation they display in emission when the excitation light is varied in wavelength. Commonly known as Photoluminesence Excitation (PLE) spectra this is detailed in section 2.1.4 and is useful in discussion of generating multiple fingerprints from one QD-PUF.

After this a theoretical introduction to Physically Unclonable Functions (PUFs) will be given in section 2.2. This will be begin by giving an overview of what PUFs are in section 2.2.1, alongside examples of them and applications of PUFs. Then the discussion will become more focussed with section 2.2.2 covering Optical Physically Unclonable Functions (OPUFs). Finally in this chapter, with the required groundwork laid, section 2.2.3 covers Quantum Dot Physically Unclonable Functions (QD-PUFs) themselves, setting the focus for the rest of thesis discussion on PUFs.

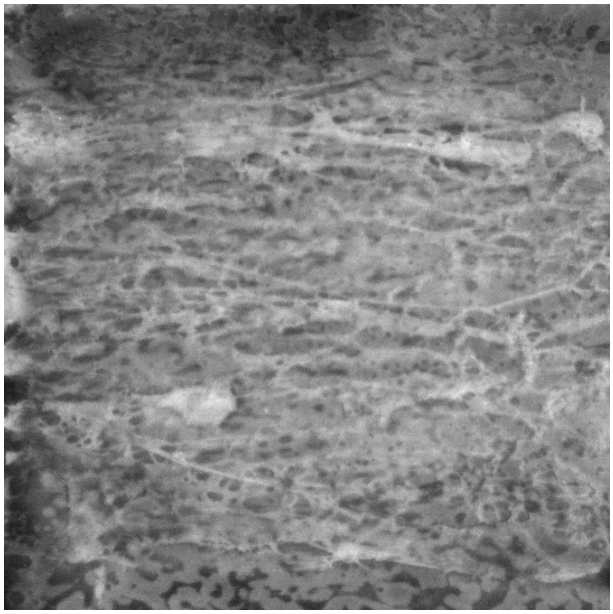

Figure 2.1: Image of a QD-PUF taken with the apparatus shown in figure 3.1. The term "quantum dot pattern" refers to the spatial variation in brightness over the deposition area. The quantum dot pattern seen in the center has been excited with blue light in order to make its emission as clear as possible.

2.1 Quantum Dots

2.1.1 Introduction to Quantum Dots

The quantum dots that are used in the QD-PUFs that are the focus of the research here are all comprised of semiconductor material. Bulk semiconductor material possesses electrical properties between that of a conductor and an insulator. Unlike conductors its band structure is split into two continuous bands, the valence band and the conduction band. For a current to flow an electron must be excited across the band gap from the valence band to the conduction band. As represented in figure 2.2a this leads to a continuous spectrum of energy levels.

Interesting changes begin to occur when we constrain the electron's degrees of freedom. For example allowing only a single degree of freedom results in a nanowire, a long thin structure with a width of the order of a nanometer. Rather than the behaviour of a standard wire, they instead show electric conductance that is constrained to discrete values[8]. When we apply constraints in all three dimensions we get a quantum dot. Nanometer in scale they can be represented by an infinite potential well in three dimensions. This results in the valence and conductance bands being split into discrete energy levels unlike the continuum seen in bulk material[9]. This drastically changes the density of states distribution as represented in figure 2.2bii. Resulting in peaks in the density of states at the energies of the discrete levels. A fact that earned quantum dots the moniker of "artificial atoms".

In bulk semiconductor material the absorption of a photon of sufficient energy causes

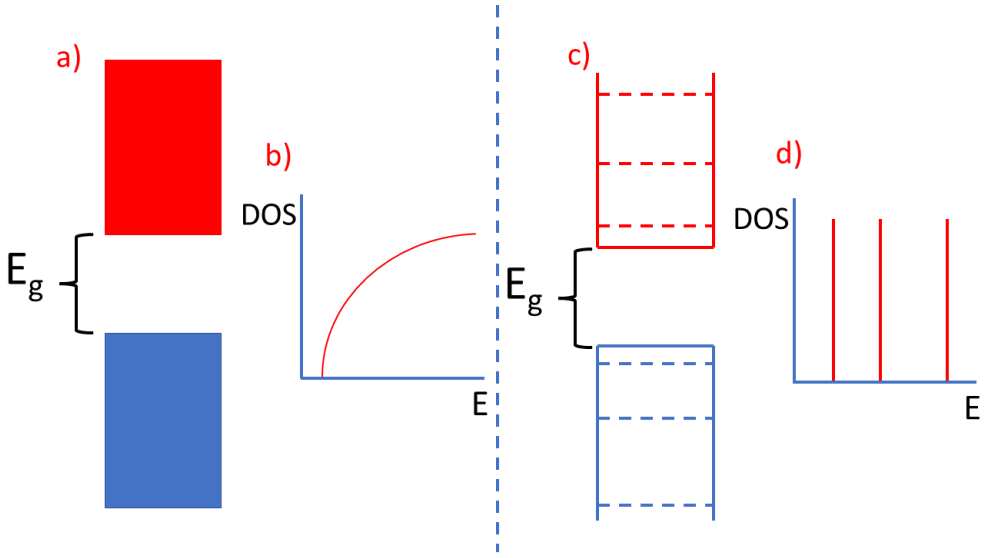

Figure 2.2: a) Diagrammatic representation of the continuous energy spectrum in bulk semiconductor material. b) Example graph of the variation of density of states (along the y-axis) against increasing energy (along the x-axis) in the conductance band of bulk semiconductor material. c) Diagrammatic representation of the discrete energy levels in quantum dots. d) Example graph of the variation of density of states (along the y-axis) against increasing energy (along the x-axis) in the conductance band of quantum dots. For both a) and c) the blue region represents the valence band and the red region the conduction band. E_g represents the bandgap energy of the material.

an electron to be excited into the conduction band. Leaving an 'electron hole' in the valence band. This bound electron-hole pair (or exciton) will emit its energy as a photon when it recombines, said energy is dependant on the band gap of the semiconductor. As quantum dots are zero dimensional semiconductor nanostructures and have their valence and conduction bands split into quantized energy levels[10] they display a narrow emission spectrum that can be tuned by altering the size of the dots. This size dependence is characterised by the Brus equation[11]:

$$E(r) = E_g + \frac{h^2}{8r^2}\left(\frac{1}{m_e^*} + \frac{1}{m_h^*}\right) \tag{2.1}$$

where $E(r)$ is the emission energy of the quantum dot at a given dot radius r. m_e^* and m_h^* are the effective mass of electrons and holes within the dot respectively. In this matter Planck's constant is given by h. As can be seen this grants a high degree of control over emission wavelength when creating quantum dots, with larger dots emitting in longer wavelengths. Such a high degree of control as well as the fact that regardless of the wavelength of incident light, the emission of the dots will remain within the same wavelength range makes them highly useful for optical authentication purposes, such as for QD-PUFS.

2.1.2 Quantum Dot Patterns and Non-linear Emission

The quantum dots used in this paper for the creation of the quantum dot physically unclonable functions (QD-PUFs) are known as colloidal quantum dots (CQDs). These consist of the semi-conductor quantum dot core surrounded by a complex ligand structure. This allows for the CQDs to be prepared in solution. CQDs have been likened to 'artificial molecules' as the ligands can bond together to form larger clusters or 'ensembles' of CQDs[12]. These ligands alter the electronic states within the quantum dot core, affecting the band-gap and quantum yield of the dots[13]. Bonding further ligands to a CQD further affects the possible exciton states. Thus, an ensemble of dots will have different emission properties to that of an individual CQD. There is no way to exactly control which or how many CQDs will bond to form an ensemble. Thus, applying a solution of CQDs to a surface will not only result in a randomised pattern of these 'clusters' but each cluster will have randomised emission properties. Resulting in the creation of a unique pattern (this is referred to as a "quantum dot pattern" throughout this thesis and an example of which is given in 2.1), the basis of QD-PUFs[2][5].

There are further properties of quantum dots that make them particularly useful for authentication purposes. In particular that they display non-linear emission response to linearly increasing incident light intensity[10]. At low incident light intensities the emission of a quantum dot is dominated by its excitons, whose production shows a linear dependence on incident light[14][15][16]. As the intensity of light increases however the exciton ground state of the quantum dot becomes fully occupied (also known as saturation)[15][17]. Any exciton that recombines is immediately replaced by a another thus preventing the intensity of emitted light from increasing further despite increasing incident intensity[14]. This causes the PL emission of the quantum dot to flatten out with respect to the incident light intensity. This is quantified by the equation for the photon production rate of excitons in quantum dots[18]:

$$R_{ex} = \frac{R_{sat}}{1 + \frac{I_{sat}}{I_{ex}}} \tag{2.2}$$

Where R_{ex} is the optical response rate at excitation and R_{sat} the rate at exciton saturation. I_{ex} and I_{sat} give the incident intensities at excitation and saturation respectively. This becomes useful as a second layer of security for QD-PUFs.

This non-linear optical photoluminesence is a well documented feature of semi-conductor quantum dots. It can be used, for example, to determine the charge carrier density in a quantum dot[14]. Alternatively, in the case of a QD-PUF it can be used to differentiate between a legitimate QD-PUF and a simulation of one[2]. The simplest example of a simulation attack would be an attacker using a high resolution photograph of a QD-PUF to attempt to fool the authentication process. For other optical PUFs that analyse images of said PUF for authentication this would be a successful attack. To the authentication algorithm there would be no difference between this simulation and the actual PUF.

The non-linearity in the PL of quantum dots is used as a secondary security check to prevent this "simulation attack"[2]. By measuring the emission of a QD-PUF with linearly increasing incident light intensity we can determine if this non-linearity is present. Any simulated QD-PUF will show a linear response to the incident light (as this will

just be the light being reflected back) and so can be detected. Such a process has been demonstrated to work both in laboratory conditions and using a more widely accessible device such as a smartphone[2][6].

Thus, highlighting why quantum dots are the material of choice when creating a new breed of optical PUFs. The unique pattern coupled with the ability to detect forgeries allows for a highly secure identification system. It is therefore imperative that an equally secure method of extracting a fingerprint from a quantum dot pattern be developed in order to exploit these features. Such a matter is addressed in the following chapters.

2.1.3 Photo-oxidation of Quantum Dots

As the most useful feature of quantum dots in the context of generating fingerprints from QD-PUFs for authentication is their optical emission pattern it is important to understand the effect that time may have on it. To create QD-PUFs colloidal quantum dots are suspended in a lacquer or solvent and then deposited onto a substrate (for further details see section 3.1). Once these quantum dots are deposited onto a substrate however the subsequent contact with oxygen causes them to begin to degrade[19]. When an excited quantum dot is exposed to oxygen, the oxygen will bond with the quantum dot core to produce ions that dissociate from the quantum dot itself (also known as surface oxidization). This process is known as photooxidation[20]. Prolonged oxygen exposure causes a reduction in size of the quantum dot core as it leads to the production of oxygen containing ions that dissociate from the core itself. The surface trap states this produces result in a permanent decrease in the photoluminescence output of the quantum dots. Prolonged degradation would therefore render a QD-PUF useless as no response would be detectable. This is a serious issue in a practical setting. InP quantum dots, such as those used in throughout the following chapters, are particularly sensitive to the effects of oxygen[21]. Although there are different quantum dot growth methods that can reduce this, the approach to degradation prevention taken here focuses on embedding the CQDs in a polymer matrix.

The principle behind this concept is that by embedding the CQDs in a polymer their exposure to oxygen is reduced[22]. The effectiveness of this approach is dependant on the oxygen diffusion rate of the polymer as well as their compatibility with the quantum dots used. Each polymer must also be optically transparent and still allow for the application of the CQDs to a substrate in order to create a QD-PUF. Such principles are taken into consideration in the creation of the QD-PUFs. The analysis of QD-PUF degradation, its effects on fingerprinting and how to reduce it is explored in chapter 6.

2.1.4 Quantum Dots Behaviour Under Varying Incident Wavelengths

Photoluminescence excitation spectroscopy is a technique commonly used to probe the electronic structure of materials. The emission of a sample is measured at the peak emission wavelength for that sample whilst the wavelength of the incident light is varied. The response of the sample will vary based on its electronic structure, giving insight into matters such as absorption peaks and the material's bandgap[23].

Two examples of absorption spectra can be seen in figure 2.3. These display the responses of Copper Indium Sulphide (CIS)[24] and Indium Phosphide/Zinc Selenium (InP/ZnS) quantum dots suspended in solution at low concentrations. In regards to quantum dots the only key difference between these and a PLE spectra is the method of measurement, both show the absorption structure of a quantum dot. When determining the electronic structure of a material that exhibits photoluminescence within a small bandgap commonly PLE techniques will be used to measure absorption spectra when a greater degree of sensitivity is required[25]. As such the location in terms of wavelength of features in both the PLE and absorption spectra will be the same[26]. This means that over the same range of measured wavelengths a PLE spectra will be identical to an absorption spectra[26].

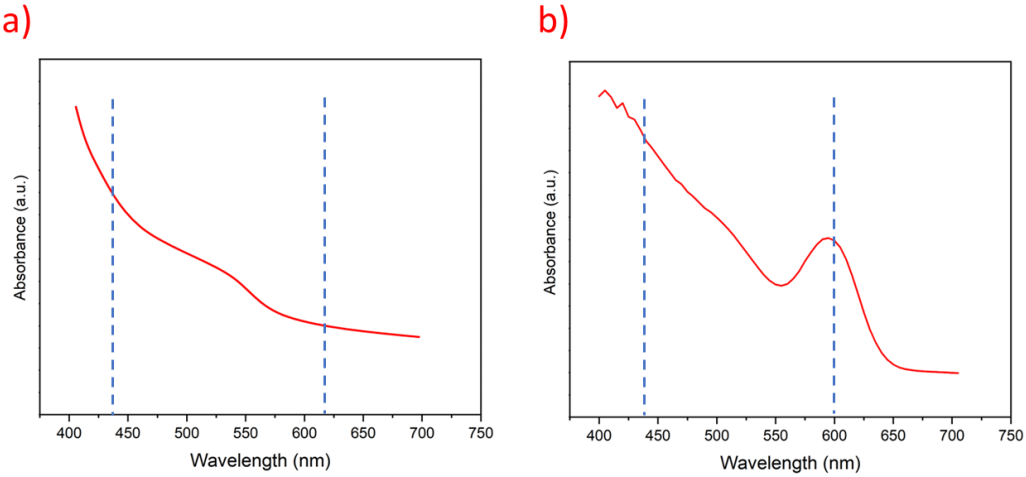

Figure 2.3: a) Absorption spectra of CIS quantum dots suspended in solution at low concentration. The blue dashed lines indicate the wavelength range analysed, in this case 440 nm to 620 nm. Graph produced by author using data made publicly available[24]. b) Absorption spectra of InP/ZnS quantum dots suspended in solution at low concentration. The blue dashed lines indicate the wavelength range analysed, in this case 440 nm to 600 nm. Graph produced by author using data taken by Angelo Lamantia (of Lancaster University at time of writing).

As can be seen in figure 2.3 the composition of the quantum dot greatly affects the absorption spectra and so PLE response. They display distinctly different PLE responses and have clearly different formations of CQD ensembles on their surface, allowing for a range of analysis.

PLE has been used to analyse the effects of quantum dot size[27] and coupling between quantum dots[28] on electronic structure. It has not been used however, to analyse the effect of CQDs forming ensembles on a substrate. As detailed in section 2.1.2 the interaction of ligands with quantum dots alters their electronic structure, an effect amplified within CQD ensembles. Therefore, it stands to reason as PLE is affected by electronic structure, that the formation of CQD ensembles will affect the PLE response. Thus, we can expect that this will lead to the PLE response to vary over the area of a quantum

dot pattern. If this is correct then it will allow for the generation of different fingerprints at each incident wavelength. This hypothesis is tested in chapter 7.

2.2 Physically Unclonable Functions (PUFs)

2.2.1 PUFs and their Applications

A Physically Unclonable Functions or PUF is an object or device that produces a completely unique output in response to a particular input[29]. Within cryptography the particular combination of specific output for a certain input is known as a challenge/response pair (CRP). An example of this would be password authentication. In this situation the request for a password is the challenge and the user giving the correct password the response. For QD-PUFs the challenge is the exciting of the QD-PUF with incident light and the response the production of the correct quantum dot pattern.

The key principle behind QD-PUFs is that it is not possible to replicate or reproduce any CRP[1]. No matter how many PUFs are produced no two of them will produce the same output despite receiving the same input. The origin of this uniqueness stems often from the process of their manufacture. This is due to the fact that in many cases aspects of manufacture are stochastic processes. Take for example the silk PUFs demonstrated by Kim et al[30]. These use the random arrangement of silk fibres in a piece of silk to produce a unique diffraction pattern. Replicating such a arrangement would require an infeasible amount of time and effort thus, ensuring the output is unique.

It is useful to note for the context under which PUFs are employed here that they can fall under two broad categories. These are known as weak or strong PUFs and are determined by the scalability of the number of CRPs with the size of the PUFs[31][32]. CRPs in weak PUFs scale with low order polynomials, meaning it is not uncommon for a weak PUF to only have a few challenge response pairs[29]. Strong PUFs on the other hand scale at much higher rates, meaning that the same sized strong PUF would have significantly more CRPs than a weak one[33][29]. An example of this is the QD-PUFs that will be the focus of the discussion here. They only posses one challenge response pair. An example of a strong PUF would be Arbiter PUFs[34] which use small random delay differences on parallel electric paths to generate multiple CRPs.

Analogously PUFs are akin to one way cryptographic functions[29][32]. Only in this case the function that maps the challenge input to a response out is a physical object. The prevention of replication is not ensured by sufficiently hard mathematical concept but instead by physical properties that cannot be reproduced. In this light then it is clear to see the uses that they may serve in a practical setting. A cryptographic function that can be embedded into items, be used as part of hardware security or even carried on ones person as a form of identification.

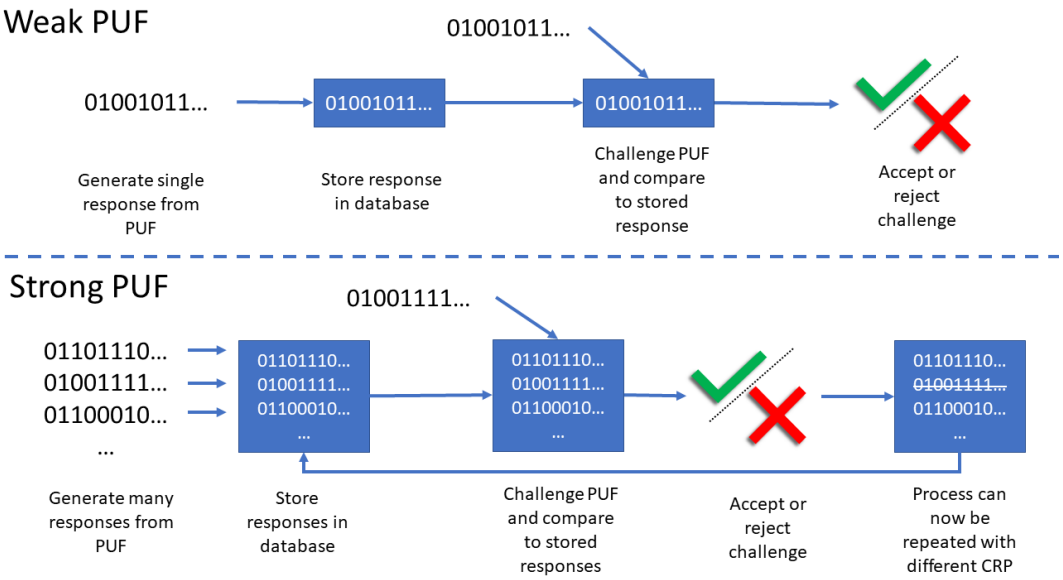

Figure 2.4: Top: Flowchart displaying an example process of the use of a weak PUF. Starting with a digital response being captured from the PUF, saved and then later compared to a challenge for authentication. Bottom: Flowchart displaying an example process of the use of a strong PUF. Starting with multiple digital responses being captured from the PUF, saved and then later one of them being compared to a challenge for authentication. In this "one time pad" approach the strong PUF can then be reused with a different CRP.

Weak PUFs are akin to a secret key[32]. As can be seen in figure 2.4 a weak PUF can be used to authenticate a user. At the manufacturing stage the PUFs unique response is recorded and stored in a database. At a later stage if a user wishes to authenticate they can challenge the weak PUF and compare the response to the expected response in the database. In this manner it allows the user to carry a secret key with them, provided they still physically have the PUF they can be confident that no one has learned their secret key. This does have drawbacks however. If an attacker can gain access to the weak PUF they will be able to measure all possible CRPs and then would be able to simulate it even without access to it. Thus, for authentication using a weak PUF to take place it must first be verified that it is indeed the PUF itself being used.

Strong PUFs alternatively are more akin to a hash function[32]. As in the same manner they take in similar challenges and producing distinctly different responses. Thus, strong PUFs have a multitude of different CRPs, to the degree that it would be infeasible for an attacker to measure all of them[31]. This allows for them to be used in different ways for authentication that does not require an extra step to verify that it is indeed the PUF itself in use. The first example of which is shown in figure 2.4, using the strong PUF as a one time pad protocol. Similar to the weak PUF CRPs are recorded at the manufacturing stage. A user would then authenticate using only one of them. Once used this CRP would then be removed from the list of valid authentication challenges. Thus, unlike the weak PUF it could then be reused. Alternatively at the manufacture stage a random sequence of CRPs would be recorded. Given the scale of the amount of possible CRPs in the strong PUF for a long enough sequence it would be almost impossible for an attacker to correctly simulate. Thus, removing the need for a verification step that the PUF is in use.

Weak PUFs are therefore of course often seen as less secure than their strong counterparts.

This is not to say however that one is "better" than the other. Instead which is more useful comes down to the situation in which they are applied in. Strong PUFs require more specialised equipment both to create and to authenticate. Meaning that they are better suited to situations where a high degree of security is absolutely necessary and the equipment is readily available. An example of this could be electronic identification in a high security building. Weak PUFs despite their lessened security are far easier to authenticate meaning they are better suited to wider public use. Making them useful in areas such as confirming the authenticity of products.

2.2.2 Optical Physically Unclonable Functions (OPUFs)

There are many different varieties of PUF that exist from electronic PUFs (EPUFs)[35] and Radio-Frequency PUFs (RFPUFs)[36] to Optical PUFs (OPUFs)[2]. It is the last of which that will be the focus of this section. OPUFs are characterised by their response being optical in nature. This could be a unique pattern produced when the OPUF is used as a transmission medium. This is shown in figure 2.5a, where light is shone through the OPUF to produce an optical pattern behind it. Examples of this include the silk PUF[30]. The other common variety of OPUF instead uses light that is "returned" from the OPUF. Whether this be through reflection such as in the paper PUF[37] or emission such as the QD-PUFs discussed here. This is represented in figure 2.5.

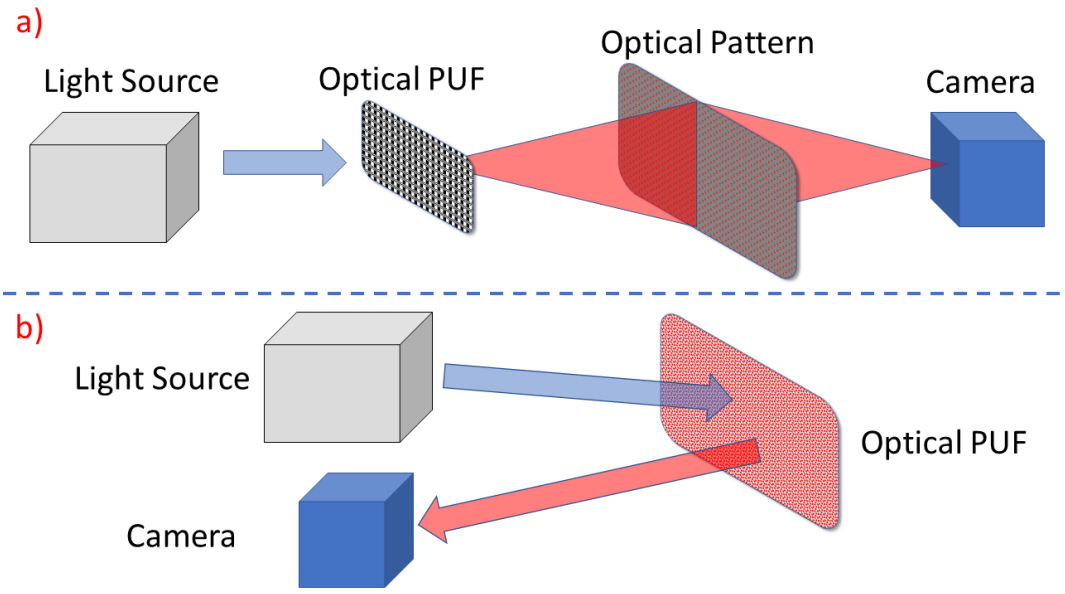

Figure 2.5: a) Pictorial representation of an OPUF that produces an optical pattern when light is shined through it. These tend to include OPUFs which have a random arrangement of holes such as the silk PUFs demonstrated by Kim et al[30]. b) Pictorial representation of an OPUF that produces an optical pattern when light is shined on it, either through reflection or emission. The QD-PUFs used in this thesis are an example of these.

The common feature of OPUFs is however that they are extrinsic PUFs. Namely that

they require an external piece of apparatus in order for them to be challenged and the response measured. Commonly this is some form of camera or CCD (or Charge Coupled Device, capacitor arrays used in the production of cameras and similar devices). This grants OPUFs some advantages such as the fact that they do not have to be embedded in a circuit like EPUFs do. In some cases they also can be used without specialist apparatus, making them viable options for wider public use[6][7]. OPUFs also have the advantage of being cheap to produce and also having a high degree of complexity in their outputs[32]. However, depending on the OPUF, they can be easily simulated by simply taking an image of the output.

To be useful an OPUF must have a pattern that possess a high degree of entropy whilst being clear to read. Optical measurements will always be subject to the issue of image noise. As such OPUF authentication is done using fuzzy authentication techniques[38]. Techniques such as fuzzy vaults[39] and the hamming distance comparison detailed in section 3.3.3 are both prime examples of this. As such nanoscale emitters are commonly used as the material for OPUFs. Their bright emission within a narrow bandwidth makes it much easier to filter out the OPUF pattern from the background. Nanowires[40], gold nanoparticles[41] and quantum dots have all been used as the material for OPUFs[5].

2.2.3 Quantum Dot Physically Unclonable Functions (QD-PUFs)

Finally we arrive at the topic of Quantum Dot Physically Unclonable Functions or QD-PUFs. Although they have been touched upon in earlier sections of this chapter here we will delve deeper into what they are. QD-PUFs fall under the category of optical PUFs or OPUFs[5]. As detailed in section 2.1.2 when CQDs are deposited onto a substrate they form a unique pattern of quantum dots. When excited with incident light this pattern will photoluminesce, such as shown in figure 2.1. As with other PUFs the manufacturing does contribute to the uniqueness of the quantum dot pattern. There is no way to predict or precisely control (a very limited degree of control is possible in the manner of the degree of clustering that occurs) how the CQDs will cluster together. Thus, this means that their arrangement upon the substrate will be completely randomised. A further degree of randomisation is introduced in that the bonding of the ligands affects the brightness of clusters. As such there is no clear way of predicting the brightness of a cluster as one cannot know how the ligands will bond within it. These both combine to two dimensional brightness topography that is the singular challenge response pair of QD-PUFs.

Although the singular CRP that QD-PUFs posses does make them a weak PUF, they do not posses the same drawback of being vulnerable to simulation attacks. As already discussed in section 2.1.2 we can use the non-linear response to incident light to validate whether the QD-PUF being challenged is a simulated fake or not. This gives QD-PUFs a novel edge over other PUF designs. Being optical in nature and requiring no specialised equipment to challenge them they can be authenticated with something as widely used as a smartphone camera and flash[2][6]. Thus, opening the door for secure cryptographic key storage that can be used for authentication by any member of the public. This could range from anti-counterfeiting on luxury items to identity verification. As such they show great potential is harnessed and developed.

Chapter 3

Methodology

In this chapter we discuss the common experimental methods used throughout subsequent chapters and details of the fingerprinting algorithms applied. First covered is the production method of the QD-PUFs used throughout this thesis, detailed in section 3.1. Following this is section 3.2, detailing the process and apparatus used to capture of images of the QD-PUFs. Finally there is section 3.3. This opens with a discussion of the requirements that a fingerprinting algorithm must meet as well as the figures of merit used to quantify this. Following this is the process of how QD-PUF authentication is performed. Finally how each of the four algorithms (RLBP.V1, RLBP.V2, RMLBP and AHB) produces a fingerprint from a QD-PUF image is discussed.

3.1 QD-PUF Creation

As the focus of most chapters here is on using the QD-PUFs and not their chemical composition the creation process will be detailed in a more general manner here. This is especially as there are several ways to produce QD-PUFs. With different combinations of their chemical compositions, the lacquers/polymers they are suspended in and their deposition methods producing different patterns on the substrate. The focus of the work in this thesis is on the optical patterns that are produced and not how to create them. As such the exact methods are not particularly of interest and so will not be detailed for each QD-PUF. Especially as a wide array of QD-PUFs are used in the following chapters. The exception to this is chapter 6, wherein the exact chemical composition is important and so is covered in much greater detail.

In each case the basic principles remain similar[5]. The CQDs are dissolved in a solvent (often toluene) with an encapsulating polymer if required. These are thoroughly mixed before being deposited onto a black polyethene substrate. The method of deposition can vary. Drop casting sees the CQD solution dripped onto the substrate from a pipette thus, forming much less uniform but far less neatly square patterns. Hand stamping as the name implies involves the CQD in solvent mixture being applied to a stamp before being stamped onto the substrate. The doctor blade is the process by which the majority of QD-PUFs in the following chapters were made. It is a device which deposits a thin film of a solution onto a substrate with a precisely controllable thickness.

3.2 QD-PUF Image Capture

In order to test the fingerprinting algorithms in as reliable a manner as possible images are needed of the excited quantum dot patterns with as little external influencing factors as possible. This allows for confidence that the conclusions drawn about the algorithms are not dependant on some unknown external factor. As such to ensure this a imaging system was designed to ensure that what was captured in each image is only the quantum dot pattern.

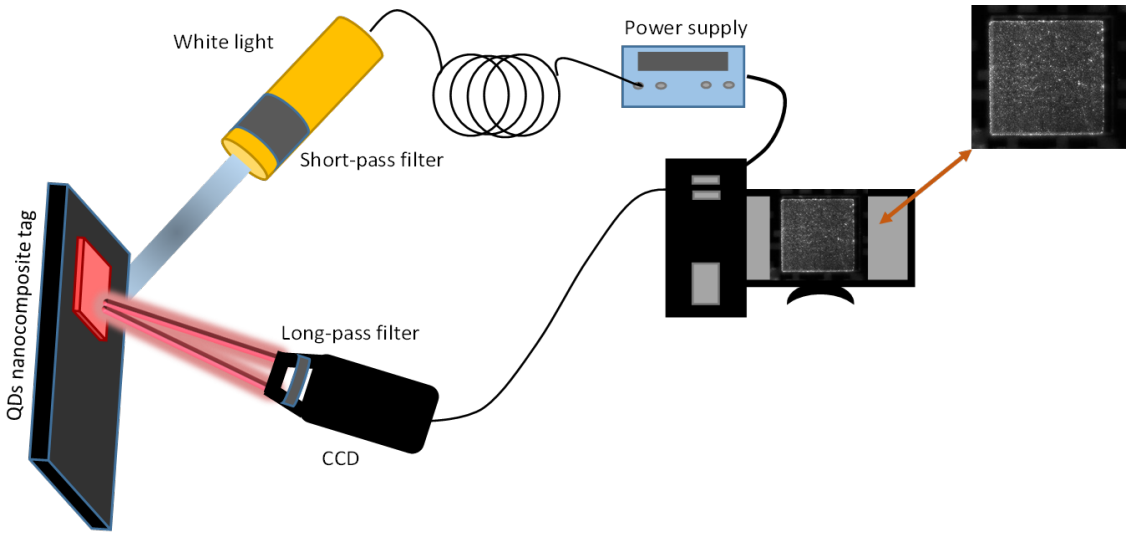

Figure 3.1: A schematic of the apparatus used to captures images of each QD pattern. The quantum dots in each token were excited using white light filtered through a 450 nm short-pass filter. A 500 nm long-pass filter placed in front of the CCD ensures only light from the emission of the QD pattern is measured. The entire apparatus is sealed within a closed black box when measurements are in progress.

Each quantum dot pattern was imaged in the apparatus displayed in figure 3.1. The tag each pattern is housed on is placed in a stand designed to ensure the patterns are all in the same location when imaged. Blue light with peak wavelength of 450 nm and an intensity of 0.31 mWcm^{-2} (at the distance the pattern is placed) is then used to excite the QD pattern. The emission of the QD pattern is then captured on the CCD, which is filtered to ensure only light from the QD emission is imaged. The exposure time for each pattern is chosen so as the image is as bright as possible with out any saturation occurring. Due to the fingerprinting techniques invariance to global brightness levels this in of itself will have no effect on the results. The only issues with exposure occur if it is too high (as the image saturates and information is lost) or if it is too low, which gives a poor signal to noise ratio. Finally this entire apparatus set is housed in a blackbox to ensure no light from external sources affects the results.

For cases when a higher magnification is required the same principle can be applied to a microscope. By choosing filters with no spectral overlap as with the apparatus in figure 3.1 we can capture images where the only emission is that from the quantum dot pattern. Owing to being able to use cameras with longer exposure times using a microscope allows for the use of bandpass filters instead of long and short pass filters (as seen in chapter 7). Although it was not possible to fit a blackbox around this apparatus the

external lights were all turned off remove any impact on the experiment.

3.3 Fingerprinting Algorithms

3.3.1 Algorithm Requirements

The primary goal of the fingerprinting algorithms is to condense an image of a quantum dot pattern into a repeatable format usable for authentication. This is done in the cases discussed in this thesis by encoding the local texture information of the image in order to generate a 2D binary matrix that can be used as a cryptographic key. The most immediate issue with this is the fact that no two images of the same quantum dot pattern will be exactly the same. This is because the value of each pixel consists of the emission signal from the quantum dot pattern as well as the value of the camera's inherent noise for that pixel. As this noise varies randomly it is what prevents two images of the same pattern form being exactly the same. On top of this for applications where the QD pattern is imaged outside of laboratory conditions environmental factors will affect the image taken of the QD pattern. These may include global scale shifts in brightness, brightness gradients due to non-uniform ambient lighting and enhanced camera noise depending on the apparatus used. Therefore, directly matching a "challenge" fingerprint is not appropriate and "fuzzy" authentication techniques must be applied. For a technique to be useful it must meet the following criteria:

- The algorithm must produce a form of key that can be used for authentication purposes. This key must be greater than or equal to 256 bits in length. This is to reflect industry standards in other more conventional algorithms used in authentication such as SHA-256[42]. This bit length also aids in ensuring that there are no collisions between fingerprints.
- Be able to produce repeat fingerprints of the same QD pattern that are similar enough to each other but different enough to fingerprints of other patterns so as to be identified as originating from the same pattern.
- Be resistant to noise such that two input images of the same QD pattern with different noise levels will still produce matching fingerprints.
- The algorithm must be invariant to global shifts in input image brightness.
- The performance of the algorithm must not be limited by the type of texture it is generating a fingerprint from. It must be applicable to all QD patterns of which vary greatly in their textures, depending on make. For example feature mapping techniques are not of use in this matter as for secure authentication they are dependant on the number of features they can detect in an image.

Whilst other computer vision techniques such as blob and feature detection/mapping algorithms can be used for authentication these were not suitable in this use case as they did not meet the all of the above criteria. When comparing techniques that do match the criteria other matters are considered. These include how accurately they can identify a fingerprint, to what degree are the techniques robust against outside damage to the input image or how repeatable the produced fingerprints are taken into consideration.

3.3.2 Figures of Merit

In order to test the performance of each of the fingerprinting algorithms four main figures of merit will be used. What these figures of merit specifically show for each test will be detailed alongside the results.

1. Intra hamming distance - if each fingerprint is treated as a bit string we can calculate the "distance" between two fingerprints. For such a case as this fractional hamming distances are often used, these represent the fraction of bits between two binary strings that are different. The fractional intra hamming distance is therefore the fraction of the bits between two fingerprints of the same QD pattern that are different. Mathematically fractional hamming distance (HD) for two 64x64 pixels (shortened to px in later uses) fingerprints is given by [43]:

$$HD = \frac{1}{4096} \sum_{i}^{64} \sum_{j}^{64} (A \oplus B)_{ij} \tag{3.1}$$

   Where A and B represent the binary matrices of the fingerprints and $\oplus$ is the XOR operator. For intra hamming distance A and B are generated from the same QD-PUF at different times. The closer to zero the intra hamming distance is the better the fingerprints match, this is the wanted outcome. In terms of fingerprints the mean intra hamming distance for repeat intra comparisons will give us a measure of how consistently the algorithm is generating fingerprints as close to the initial fingerprint as possible for repeat images of the same QD-PUF. The standard deviation provides a measure of how repeatable the algorithm is at performing this.

2. Inter hamming distance - the same as the intra hamming distance apart from the fact that this is between two fingerprints of different QD patterns. It is also calculated from equation 3.1 as with intra hamming distance. The only difference being that A and B represent fingerprints generated from different QD-PUFs. In this case the optimal value is as close to 0.5 as possible, as this is maximum separation for two binary strings. Inter hamming distance standard deviation provides a measure of how unique a fingerprint is when compared to fingerprints of other patterns.

3. False Positive Rate (FPR) - the FPR of a challenge fingerprint represents the possibility that this fingerprint is falsely matched to the chosen reference fingerprint. The lower the FPR is the more confident the person performing the authentication can be that the challenge fingerprint has authenticated correctly. It is calculated from the crossover between the intra and inter hamming distance distribution curves. Making it almost a measure of the confidence that a noisy fingerprint is more like repeats of itself that fingerprints of other patterns. Mathematically it is given by the equation [5]:

$$FPR = \int_{0}^{T} f(x)dx \tag{3.2}$$

   Where $f(x)$ is the function describing the normalised cumulative density function of the inter hamming distance distribution. T gives the maximal value of the intra

hamming distance distribution. Making it a measure of how likely a member of the inter distribution falls within the intra distribution. For authentication purposes a maximum FPR of 10^{-6} was chosen. This value was born both out of experience from preliminary testing and discussion based on use case scenarios. Providing a sufficient degree of security for many applications whilst allowing for it to be made stricter as required.

4. Effective Number of Independent Bits (ENIB)[43] - provides a measure of the number of bits in the fingerprint that do not feature in a pattern that is repeated in other fingerprints. It is calculated using the mean (μ) and standard deviation (σ) of the inter hamming distance distribution via:

$$ENIB = \frac{\mu(1-\mu)}{\sigma^2} \tag{3.3}$$

   It acts as a metric to describe how many bits in the fingerprint can actually be used in authentication. A minimum of 256 bits would be required.

For the sake of completeness the False Negative Rate (FNR) has not been used as a figure of merit owing to the fact that during testing the value of it fell below the precision MATLAB was able to process at (i.e. 10^{-308}) for all fingerprints. As such all values of it were treated as 0, rendering analysis of them redundant. The FNR is also more useful from an applications standpoint (e.g. how easy it would be for a user to scan a QD-PUF and it to register successfully) than for looking at the security of generated fingerprints.

Another important metric that is referred to throughout this thesis is the entropy of fingerprints. With the exception of the analysis performed in chapter 5 this is used as a qualitative term. The estimation of entropy in a 2D matrix is more complex than that of a simple 1D string [44], as Shannon entropy is used for. As one must consider not only the complexity of patterns along a plane but also their arrangement relative to each other on said plane. Whilst there are methods to create an estimation of such values (such as Voronoi diagrams [44]) such calculations as complex and would not provide a proportional degree of benefit to the discussion. Instead entropy is discussed in a qualitative manner based on visual inspection of fingerprints.

3.3.3 Fingerprint Authentication Process

Despite each algorithm creating the fingerprint in a different manner the overall structure of the fingerprinting process will always remain the same. The first step that must occur before any authentication can take place is the generation of the "reference" fingerprints. This involves the party, Alice, that distributes the QD patterns for use generating a database of fingerprints which can be kept private or public (for the latter it is recommended they are encrypted, potentially in a manner such as a fuzzy vault scheme[39] or via XOR debiasing as shown in chapter 5.2). The database must contain at least five repeat fingerprints of each QD pattern that has been distributed. This is to ensure that their are enough repeats for the intra hamming distance value to be reliable without causing too much of an increase in required computational time. Each of these fingerprints should be generated by taking repeat images of the same pattern (whilst it is excited by an external light source) and applying the fingerprinting algorithm to each separately.

When it comes to the authentication stage this will aid an accurate result by reducing the effects of noise. Once this is complete Alice may distribute her QD patterns and database, if it is public.

If a secondary party, Bob, has possession of a QD pattern and wishes to use it for authentication purposes the following process is followed:

1. The QD pattern is imaged by Bob's chosen apparatus. As with Alice he must ensure it is excited by an external light source. This is the "challenge" image.

2. Any pre-fingerprinting processing is then applied to the challenge image. In all cases this will include cropping the challenge image such that it only features the QD pattern.

3. The chosen fingerprinting algorithm is then applied to the challenge image to produce the challenge fingerprint. This will be in the form of a 2D binary matrix.

4. Post-fingerprinting processing will then be applied to the fingerprint. In all cases this includes resizing the fingerprint to be 64x64 pixels in size.

5. At this stage Bob will then authenticate the fingerprint, either by sending it to Alice to compare to the reference fingerprints (if the database is private) or by comparing them himself.

6. If the fingerprint is deemed a match by the chosen fuzzy authentication technique then the QD pattern in Bob's possession is authentic.

3.3.4 RLBP.V1

Local binary patterns (LBP) is a texture descriptor technique first proposed by Ojala et al[45]. It compares each pixel in an image to N of it's neighbours, each of which sit on the circumference of a circle of radius R (this value is always measured in terms of pixels). Moving in a clockwise direction starting from the pixel that lies on the positive y-axis of the central pixel (see the red circled point in figure 3.2) the value of each circumference pixel is compared to that of the central pixel. If it is greater or equal to the value of the central pixel it is assigned a value of 1. Otherwise it is assigned a value of 0. These values are then concatenated together to form a binary string known as a feature vector which is assigned to the central pixel, an example of which is shown in figure 3.2. This feature vector encodes local contrast information as well as positional information (by reading it off you can reconstruct the relative values of the pixels measure to the central pixel), allowing it to describe a set of features. Further discussion on this is however not necessary for the topic of this paper.

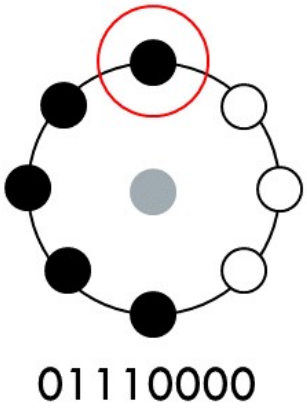

Figure 3.2: Pictorial representation of the "LBP circle" used by RLBP.V1. The grey circle represents the central pixel. The black and white circles represent the pixels being compared to the central pixel, each of which lies on the circumference of a circle with radius R centred on the central pixel. A black circumference pixel represents that it is lower in value than the central pixel, white represents that it is equal to or greater than the central pixel in value. Below the diagram is the feature vector string that LBP would have generated for this central pixel.

The appeal of using LBP as a base for a fingerprinting algorithm stems from a few reasons. First and foremost that it encodes feature information into a binary string. Thus allowing for the easy digitisation of QD patterns into a cryptographic key. As it is based on local contrast information it also has no limitations set upon it by the texture analysed. Secondly the fact that it is based on relative pixel values it is invariant to global shifts in illumination. Finally there is its reported performance in use as a reliable texture descriptor and feature matching algorithm.

The feature vector in of itself however cannot be used in a fingerprint. Preliminary testing found that, as would be expected, using the entirety of each feature vector for each pixel in authentication was too prone to the effects of noise to be accurate. Thus, as a simplistic first fingerprinting technique, only a comparison between the central pixel and the first pixel was used to generate the binary value of the central pixel. The example in figure 3.2 describes this process. The central pixel is compared to the pixel circled in red. As the circled pixel is lower in value than the central pixel this means the central pixel is assigned a bit value of 0 in the final fingerprint. In this manner the fingerprinting algorithm encodes gradient information in the y-axis rather than contrast information. This process is repeated for each pixel in the image.

This algorithm is known as Reduced-LBP (R-LBP) due to the fact the binarization step reduces the amount of information used from what is in LBP. By doing this we maintain the global illumination invariance of LBP whilst removing the need to use the entire feature vector in authentication. However, this also reduces the number of pixel comparisons down from N to 1. Thus making R-LBP.V1 vulnerable to noise. Any alteration to the first or central pixel in a repeat image will result in a different value in the fingeprint. This will be a particular issue for QD patterns that are "flat" (texture is uniform with all pixel values lying within a small range) in nature. It is used in this thesis however, as

an example of the simplest possible solution to compare to.

3.3.5 RLBP.V2

The driving force behind RLBP.V2 is to maximise the information that is encoded into the value of the central pixel in the final fingerprint. As already discussed in section 3.3.4 comparing between only two pixels reduces not only the fingerprinting algorithm's resistance to noise or other outside effects but also the entropy present in the final fingerprint. For example see figure 3.3. In RLBP.V1 a feature that spans any width of the image will be the only area of comparison for the pixels spanning the same width a distance of R below it. The QD pattern in figure 3.3 has a clear example of this within the two large black areas within it, located in the top left and bottom right of the image. In the fingerprint generated from the pattern there can be seen two black areas with no variation that correspond to these. Similarly is the large bright areas in the middle and top left of the image which have matching white areas in the fingerprint.

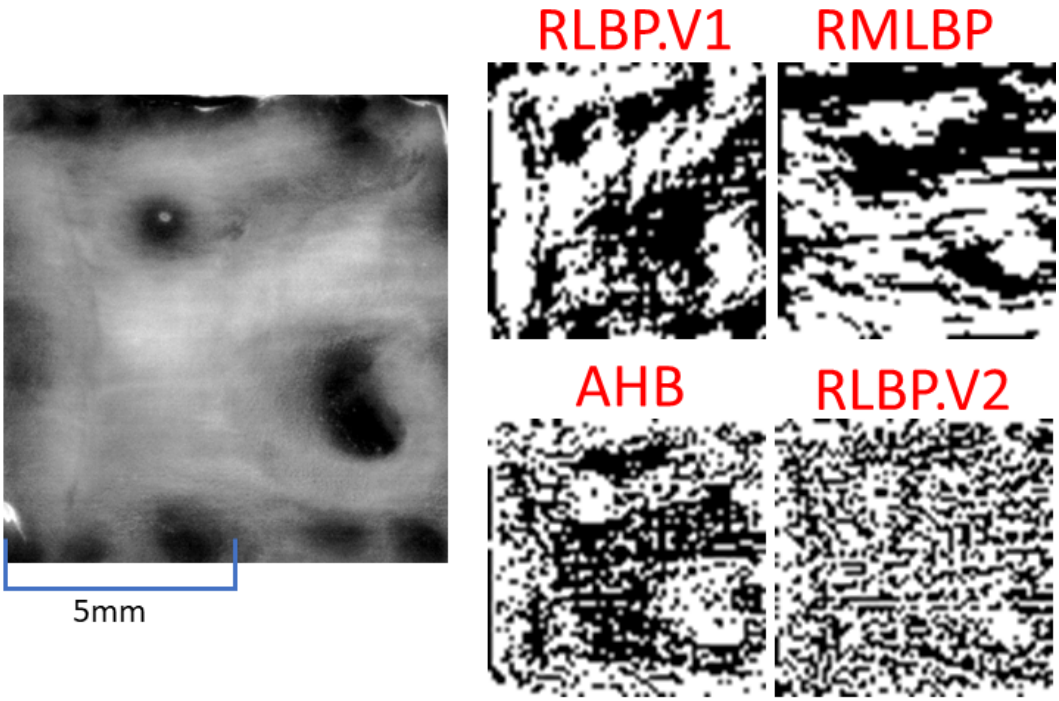

Figure 3.3: Left: Image of a quantum dot pattern taken from a tag made with InP in a SEBS lacquer. Image is brightened for clarity of viewing. Right: Example fingerprints of the pattern to the left made with each of the four techniques analysed in this paper. Each was created at $R = 7$, R-MLBP and RLBP.V2 were created with $N = 16$. Each fingerprint is 64x64 px in size.

In order to correct for these issues RLBP.V2 uses all of the circumference pixels in its comparison (as can be seen in figure 3.4). The first part of the feature vector is generated

in the same manner as LBP, with each pixel being compared to that of the central pixel. Starting from the top pixel each is assigned a value of 1 in the feature vector if they are greater than or equal to the central pixel in value, 0 if they are not. In this case however, a final bit is added to the end of the feature vector. For this the central pixel value is compared to the mean value of all of the pixels on the circumference. If the central pixel is greater than or equal to the mean value then this final bit is given a value of 1, if not it is given a value of 0. Not only does this now encode the relative brightness between the central pixel and its local area it gives an odd numbered bit length feature vector (as N is always even), see figure 3.3 for example. This now allows for the final value of the central pixel that is passed to the fingerprint to be determined by majority voting. The modal value of the feature vector is taken to create the bit value that is used in the fingerprint. Thus, successfully using as much of the local texture information as possible to create the fingerprint.

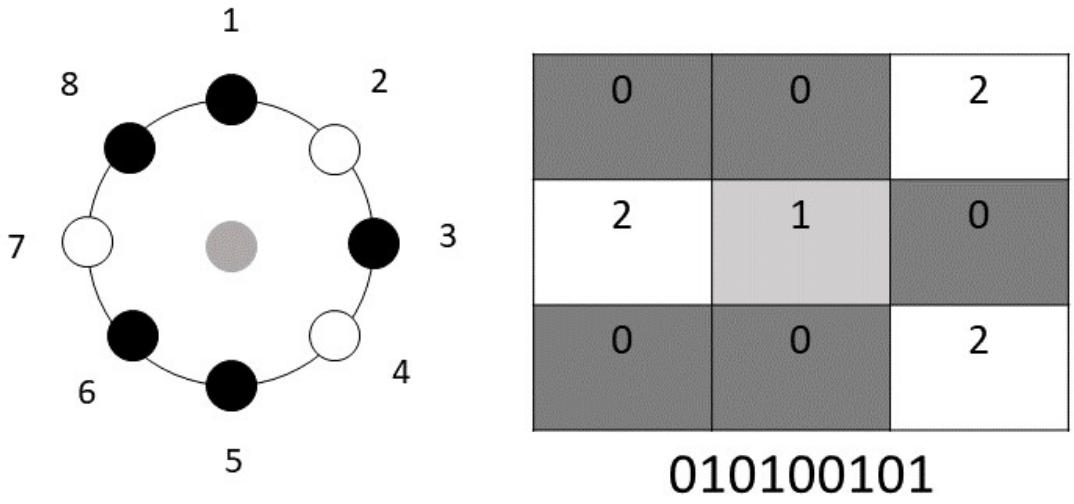

Figure 3.4: Left: Pictorial representation of the "LBP circle" used by RLBP.V2. The grey circle represents the central pixel. The black and white circles represent the pixels being compared to the central pixel, each of which lies on the circumference of a circle with radius R centred on the central pixel. A black circumference pixel represents that it is lower in value than the central pixel, white represents that it is equal to or greater than the central pixel in value. The numbers represent the order each pixel is compared to the central pixel in. Right: Mock up of the section of an image the LBP circle to the left is analysing (assuming $R = 1$). Again the central pixel is coloured in grey. The values written in each pixel are arbitrary brightness values. Below the diagram is the feature vector string that RLBP.V2 would have generated for this central pixel.

This particular method grants RLBP.V2 some advantages over the over three techniques discussed here. The first of all is the entropy that the fingerprints produced from it possess. As will be detailed in chapter 4 this allows for RLBP.V2 to produce fingerprints with a high degree of uniqueness. Which in turn leads to it being able to be used to accurately match tags through fuzzy authentication methods. Not only does it maintain the global illumination invariance of LBP but it is also rotationally invariant. This is due to the fact that it does not matter the order of the bits in an RLBP.V2 feature vector when majority voting is applied. What this means is that if the challenge image is rotated

through any number of $\frac{360^\circ}{N}$ increments the output fingerprint will be the exact same only rotated through the same increment. This would not occur with the other LBP adjacent schemes analysed here as they have directional dependence to their fingerprinting. There is however, an issue with this technique. Every bit in the feature vector is dependant on the central pixel, as such any shift in the value of the central pixel between the challenge and reference image may change the value of the bit in the fingerprint. Thus, indicating that RLBP.V2 will still be affected to damage to the challenge image.

3.3.6 RMLBP

To first discuss Reduced Modified-LBP (RMLBP) it is important to break down the two key components within the fingerprinting algorithms. There is the feature extraction algorithm that makes up the base of it (such as LBP) and the binarisation technique that reduces the information for a pixel to a single bit value (such as majority voting). The purpose of RMLBP is to create a fingerprinting algorithm that is as resilient to damage, including image noise, to the image as possible.

To achieve this the base algorithm was altered from LBP to Modified-LBP (M-LBP). The binarisation algorithm was kept the same however as this had shown to provide some degree of noise resilience in other techniques during the refinement and testing process. Modified-LBP[46] was designed to reduce the length of LBP feature vectors to reduce the difficulty of using them in texture classification. It also acts to encode gradient and local contrast information into the feature vector. Coupled with the majority voting binarisation technique this gives Reduced MLBP (RMLBP). To first generate the feature vector RMLBP splits the LBP circle into two halves, left and right, each with $\frac{N}{2}$ pixels. The value of centre symmetric pixels across the LBP circle are then compared (pixels with matching colours in figure 3.5). If the pixel in the right hand side of the LBP circle is greater or less than the value of that in the right that pair is assigned a value of 1, if it is lower the pair is assigned a value of 0. Finally the centre pixel value is compared to the mean value of the circumference pixels. If the central pixel is greater than or equal to the mean value then this final bit is given a value of 1, if not it is given a value of 0. All of the pair bit values and the bit value of the centre-mean comparison are concatenated together to make a feature vector $\frac{N}{2} + 1$ in length. To determine the final bit value of the central pixel the modal value of the feature vector is taken.

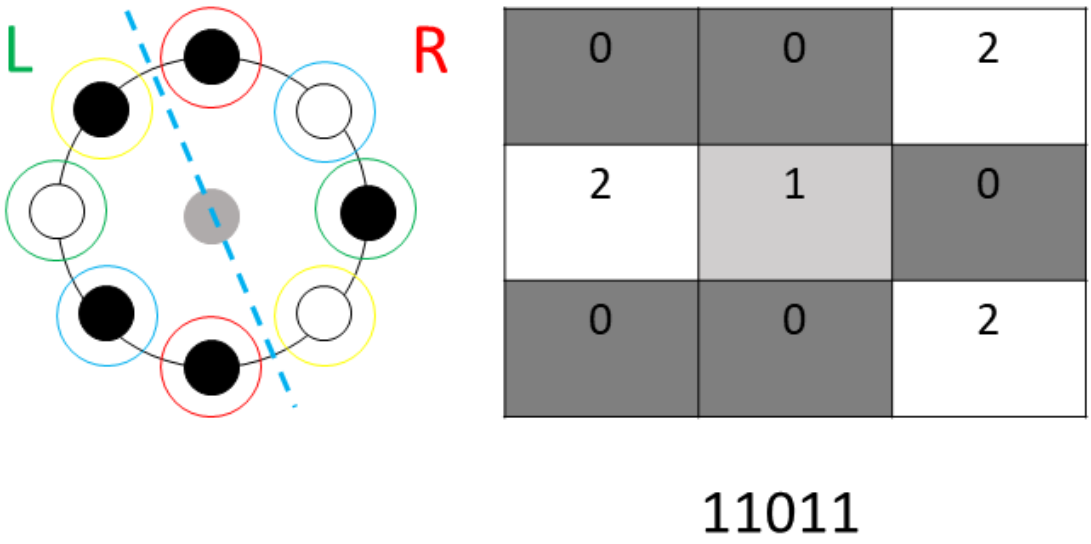

Figure 3.5: Left: Pictorial representation of the "LBP circle" used by RMLBP[46]. The grey circle represents the central pixel. The black and white circles represent the pixels being compared to the central pixel, each of which lies on the circumference of a circle with radius R centred on the central pixel. A black circumference pixel represents that it is lower in value than the central pixel, white represents that it is equal to or greater than the central pixel in value. The coloured rings represent which pixel is compared to which. "L" and "R" represent which half of the LBP circle is dubbed the left and the right. Right: Mock up of the section of an image the LBP circle to the left is analysing (assuming $R = 1$). Again the central pixel is coloured in grey. The values written in each pixel are arbitrary brightness values. Below the diagram is the feature vector string that RMLBP would have generated for this central pixel.

The fact that this algorithm encodes gradient orientation, that the central pixel is only used in the comparison for one bit in the feature vector and with the binarisation it grants several boons to this method. Primarily that it makes this technique highly noise resistant[46], even on flat QD patterns which are most prone to poor fingerprints in noisy conditions. This is demonstrated in chapter 4 RMLBP produces the fingerprints with the highest degree of repeatability, regardless of what damage is done to the challenge image. The catch here however is that the fingerprints do bear large areas with little variation similarly to RLBP.V1 (as can be seen in figure 4.1). This hampers the ability to accurately tell them apart from fingerprints of other QD patterns despite fingerprints of the same pattern being so alike (as later shown in chapter 4). This is because when all the fingerprints contain large uniform areas the probability of two pixels having the same value is increased. Further testing has shown however that RMLBP fingerprints contain little enough noise that entropy increasing techniques (such as XOR debiasing detailed in section 5.2) can be used to solve this issue and still give repeatable fingerprints.

3.3.7 AHB

The last of the algorithms analysed in this thesis is the only one not based on LBP or a variant thereof. It is included in this thesis to build on the work performed by Marcinkevicius et al[2]. In that work it was demonstrated that Adaptive High Boost (AHB) can be used to extract a binary fingerprint from a QD pattern when it is imaged under a

microscope. Here we demonstrate that such a level of magnification is not needed and compare it to other novel techniques.

AHB was proposed originally as an alternative to Gabor filters for use with speckle pattern optical PUFs[2]. In simple terms AHB assigns a pixel a value of 1 or 0 depending on its value relative to the values of its neighbouring pixels. It does this by passing a convolution kernel over the image on a pixel-wise basis. For each position in the image, the centre pixel brightness value is multiplied by $1 - n^2$ (where n is the size of the kernel) and every other pixel covered by the kernel is multiplied by 1. The sum of all the kernel values is then calculated. If the sum is less than 0 the central pixel is brighter than its surroundings and dimmer if it is greater than 0. In the case of the former the central pixel is assigned the value of 1 and in the latter a value of 0. This dependence on relative brightness values over a neighbourhood of n^2 pixels makes the generated binary fingerprint independent of global shifts in pixel brightness. The kernel also ensures that AHB is computationally simple to use, demonstrated in that it is quicker to generate a fingerprint with that LBP based schemes (in order of fraction of seconds). At high R values taking in so many pixels reduces the effect of noise on the final pixel result, at the cost of a larger amount of data than needed for LBP techniques. It does also reduce the ability of AHB to encode small scale details into its final fingerprint and its accuracy at handling flat patterns.

Chapter 4

Fingerprinting Algorithm Performance Testing

In order to harness the uniqueness of the QD-PUFs discussed in this thesis a method is needed to digitise them so that they can be used in authentication. Section 3.3 has detailed the process by which the fingerprinting algorithms perform this process. Although qualitative predictions can be made about their performance, these are no use when looking to compare the algorithms and determine potential use cases. In this chapter the algorithms will be quantitatively analysed in terms of their performance. The first test of this will be a direct comparison. Three QD-PUFs have been chosen such that they each have distinctly different textures. Fingerprints over a range of radii will be generated from these by each of the algorithms, giving us figures of merit that can be compared. This provides a baseline performance for the algorithms, showing how they perform in optimal conditions. This is valuable information for the use and application of them.

In the majority of cases that QD-PUFs may be used outside of the laboratory they will not be used in these optimal conditions. Thus, the remainder of this chapter is dedicated to simulating less than optimal conditions. Chiefly by "damaging" the QD-PUF images by increasing amounts of damage and comparing them to their undamaged counterparts. This will give a measure of which algorithms are the most resistant to change in their output fingerprint outside of laboratory settings. The more robust an algorithm is to damage to the input image the closer the generated fingerprint will be to one created under optimal conditions. Two types of damage to the QD-PUF image are tested, chosen as these are the most common to occur when using lower quality imaging apparatus (such as a smartphone) in non-laboratory conditions. These are the addition of blur to the image and separately the addition of noise. This will give highly useful information for how the algorithms will perform in a more practical setting.

Section 4.1 provides an in depth analysis of the algorithms in terms of quantitative figures of merit. It acts as a proof of concept of the fingerprinting process. Section 4.2 takes this process further to analyse the limitations of each algorithm, with particular regards to their robustness against blur and noise.

4.1 Comparison of Algorithms

Although each algorithm in section 3.3 produces a binary output from a grey scale image each encodes the information in a different manner. Even within the two separate groupings, contrast based or gradient based, the number of data points is different. As such it is important to test how each performs, this will inform us as to which of them meet the aforementioned minimum criteria and what use case each is best suited to. This section therefore will provide an in-depth quantitative analysis of the performance of the fingerprinting techniques.

4.1.1 Analysis Process

To generate the data required for this analysis 25 repeat images of a series of three different quantum dot patterns is taken using the blackbox apparatus shown in figure 3.1. Each QD pattern image is then fingerprinted by each of the four fingerprinting algorithms (RLBP.V1, RLBP.V2, RMLBP and AHB). Fingerprints are generated for each integer value radius in the range $R = 1 - R = 20$, with R being measured in pixels. For RLBP.V2 and RMLBP a N value of 16 is used. The fingerprints are then grouped based on QD pattern, algorithm and radius.

For intra hamming distance calculations the first two fingerprints of the 25 repeats for the pattern at the radius being tested are used as "challenge" fingerprints. The rest of the fingerprints are then used as "reference" fingerprints. The challenge fingerprints are then compared to the reference fingerprints in order to generate the intra hamming distance distributions. For the inter hamming distance distribution the same two challenge fingerprints are then compared to each of the fingerprints generated for other patterns. In total each challenge fingerprint was compared to fingerprints generated from 47 other separate QD patterns. This database of reference fingerprints is used throughout the thesis whenever figures of merit for fingerprints are generated. It is important to note when comparing to only compare between fingerprints generated at the same radius. Intra and inter hamming distance mean and standard deviation, FPR and ENIB are then calculated for each value of R. This process is then repeated for each pattern at each value of R.

For all of the analysis undertaken within this chapter, three different quantum dot patterns will be used as the challenge QD-PUFs. CISPMS (CIS620 dots in PMS lacquer), SEBS (InP dots in SEBS lacquer) and PVDFPLMA (InP dots in PVDFPLMA lacquer). Given the number of different algorithms and parameters to be tested any more would be impractical to cover in this chapter. Therefore in order to cover the algorithms in detail the analysis is limited to these three. Each pattern was chosen because they represent very different types of QD patterns. Quantitative classification of the types of patterns is beyond the scope of this thesis so more qualitative terms will be used. This is because texture classification is a complex field of computer vision within itself. The time required to develop a classification system for the variety of quantum dot patterns used was not viable within the time frame of this thesis. CISPMS represents QD patterns with a high degree of contrast and discrete patterns (i.e. the bright dots on a black background). PVDFPLMA represents "flat" QD patterns, these have low variation in the brightness values across the entire pattern and have no distinct features or features who's scale is comparable to the size of the whole QD-PUF. SEBS represents the middle ground be-

tween the two with larger features and gradually changing brightness. Images of these can be found in figure 4.1.

4.1.2 Analysis and Results

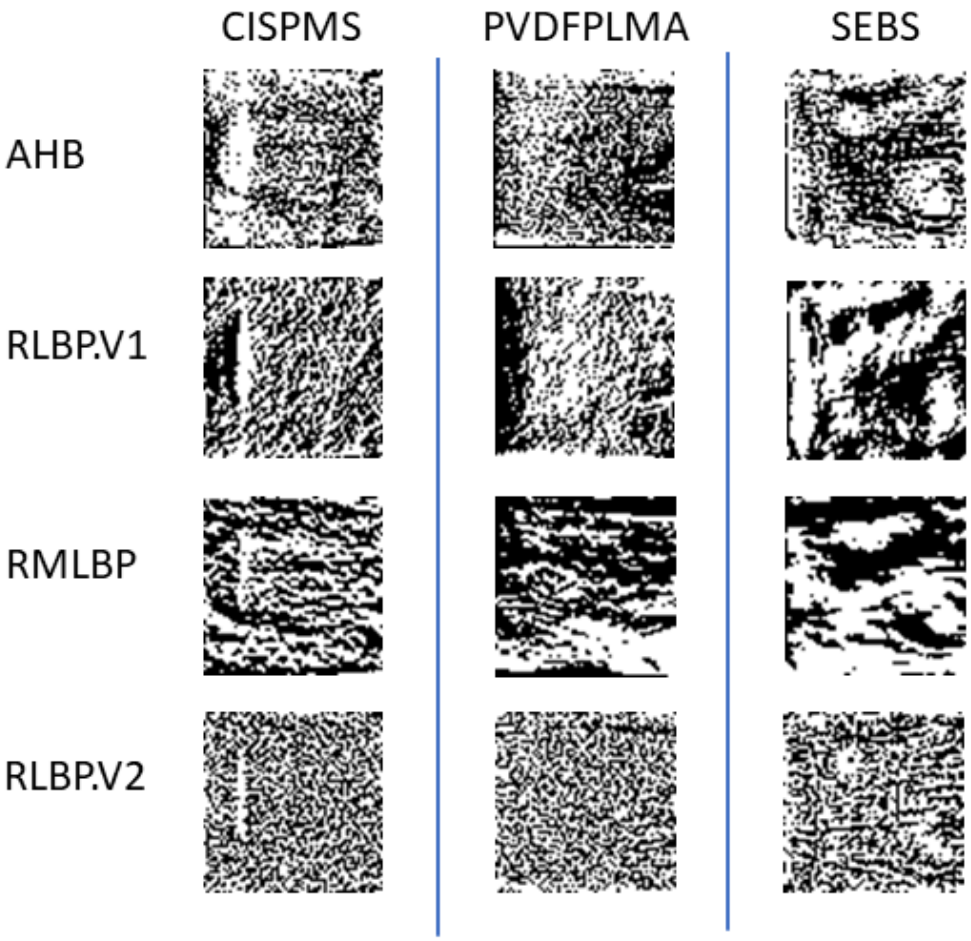

Figure 4.1: Examples of fingerprints generated by each algorithm at a radius of 10 for each of the QD-PUFs tested in this section. Columns represent the same QD-PUF and rows represent the same algorithm.

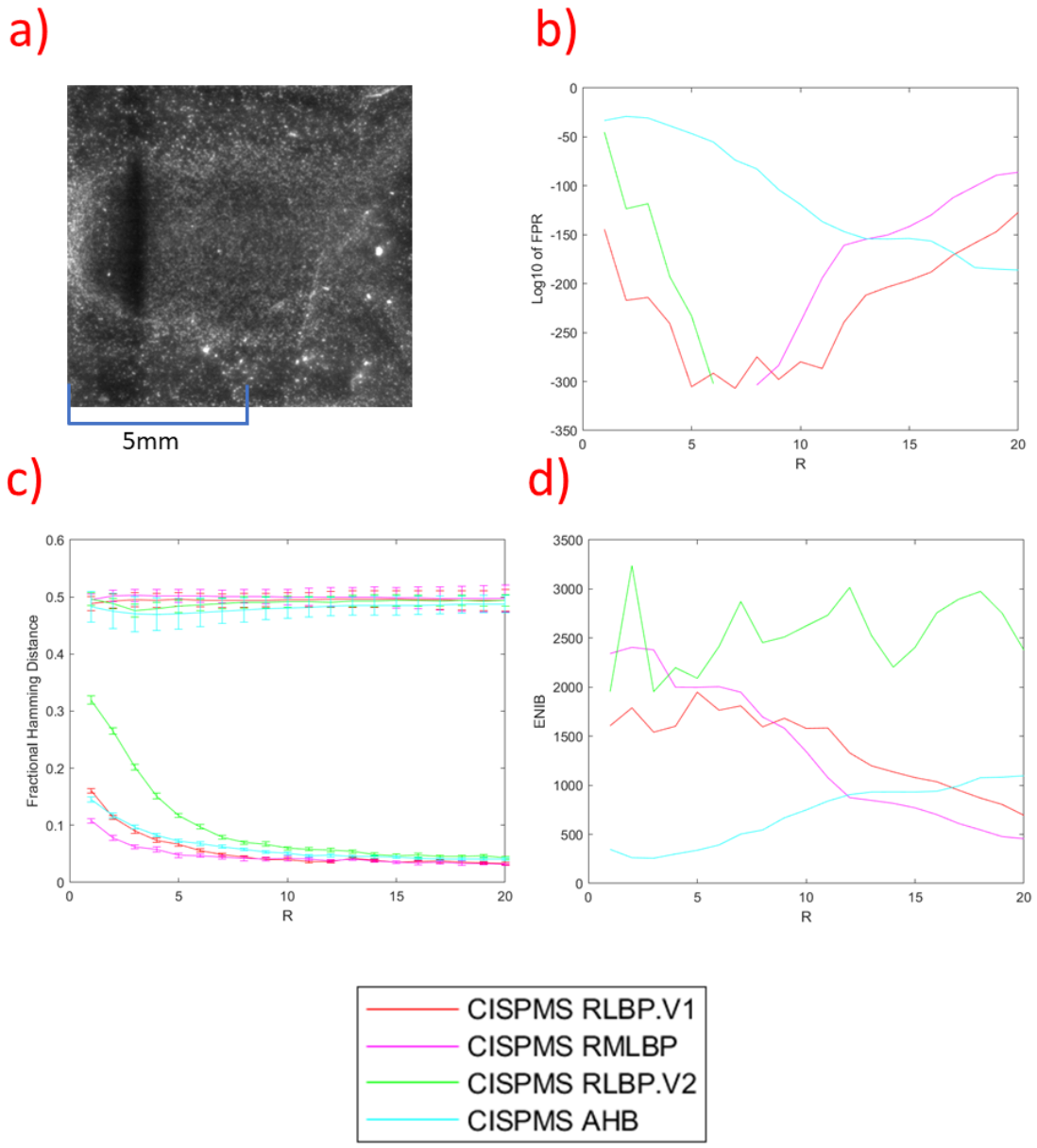

Figure 4.2: a) image of a quantum dot pattern made with CIS620 dots in PMS lacquer. Taken with the system shown in figure 3.1. b) Graph of log_{10} of the FPR against increasing radius. c) Graph of fractional intra and inter hamming distances against increasing radius. Error bars show the standard deviation of the hamming distance over the fingerprints compared. The top line represents a given QD-PUF's inter hamming distance and the bottom the intra hamming distance. d) Graph of Effective Number of Independent Bits against increasing radius.

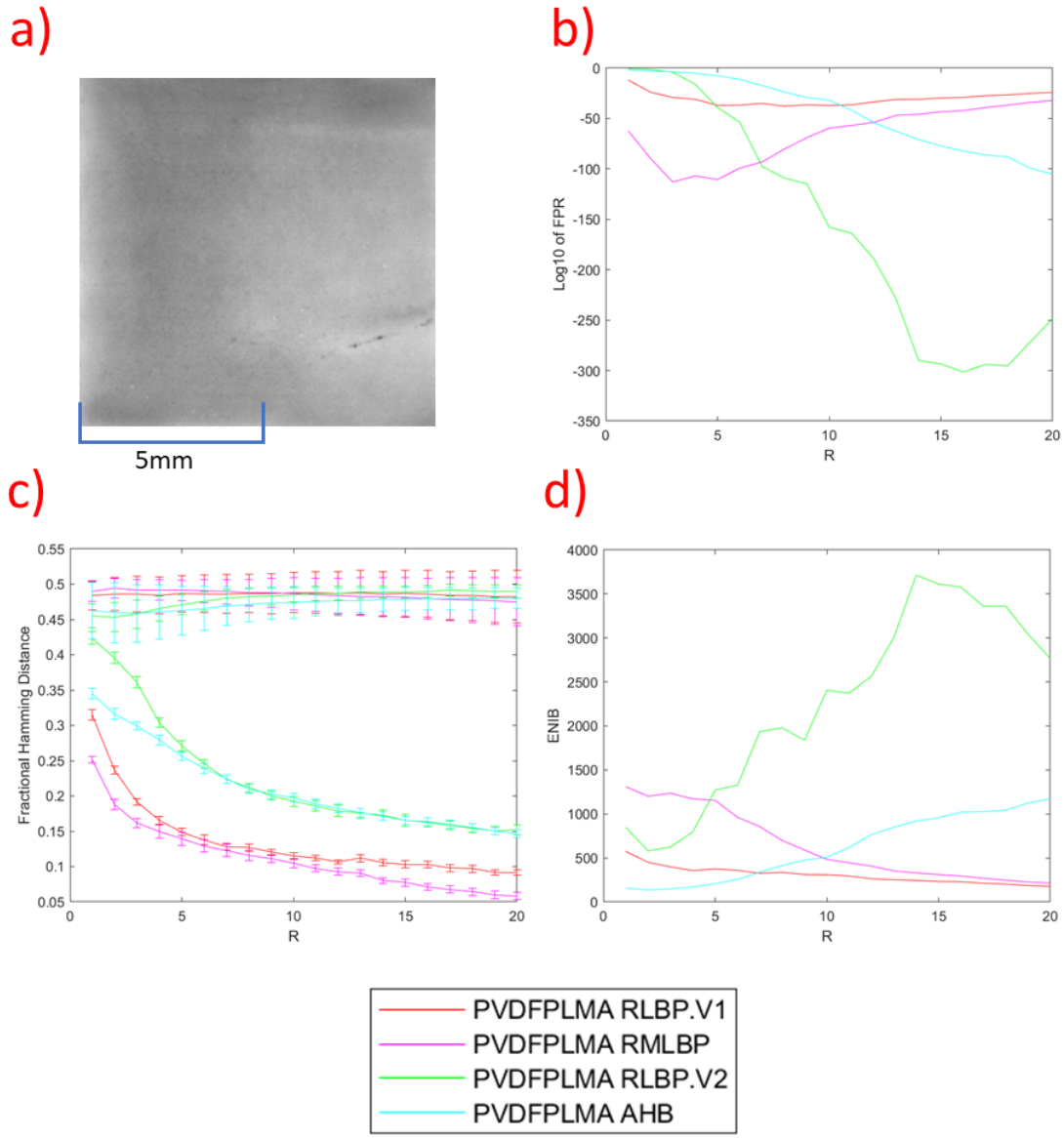

Figure 4.3: a) image of a quantum dot pattern made with InP dots in PVDFPLMA lacquer. Taken with the system shown in figure 3.1. b) Graph of log_{10} of the FPR against increasing radius. c) Graph of fractional intra and inter hamming distances against increasing radius. Error bars show the standard deviation of the hamming distance over the fingerprints compared. The top line represents a given QD-PUF's inter hamming distance and the bottom the intra hamming distance. d) Graph of Effective Number of Independent Bits against increasing radius.

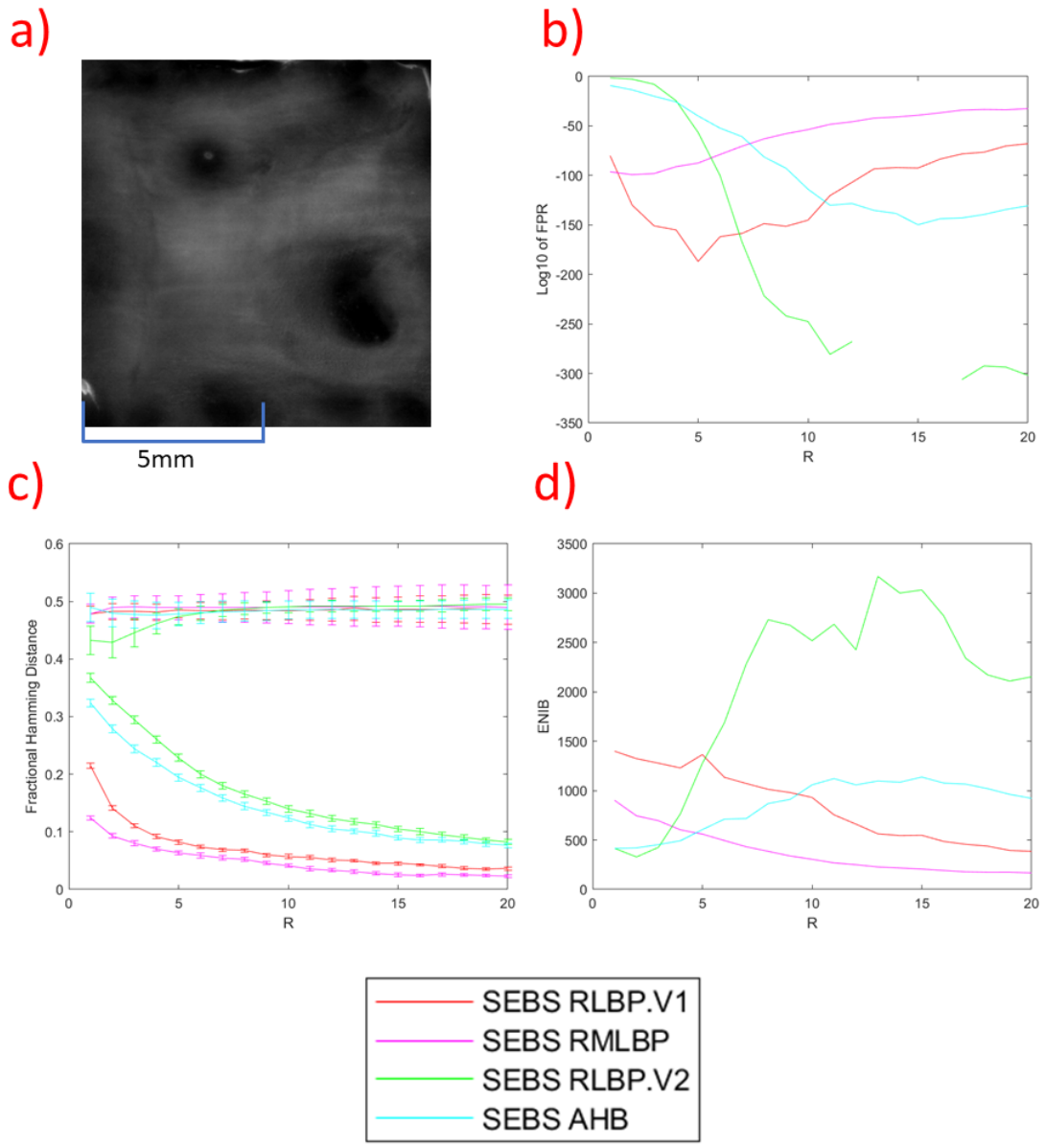

Figure 4.4: a) image of a quantum dot pattern made with InP dots in SEBS lacquer. Taken with the system shown in figure 3.1. b) Graph of log_{10} of the FPR against increasing radius. c) Graph of fractional intra and inter hamming distances against increasing radius. Error bars show the standard deviation of the hamming distance over the fingerprints compared. The top line represents a given QD-PUF's inter hamming distance and the bottom the intra hamming distance. d) Graph of Effective Number of Independent Bits against increasing radius.

When observing the FPRs of the different fingerprinting algorithms the most obvious point is the differing performance of RLBP.V2 over the other three techniques. All of the algorithms produce FPR minima many orders of magnitude below the requirement of 10^{-6}, even for PVDFPLMA of which is has the highest FPR minima for all of them. Despite this however RLBP.V2 has minima multiple orders of magnitude lower than each of the other algorithms. The origin of this lies in a matter discussed in section 3.3.5, out of all of the algorithms RLBP.V2 produces the fingerprints with the highest degree of entropy. As can be seen in figure 4.1 all but RLBP.V2 tend to produce fingerprints

with more structured patterns, often consisting of large uniform areas of 1's or 0's (shown pictorially as white or black pixels respectively). This poses an issue when considering fingerprint uniqueness, large areas of singular value make it more likely a particular pixel will match in value its corresponding pixel in a fingerprint of another pattern. This is even more likely in the case of RMLBP who's fingerprints show a bias for large uniform areas stretching horizontally across the fingerprint. Therefore this increases the mean FPR of RLBP.V1, RMLBP and AHB over almost all R when compared to RLBP.V2. This is supported by the ENIB of each algorithm. At $R = 15$ where RLBP.V2's FPR minima tends to lie its ENIB is ~ 1000 bits greater than the next closest algorithm in each case presented here. Mathematically speaking this means that RLBP.V2's fingerprints show the least repeated patterns when one qualitatively observes over the fingerprints of all patterns in the database.

This has a pay-off however in that RLBP.V2 does have the highest mean intra hamming distance over all R values (in the case of PVDFPLMA matching closely with AHB for $R \geq 7$). The implications of this will be discussed in greater detail later. Despite this fact RLBP.V2 still achieves the lowest FPR, this is due to it's unique fingerprints granting it the lowest inter standard deviation of the algorithms. Visually speaking this is due to the more complex, higher entropy patterns in RLBP.V2 fingerprints. The lack of blocky areas giving it a larger degree of difference between fingerprints of different QD-PUFs. For example, in the case of SEBS where the intra over all R for RLBP.V2 is highest relative to the other algorithms, it had an inter hamming distance of 0.491 ± 0.008 at $R = 15$. RLBP.V1 achieved 0.49 ± 0.02, RMLBP achieved 0.49 ± 0.03 and AHB achieved 0.49 ± 0.01. Thus, indicating when creating a fingerprinting algorithm the uniqueness of the fingerprints generated is more important for accurate identification than the consistency of repeat fingerprints from the same pattern.

Continuing the comparison between the FPR behaviours of each technique we come to the location of the minima of each of the algorithms. The four algorithms can be split into two pairs, those that encode local contrast information (RLBP.V2 and AHB) and those that encode local gradient information (RLBP.V1 and RMLBP). As we will see throughout this thesis the algorithms show more similar behaviour to their pair partner than the other algorithms. The location of FPR minima is one such example, in each case the minima for the contrast based schemes occurs at a higher R value than those of the gradient based schemes. Indicating that the gradient based schemes produce fingerprints with more accurate authentication when encoding fine scale details. This is because at higher R values local gradient changes become smeared out, causing the fingerprints to be dependant on any gradients that are approaching global in scale. These being much larger in size they create large uniform areas of 1's and 0's within the fingerprint. Whilst this makes for highly repeatable fingerprints (see intra hamming distance discussion) it has a negative impact on the entropy and uniqueness of the fingerprint. This is indicated by a higher inter hamming distance standard deviation and a lower ENIB. As has already been discussed the uniqueness of the fingerprint is more important than it's repeatability in achieving low FPR values thus, limiting the FPR minima of gradient based schemes to lower R values. Contrast based schemes however are less effected by these global patterns and so maintain their entropy whilst losing the issues of noise that plague at low R. Causing them to outperform gradient based schemes at high R values. It should however, be noted that due to the greater resilience to noise possessed by gradient based schemes

their intra hamming distances at their FPR minimum are still lower than those of the contrast based schemes at a higher R value.

The behaviour of the hamming distances of each of the pairs of algorithms gives further insight into their behaviour. It is clear that the gradient based schemes produce lower fractional intra hamming distances for all R values (this is less clear cut with CISPMS which will be discussed shortly). As previously mentioned this is due to the fact that the gradient based schemes are more resilient to noise than their contrast based counterparts. This allows them to produce more repeatable fingerprints. Consistently over all of the data analysed RMLBP does produce the lowest intra hamming distance for all R. It achieves fingerprints whose mean difference to repeats from the same pattern can fall as low as 2% (SEBS at $R = 20$) and in the worst case are as high as 25% (PVDFPLMA at $R = 1$). This outstrips the other schemes whose ranges are: $3\% - 31\%$ for RLBP.V1, $4\% - 42\%$ for RLBP.V2 and $4\% - 34\%$ for AHB. This is because gradient based schemes produce the most stable fingerprints and out of the two RMLBP takes in the most information to generate each bit in the fingerprint, (9 bits are used in RMLBP as opposed to 2 in RLBP.V1). Thus, furthering improving its resilience to any camera noise. As well as this RMLBP is the only one of the algorithms to not use its central pixel to calculate every bit in its feature vector. Only one of RMLBP's bits is calculated using the central pixel. This grants it an advantage over the over algorithms in that any issue with the central pixel (that the fingerprint value is being calculated for) will have no effect on the final fingerprint bit. Granting RMLBP an extra degree of robustness that is reflected in its highly repeatable fingerprints.

For the pair of contrast based schemes the difference between them also falls down to how many bits are used to create the final fingerprint value. AHB takes in more bits than RLBP.V2 this gives it a higher resilience to noise as any noisy pixels have less of an effect on the final value. Although this grants AHB a lower intra hamming in most cases, it reduces the entropy of AHB fingerprints. As the AHB kernel passes over the image there will be a large amount of overlap between the pixels analysed for nearby central pixels. Particularly for adjacent pixels with similar values this leads to the same fingerprint value being calculated for all central pixels in a local area. As previously discussed in achieving a low FPR the entropy of the fingerprint is more important than the repeatability of it. Hence, AHB is the more resilient algorithm of the contrast based schemes but RLBP.V2 produces fingerprints with more accurate matches.

There is also a degree of difference in the performance of the schemes when looking over the three different QD patterns analysed in this paper. For contrast based schemes the fractional intra hamming distance is lower for CISPMS and highest for PVDFPLMA. This is unsurprising as CISPMS shows the greatest contrast over all of the patterns, with a dark background and bright dots. PVDFPLMA however has a much more flat pattern, the lower contrast over the area meaning that pixel noise has a greater effect thus, worsening the intra. On the opposite side the gradient based schemes show less of difference between the different patterns in terms of intra. Indicating less of a dependence of QD pattern "type" for producing reliable fingerprints.

To summarise, most importantly all of the algorithms met the criteria set down in section 3.3.1. Each produces an FPR minima far below the required limit and (with the excep-

tion of RLBP.V1 for PVDFPLMA) produce an ENIB about 512bits at the corresponding radius. Gradient based algorithms produce the more repeatable fingerprints but contrast based ones produce fingerprints with higher authentication accuracy due to higher entropy, with RMLBP and RLBP.V2 being the best performing at these tasks out of each group respectively.

4.2 Robustness Testing

In a more realistic setting outside of a laboratory the quantum dot patterns will be fingerprinted in sub-optimal conditions. Whilst it is important to know the performance of the fingerprinting techniques in laboratory conditions to set a standard for performance, this same standard will not be met outside of a laboratory. Damage to the input image will worsen the measured figures of merit, potentially to the point where the fingerprinting technique is no longer useful for authentication. This section aims to quantify the effects of common types of image damage on the quality of produced fingerprints.

4.2.1 Analysis Process

For the damage testing two different "types" of damage were analysed, each with ten increasing levels of severity (details of which are given below). To create the fingerprint sets for the robustness testing a copy is made of the images of the QD pattern being tested. This is done for each of the different types of "damage" and levels of severity applied to the QD pattern images. In each case the images that will become the challenge fingerprints have the damage applied to them. The reference images are left unaffected. This simulates an issue with the capture device when Bob is attempting to authenticate the QD patterns. Fingerprints are then generated from these damaged images with each of the algorithms at $R = 1 - 20$. The rest of the analysis to generate hamming distances and figures of merit then continues as detailed in section 4.1.1. It should be noted however that in the case of these tests the intra hamming distance now represents a measure of how much the damage to the challenge image has changed the fingerprint from the original. Giving a measure of how robust the fingerprinting algorithm is to the effects of the damage.

The details of the different types of damage applied to the QD pattern challenge images are as follows (note, only one is ever applied at a time):

- **Blurring:** The challenge image has a Gaussian filter applied to it using the *imgaussfilt* function in MATLAB[47]. The levels of severity span from 1 to 10 in steps of 1 and signify the standard deviation of the smoothing kernel applied. The higher the standard deviation the more blurred the image becomes.
- **Noise Adding:** The *imnoise* function in MATLAB was applied to the challenge image, with type set to "speckle". This "adds noise adds multiplicative noise using the equation $J = I + nI$, where n is uniformly distributed random noise with mean 0 and variance" defined by the user (quoted from[48]). I represents the initial pixel value and J the final value of the pixel after noise has been applied. The levels of severity are determined by the variance of n which spans the range of 0.1 to 1 in steps of 0.1 with 0.1 being the least noisy and 1 being the most.

4.2.2 Blurring

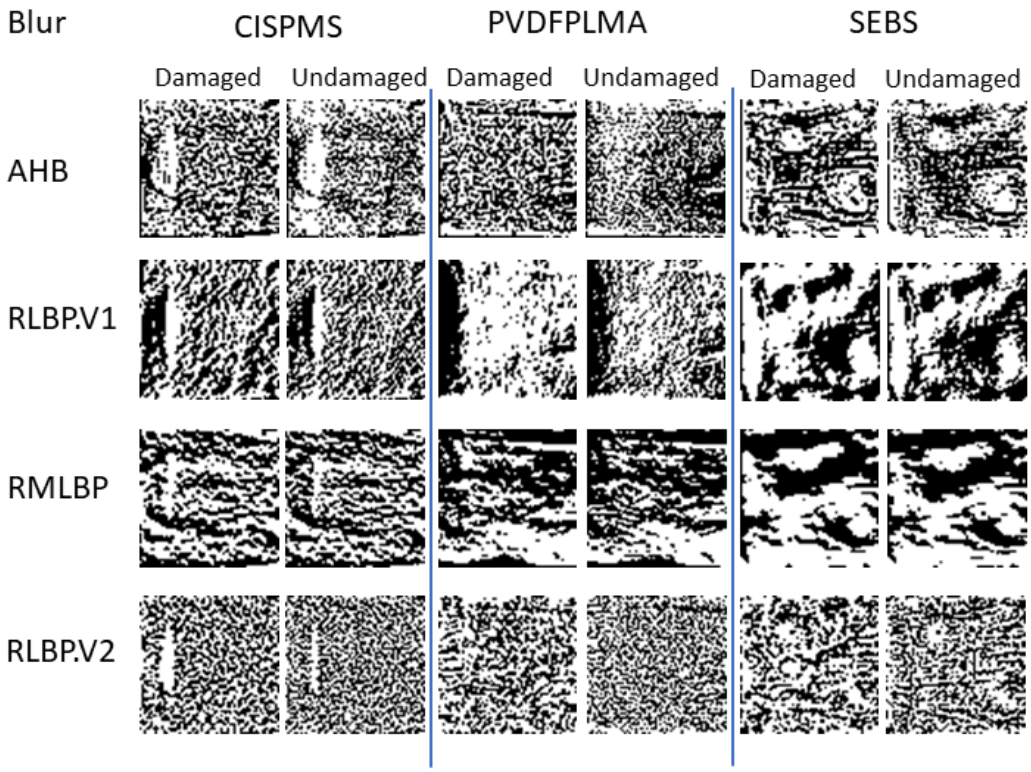

Figure 4.5: Table of example fingerprints generated for the blur section of robustness testing. Rows represent different fingerprinting techniques. Columns represent individual quantum dot patterns, with each column split into a fingerprint generated from a blurred image on the left and an undamaged image on the right. Each fingerprint shown was generated at $R = 10$ and the level of blur was set to a standard deviation of 5 as this is the midpoint of the blur severity available with the $imgaussfilt$ function, as discussed in section 4.2.1.

The application of greater degrees of Gaussian blur to the challenge images serves to smooth out larger and larger scale features with each increase in standard deviation. The techniques that can produce the most accurate fingerprints from these damaged challenge images will be those that can maintain the uniqueness of their fingerprints despite the loss of small scale features. Disregarding AHB (as its performance under blur was unique in comparison to the others), we can see in figure 4.5 that granular detail has been lost in the fingerprints when blur is applied. What is most striking of these three is that the damaged fingerprints of RMLBP appear almost untouched when compared to their undamaged counterparts at this blur and R value. A fact that supports the hypothesis put forward in section 4.1.2 that RMLBP can produce such low intra hamming distance values because on a larger scale, changes of brightness within an image are unaffected by any noise within them. The fact that when any noise and small scale details are removed the fingerprints are so similar serves as proof of this. It should be remembered though that such conclusions are qualitative and only apply under these particular parameters.

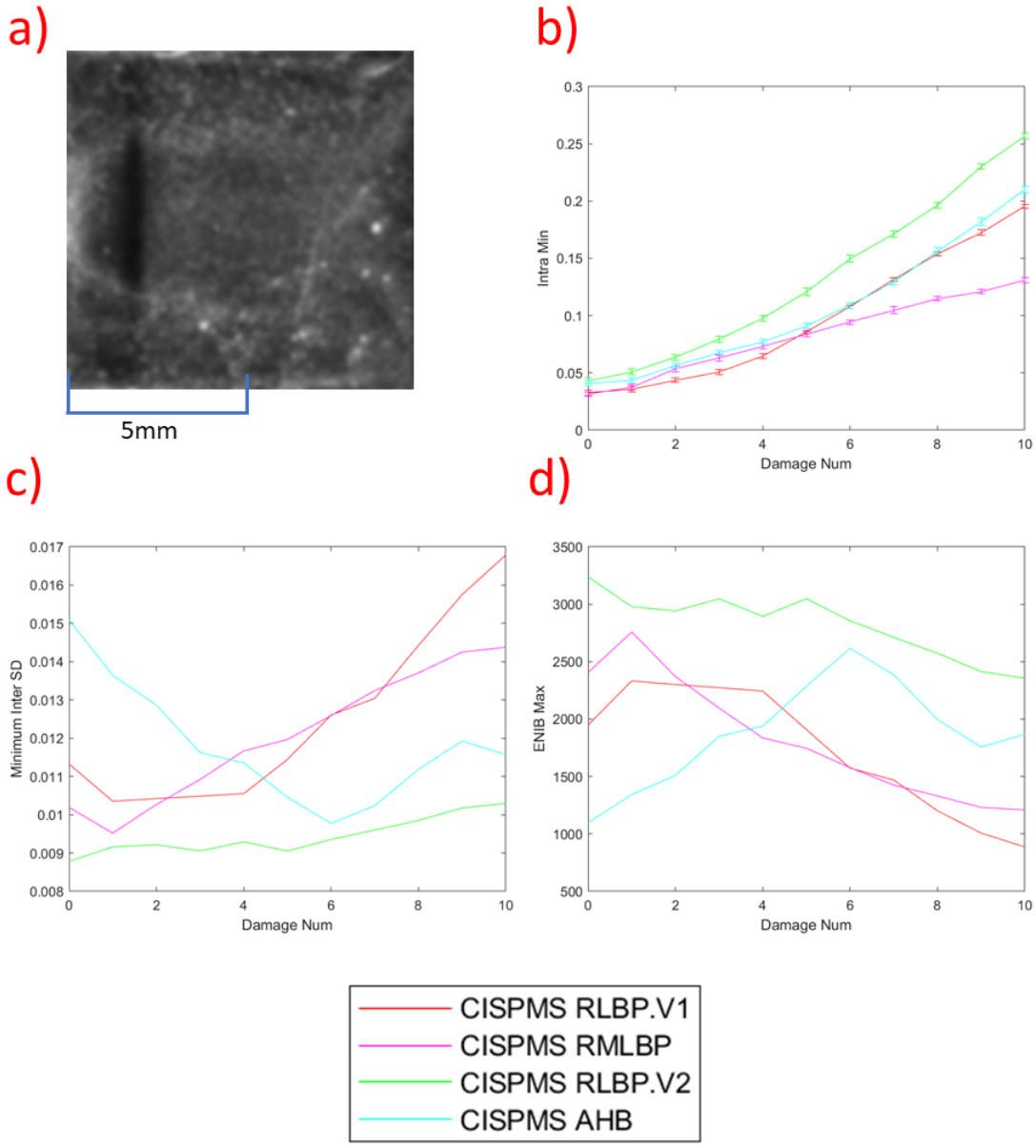

Figure 4.6: a) image of a quantum dot pattern made with CIS620 dots in PMS lacquer, the image was then blurred with a Gaussian filter with a standard deviation of 5. Taken with the system shown in figure 3.1. b) Graph of the minimum intra hamming distance achieved over all R at each increment of increasing blur severity. c) Graph of the minimum inter hamming distance standard deviation achieved over all R at each increment of increasing blur severity. d) Graph of the maximum ENIB achieved over all R at each increment of increasing blur severity.

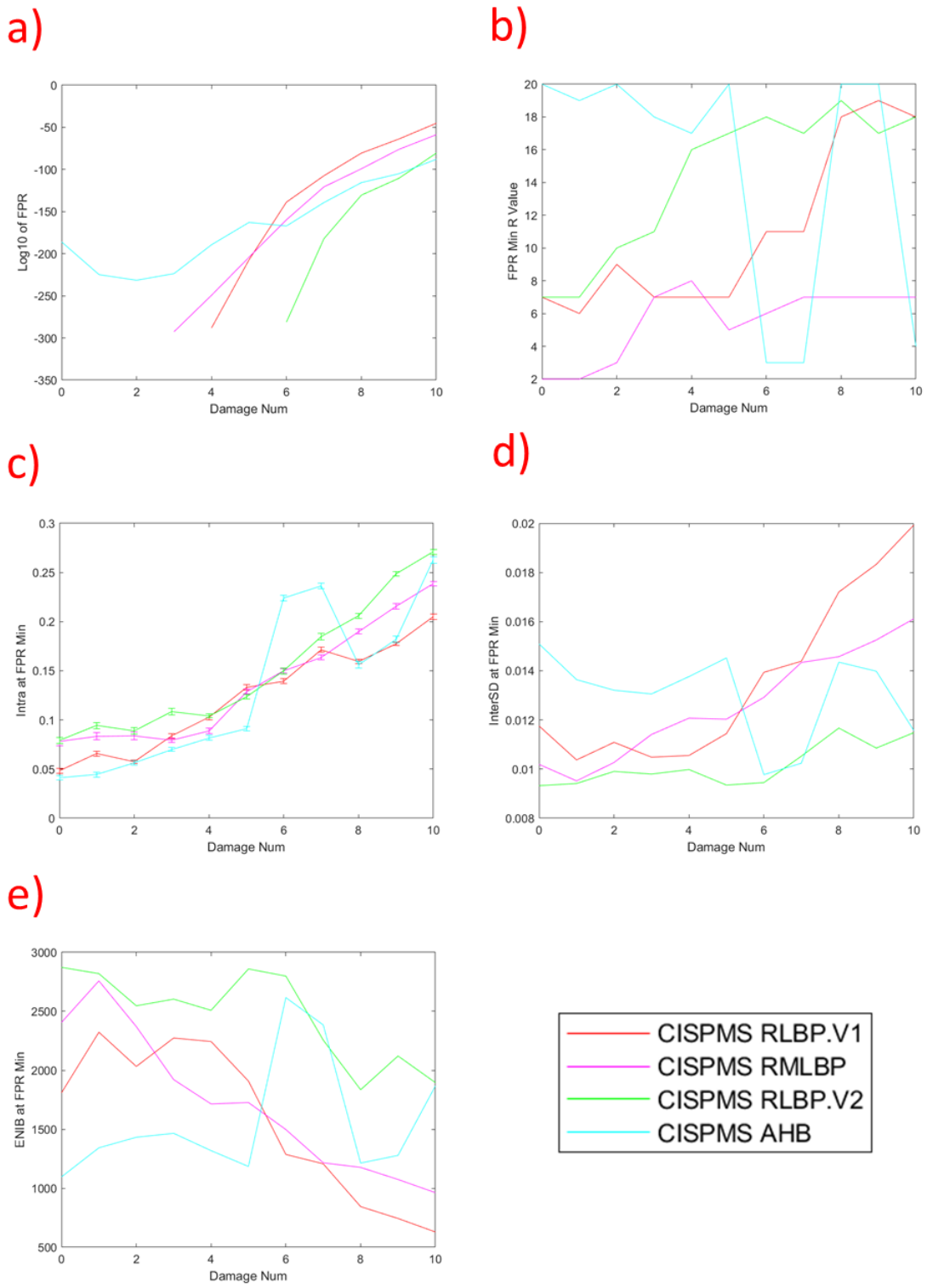

Figure 4.7: a) Graph of log_{10} of the minimum FPR achieved at each increment of increasing blur severity over all R for the CISPMS quantum dot pattern. Missing data points occur when the generated FPR falls below the precision of MATLAB, 10^{-308}. b) Graph of the radius values R where the FPR minimum show in graph a) occurs at each increment of increasing blur severity. c) Graph of the intra hamming distance at the R value where the FPR minimum occurs at each increment of increasing blur severity. d) Graph of the inter hamming distance standard deviation at the R value where the FPR minimum occurs at each increment of increasing blur severity. e) Graph of the ENIB at the R value where the FPR minimum occurs at each increment of increasing blur severity.

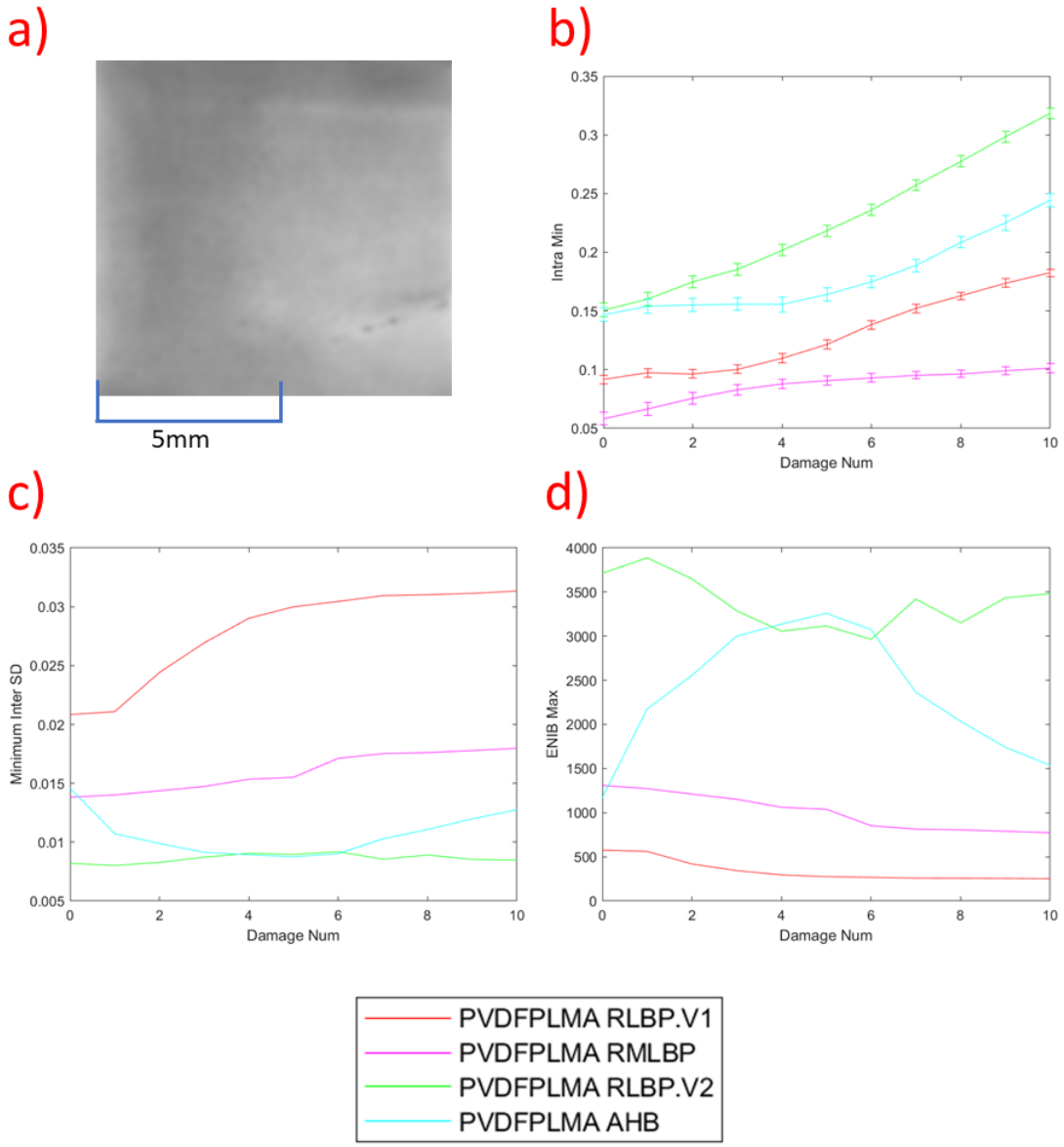

Figure 4.8: a) image of a quantum dot pattern made with InP dots in PVDFPLMA lacquer, the image was then blurred with a Gaussian filter with a standard deviation of 5. Taken with the system shown in figure 3.1. b) Graph of the minimum intra hamming distance achieved over all R at each increment of increasing blur severity. c) Graph of the minimum inter hamming distance standard deviation achieved over all R at each increment of increasing blur severity. d) Graph of the maximum ENIB achieved over all R at each increment of increasing blur severity.

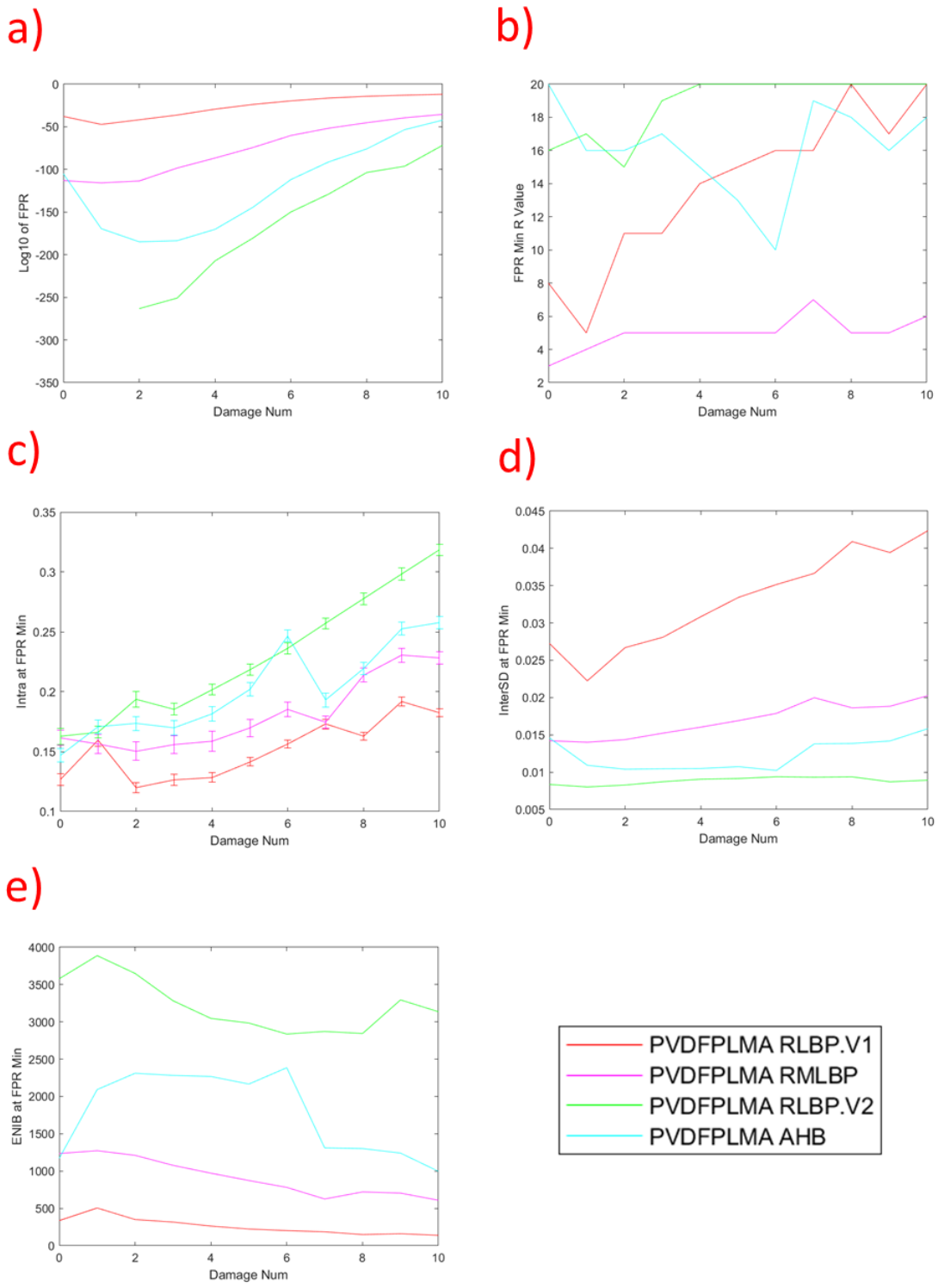

Figure 4.9: a) Graph of log_{10} of the minimum FPR achieved at each increment of increasing blur severity over all R for the PVDFPLMA quantum dot pattern. Missing data points occur when the generated FPR falls below the precision of MATLAB, 10^{-308}. b) Graph of the radius values R where the FPR minimum show in graph a) occurs at each increment of increasing blur severity. c) Graph of the intra hamming distance at the R value where the FPR minimum occurs at each increment of increasing blur severity. d) Graph of the inter hamming distance standard deviation at the R value where the FPR minimum occurs at each increment of increasing blur severity. e) Graph of the ENIB at the R value where the FPR minimum occurs at each increment of increasing blur severity.

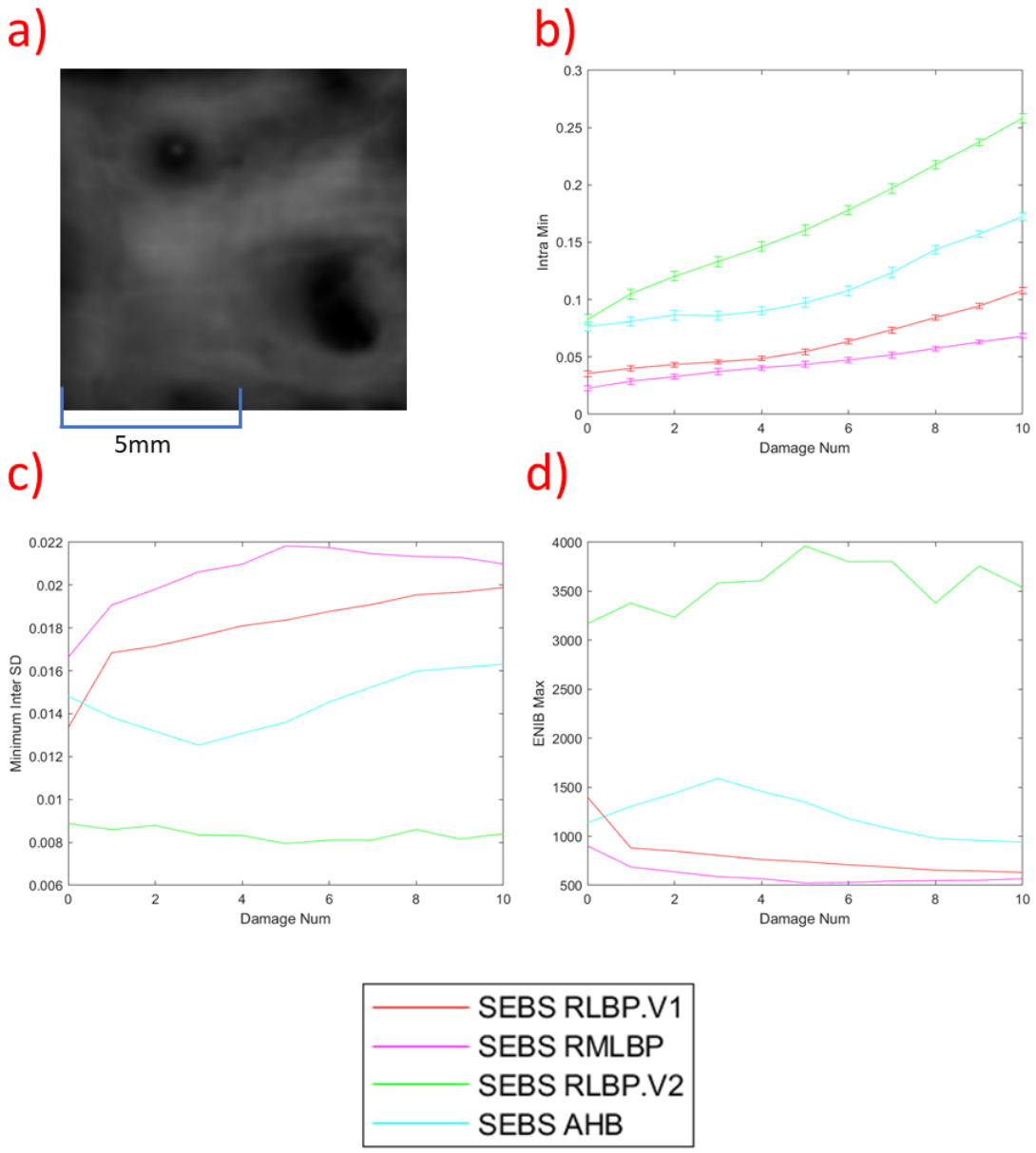

Figure 4.10: a) image of a quantum dot pattern made with InP dots in PVDFPLMA lacquer, the image was then blurred with a Gaussian filter with a standard deviation of 5. Taken with the system shown in figure 3.1. b) Graph of the minimum intra hamming distance achieved over all R at each increment of increasing blur severity. c) Graph of the minimum inter hamming distance standard deviation achieved over all R at each increment of increasing blur severity. d) Graph of the maximum ENIB achieved over all R at each increment of increasing blur severity.

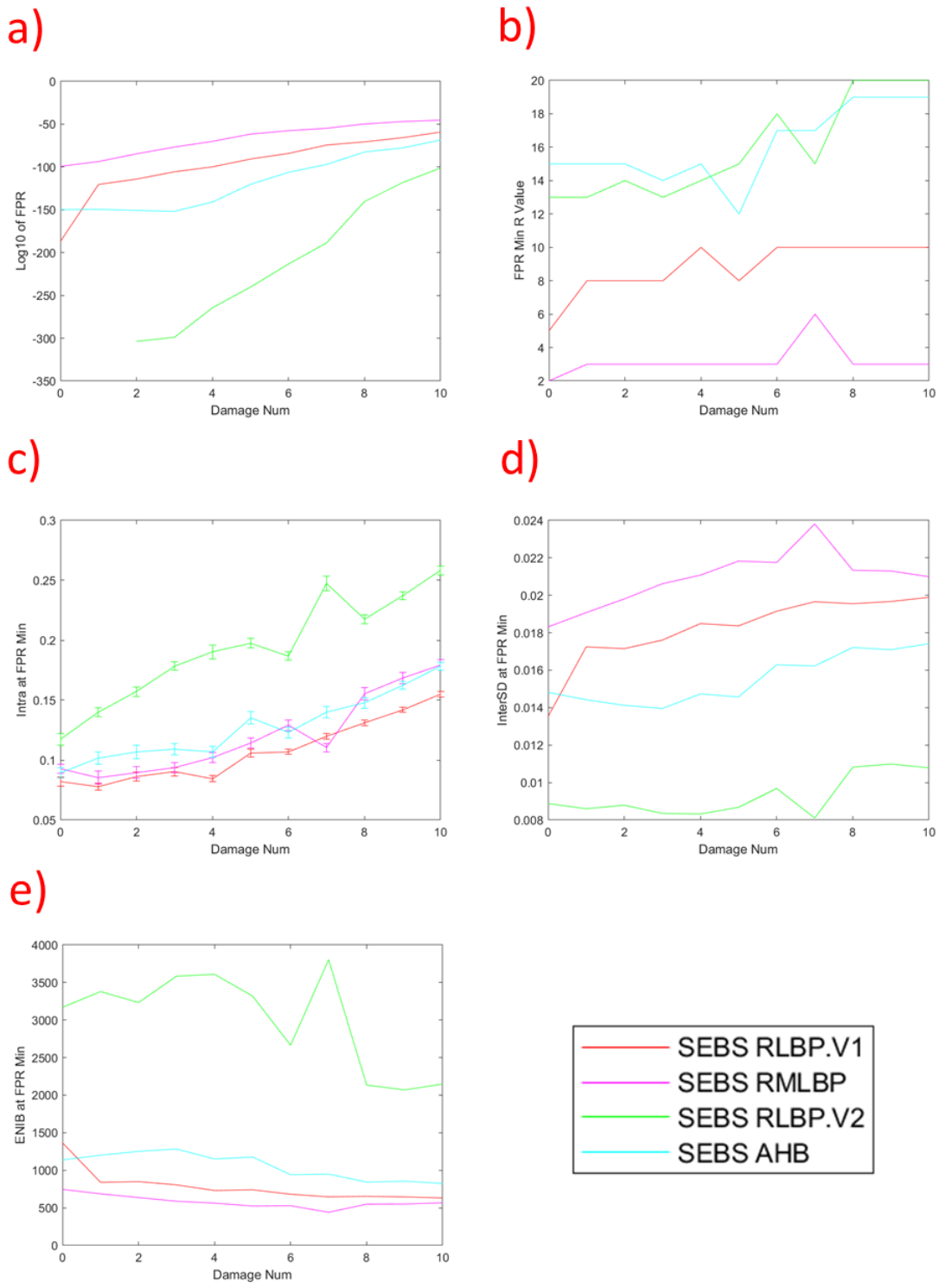

Figure 4.11: a) Graph of log_{10} of the minimum FPR achieved at each increment of increasing blur severity over all R for the SEBS quantum dot pattern. Missing data points occur when the generated FPR falls below the precision of MATLAB, 10^{-308}. b) Graph of the radius values R where the FPR minimum show in graph a) occurs at each increment of increasing blur severity. c) Graph of the intra hamming distance at the R value where the FPR minimum occurs at each increment of increasing blur severity. d) Graph of the inter hamming distance standard deviation at the R value where the FPR minimum occurs at each increment of increasing blur severity. e) Graph of the ENIB at the R value where the FPR minimum occurs at each increment of increasing blur severity.

As to be expected the contrast based schemes still produce the lower FPRs out of the two groups of fingerprinting algorithms. This can once again be traced to the standard deviation of their inter hamming distance at the FPR minima (figures 4.7c, 4.9c and 4.11c) the measures of uniqueness and entropy. RLBP.V2 for example almost always has the highest intra hamming distance values (both in intra minima and intra at FPR minima) but maintains the lowest FPR. This shows that in order to achieve an accurate authentication of a blurred image of a QD pattern the uniqueness of the pattern is more important than how close the damaged fingerprint is to the original. Logically this makes sense. The ability to tell two fingerprints apart due to them being unique will aid accurate authentication more. It is hypothesised however that there is an upper limit to how far this can be taken. Given the upward trend of the intra hamming distance as the severity of the blur is increased, eventually the damaged fingerprint will become too dissimilar to the original to be a match as it will start to overlap with the inter hamming distribution. It is at these more extreme cases where the other schemes would outperform RLBP.V2 in terms of FPR thanks to their lower intra hamming distance values. This could be potentially counteracted by increasing the range of R values that RLBP.V2 is tested at. As can be seen from figures 4.7b, 4.9b and 4.11b the R value at which the FPR minima occurs for RLBP.V2 consistently increases with increasing blur. Even flattening out at the maximum R of 20 for PVDFPLMA and SEBS. This shows that the scale at which RLBP.V2 is most accurate increases with the scale of structure made dominant by the smoothing. Something which is achievable by the fact that RLBP.V2s fingerprints lose their uniqueness at higher R much less than other algorithms (see the much lower increase in inter SD with increasing damage).

Of the two contrast based schemes AHB's FPR performance is the most interesting. Unique to AHB its FPR minima values initially improve as blur is increased before beginning increase themselves. Mathematically speaking this occurs because its inter hamming distance standard deviation initially decreases before either flattening out or rising. Physically speaking this is because a small amount of blur improves the uniqueness of the fingerprints that AHB produces. As touched on with RLBP.V2, to a degree, this is more important to accurate authentication using FPR than a close matching fingerprint. The origin of this lies in the fact that for all three of the QD patterns the ENIB increases blur standard deviation values where the FPR is improved (for example averaging over the QD patterns at a blur of 4 sees a 41.7% ENIB increase). This indicates that the blurring is causing the large uniform areas in the AHB fingerprint to break apart at low blur values. This does cause an increase in the intra hamming distance, which we would expect given the growing separation between the blurred and undamaged fingerprints. The significant increase in entropy however, more than accounts for this. The reasoning behind this improvement lies within the reduction of image contrast from the flattening of local brightness areas that occurs with blur. For undamaged images areas of similar brightness all are assigned the same value in the fingerprint (discussed in section 3.3.7). This is because they are similar to each other but distinct to neighbouring regions. See for example the large black area in the left of CISPMS in figure 4.2a and how it was fingerprinted. When blur is applied similar regions are no longer as distinct from their neighbours as such it is now more likely that a particular pixel will be assigned a different value in the fingerprint than that of its neighbours (see figure 4.5). Thus, breaking apart the large uniform regions. However, when the blur increases past a certain point we see the ENIB decrease and the inter hamming standard deviation increase. Indicating that

the blur is now creating larger uniform areas as its smoothing gets more severe. Thus, showing that both the contrast based schemes can produce accurate authentication at low blur values but both may suffer in performance as it increases.

The FPR minima trends of the gradient based schemes are similar to that of RLBP.V2 in that they increase with increasing applied blur. This is due not only to the increasing intra hamming distance at the FPR minima as the damage increases but the increasing inter standard deviation as well. The smoothing of the challenge image leads to small details being removed and as such large uniform areas are introduced in the fingerprint. As fingerprints with low entropy are an issue with gradient based schemes without any applied damage (see section 4.1.2) this only serves to compound this matter, leading to the gradient based schemes FPR minima performing worse than that of the contrast based schemes. Their lower intra hamming distances at their FPR minima however raises an interesting debate for use cases. It arises as the gradient based schemes are less affected by the presence, or lack thereof, of small details and features. If only a certain value of FPR is required for the use case, such as the 10^{-6} discussed in section 3.3.2 and both sets of schemes meet this requirement then the optimal to chose would then be the one with the lowest intra hamming at its FPR minima. Although the contrast based schemes may produce more accurate results their fingerprints are not as consistent as those for contrast based schemes. This would therefore provide a balance between a robustness and accuracy.

One other interesting feature of the FPR minima of the gradient based schemes is how the R value of the minima shifts with increasing damage. RLBP.V1 performs much as RLBP.V2 did with the R value of the minima increasing as the damage increases, shifting the focus of the fingerprinting to the larger scale features that are now dominant. RMLBP does not do this however. Its R value for the FPR minima flattens out with increasing damage at a value no higher than 7. It is due to this why RLBP.V1 displays a lower intra hamming distance at its FPR minimum. As RMLBP fingerprints lose their uniqueness at high R values in order to achieve its most accurate FPR some of the robustness of the algorithm is sacrificed. Although the intra that can be achieved by RMLBP outstrips that of the other algorithms, it's robustness comes as a double edged sword at the sacrifice of fingerprint uniqueness.

Stepping on from this point we can see that maximum achievable robustness of each of the algorithms is separated in a similar manner to the accuracy of authentication achievable. Figures 4.6b, 4.8b and 4.10b give this in the form of the minimum intra hamming distance achieved by each algorithm at each level of applied blur. Although CISPMS is less clear cut in each case the two gradient based schemes display lower intra minima than their contrast based counterparts. Within each group of algorithms the algorithm that takes in more data to create its fingerprint (AHB and RMLBP) consistently produces lower intra hamming values. Showing that in the case of blur the more data points used to create the fingerprint the more robust the algorithm will be. As uniqueness is not a consideration here the intra minimum almost exclusively occur at $R = 20$. Therefore, the gradient based schemes are more robust to the effects of blur as the orientation of gradients between points on an image is less susceptible to change than the absolute values of points. Especially given that smoothing will flatten out the values of these points but not effect gradient orientation.

How the intra minimum increases with increasing blur also raises interesting points on the development of fingerprint algorithms resistant to blur. Between the undamaged fingerprint and the maximally blurred fingerprint (Gaussian blur standard deviation of 10), RMLBP and AHB see the lowest average increase in intra minimum (given to three significant figures to reflect that of the intra hamming distance values) over all three QD patterns at 199% and 201% respectively. With RMLBP maintaining the lower absolute values. RLBP.V1 and RLBP.V2 give increases of 266% and 274%, with RLBP.V1 giving the lower absolute values. This is interesting to note as although RLBP.V1 gives lower intra minimum values than AHB at all R values, AHB sees a significantly lower increase as the blur applied increases. Suggesting that when designing a fingerprinting algorithm the top priority for minimising damage as blur increases is the number of data points taken in, rather than the exact method of converting the image to a fingerprint. Statistically this is a logical conclusion as the more data is used to calculate a value the more accurate it tends to be. The proximity of AHB's percentage increase to that of RMLBP supports this and suggests that RMLBP's robustness could be further improved by increasing the number of neighbour points used.

Even when not looking specifically at accuracy of authentication the robustness of the algorithm's comes at a cost. With the exception of CISPMS the gradient based algorithms consistently give higher inter hamming standard deviation minima and lower ENIB values, as shown in sub figures c and d in figures 4.6, 4.8 and 4.10. With CISPMS this is only clear cut between RLBP.V2 and the gradient schemes. The lower entropy fingerprints of the gradient schemes give them a greater degree of robustness as they allow for a greater chance of a pixel to match between the blurred and undamaged fingerprints. This is especially the case here where blurring removed granular features from fingerprints. From a cryptographic standpoint however this lower achievable uniqueness will mean gradient based fingerprints are less useful as secure cryptographic keys.

Which algorithm is optimal will depend entirely on the situation it is being applied in. If highly accurate authentication is needed but the expected blur that will occur on input images will remain low then RLBP.V2 would be optimal. However, given RLBP.V2 is the least robust, if accuracy was paramount but a higher degree of blur was expected then AHB would be a safer choice. In a scenario where a higher degree of accuracy wasn't as great an issue (such as where a maximum FPR limit is set), then RMLBP would be the better choice. It's robustness against the damage to fingerprint caused by blur is greater than all that of the others. Giving a greater degree of confidence that a matching fingerprint can be generated from a legitimate QD pattern, no matter the blur applied. RLBP.V1 does produce lower intra hamming distances when comparing FPR minima but if RMLBP is not restricted to its FPR min R value then this is not an issue. As well as this is the FPR minimum of RLBP.V1 is not consistently lower than that of RMLBP and thus, it gains no advantage there.

In reference to the figures of merit discussed in section 3.3.2 it is promising to note that none of the algorithms for any of the QD patterns fall above the required FPR threshold of 10^{-6} for any level of blur tested. Indicating that in broad terms they are all capable of being used as fingerprinting algorithms for the situation when the challenge image may suffer damage from blur. Only one of the algorithms also ever falls below the

required ENIB of 256bits, RLBP.V1 for PVDFPLMA at high blur values.

Finally there is the matter of how each different QD pattern behaved under differing levels of applied blur. Despite CISPMS possessing the lowest intra hamming distance and FPR in the undamaged dataset, with the application of blur it suffers the heaviest losses in terms of FPR minima and intra minima performance. The order of magnitude of CISPMS' FPR when averaged over all fingerprinting algorithms increases by 73% when comparing undamaged FPR to maximum applied blur, compared to the 68% of PVDFPLMA and the 61% of SEBS. Similarly CISPMS intra min when averaged other all algorithms increases by 430%, compared to 88% for PVDFPLMA and 190% for SEBS. This dramatic difference is due to the feature size in each case. The predominant features in CISPMS are the bright dots present on the QD pattern. SEBS does possess smaller features but is mostly dominated by gradual changes in brightness. PVDFPLMA is a similar story to SEBS albeit with less detail and lower contrast. When blur is applied the predominant features in CISPMS are smoothed out. Thus, removing the original information that would have been fingerprinted. This drastic change is the likely origin of the odd behaviour for AHB with CISPMS and the reason that many of the graphs show sporadic jumps or decreases. As the blur standard deviation increases the features that would have dominated are removed, leading to others dominating the texture. As shown from chapter 4.1 different features do fingerprint better or worse. For example the relatively flat PVDFPLMA consistently gave the highest intra hamming distance values, especially when compared to the discretely patterned CISPMS. In line with this SEBS and PVDFPLMA being dominated by larger scale features ensures that less information is lost when blur shifts the focus to larger scales as their features are already predominately at this scale. Overall the greater degree of variation in the quantum dot pattern of SEBS leads to better performance.

4.2.3 Noise Adding

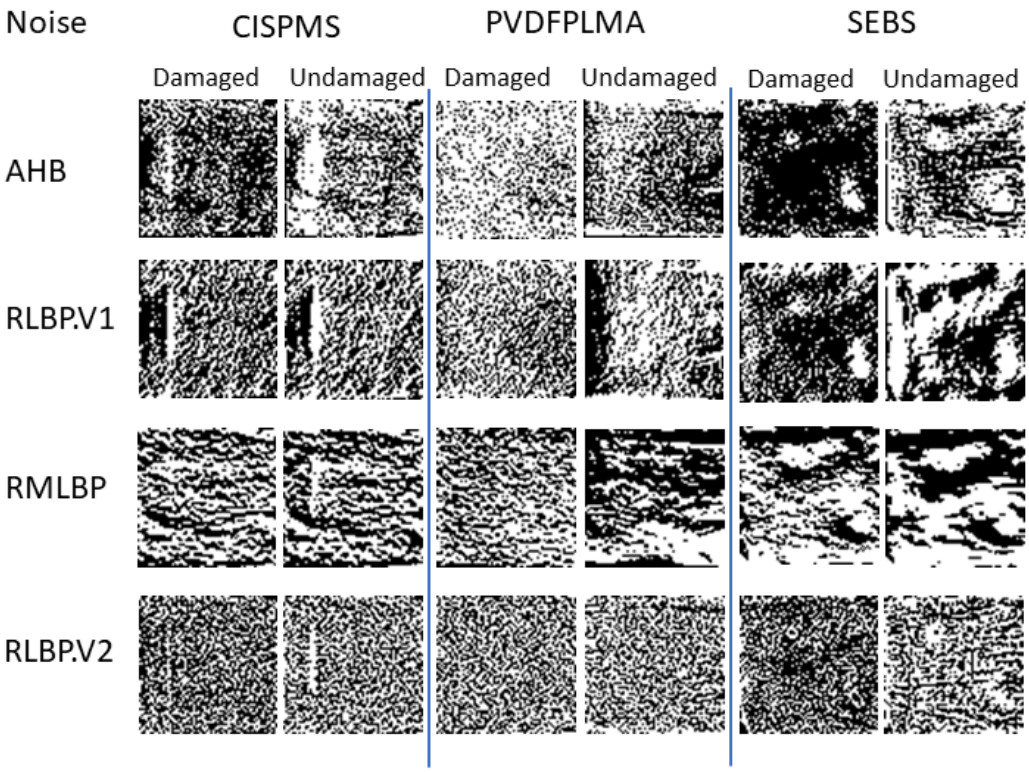

Figure 4.12: Table of example fingerprints generated for the noise section of robustness testing. Rows represent different fingerprinting techniques. Columns represent individual quantum dot patterns, with each column split into a fingerprint generated from a noise affected image on the left and an undamaged image on the right. Each fingerprint shown was generated at $R = 10$ and the level of noise was set to a variance of 0.5 as this is the midpoint of the noise severity available with the *imnoise* function, as discussed in section 4.2.1.

When observing the fingerprints in figure 4.12 we can see a very distinct difference to their undamaged counterparts and those in figure 4.5. With the exception of AHB the addition of noise has broken down larger uniform areas, as one would expect. In all cases CISPMS visually shows the least difference with the addition of noise, PVDFPLMA by far showing the most. As expected the presence of the distinct high contrast features in CISPMS makes its fingerprints more resistant to damage to the input image. The relative lack of features in PVDFPLMA making the noise the dominant factor in the fingerprinting. AHB is the exception as the addition of noise appears has caused a significant change in the white to black pixel bias of the fingerprints. Averaging over all three quantum dot patterns AHB showed a change of 27.9% in bias (as opposed to for example 6.1% change for RMLBP). A factor that will affect the inter hamming standard deviation of AHB and thus, its FPR.

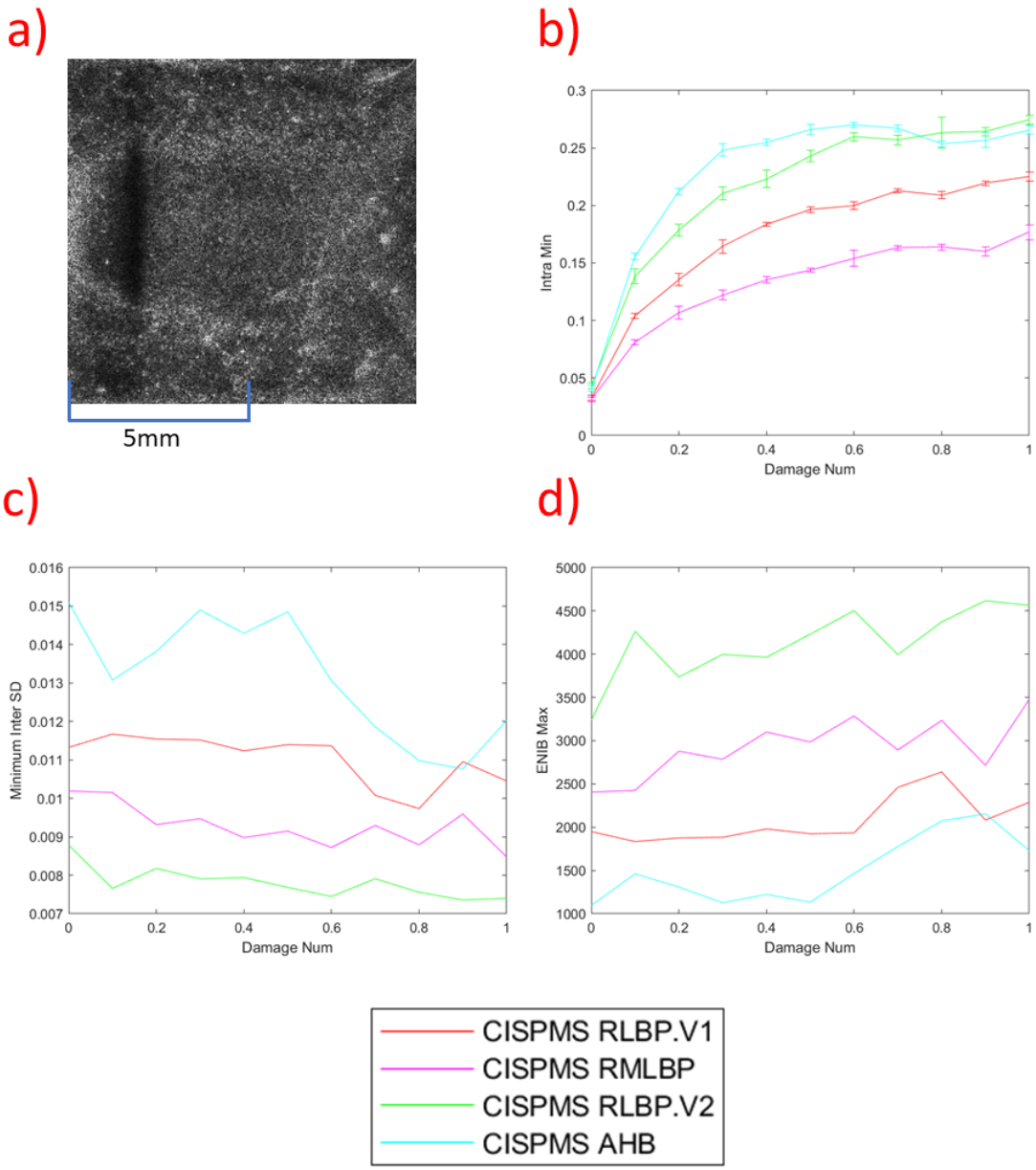

Figure 4.13: a) image of a quantum dot pattern made with CIS620 dots in PMS lacquer, noise was then added to the images with a variance value of 0.5. Taken with the system shown in figure 3.1. b) Graph of the minimum intra hamming distance achieved over all R at each increment of noise severity. c) Graph of the minimum inter hamming distance standard deviation achieved over all R at each increment of noise severity. d) Graph of the maximum ENIB achieved over all R at each increment of noise severity.

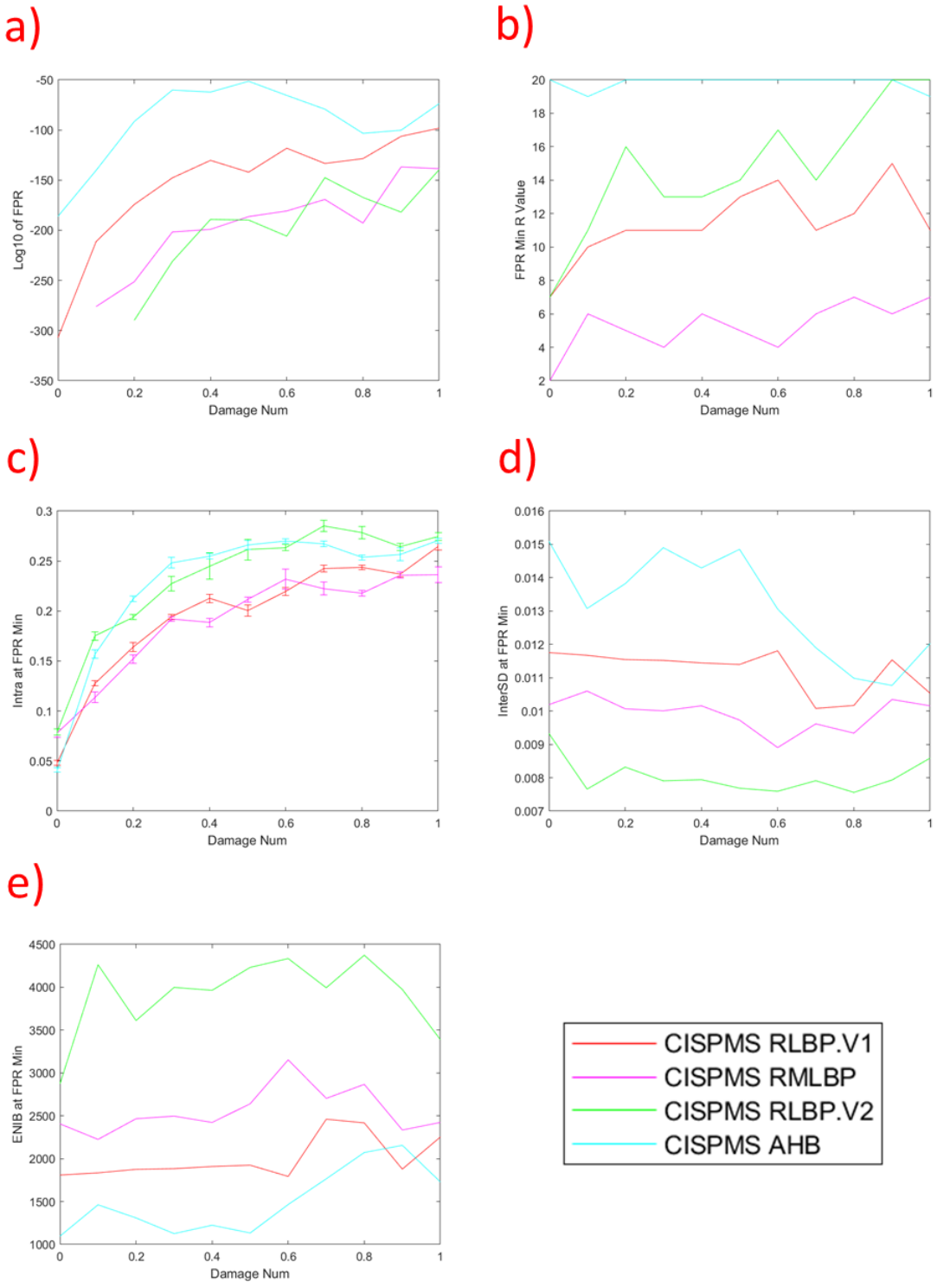

Figure 4.14: a) Graph of log_{10} of the minimum FPR achieved at each increment of noise severity over all R for the CISPMS quantum dot pattern. Missing data points occur when the generated FPR falls below the precision of MATLAB, 10^{-308}. b) Graph of the radius values R where the FPR minimum show in graph a) occurs at each increment of noise severity. c) Graph of the intra hamming distance at the R value where the FPR minimum occurs at each increment of noise severity. d) Graph of the inter hamming distance standard deviation at the R value where the FPR minimum occurs at each increment of noise severity. e) Graph of the ENIB at the R value where the FPR minimum occurs at each increment of noise severity.

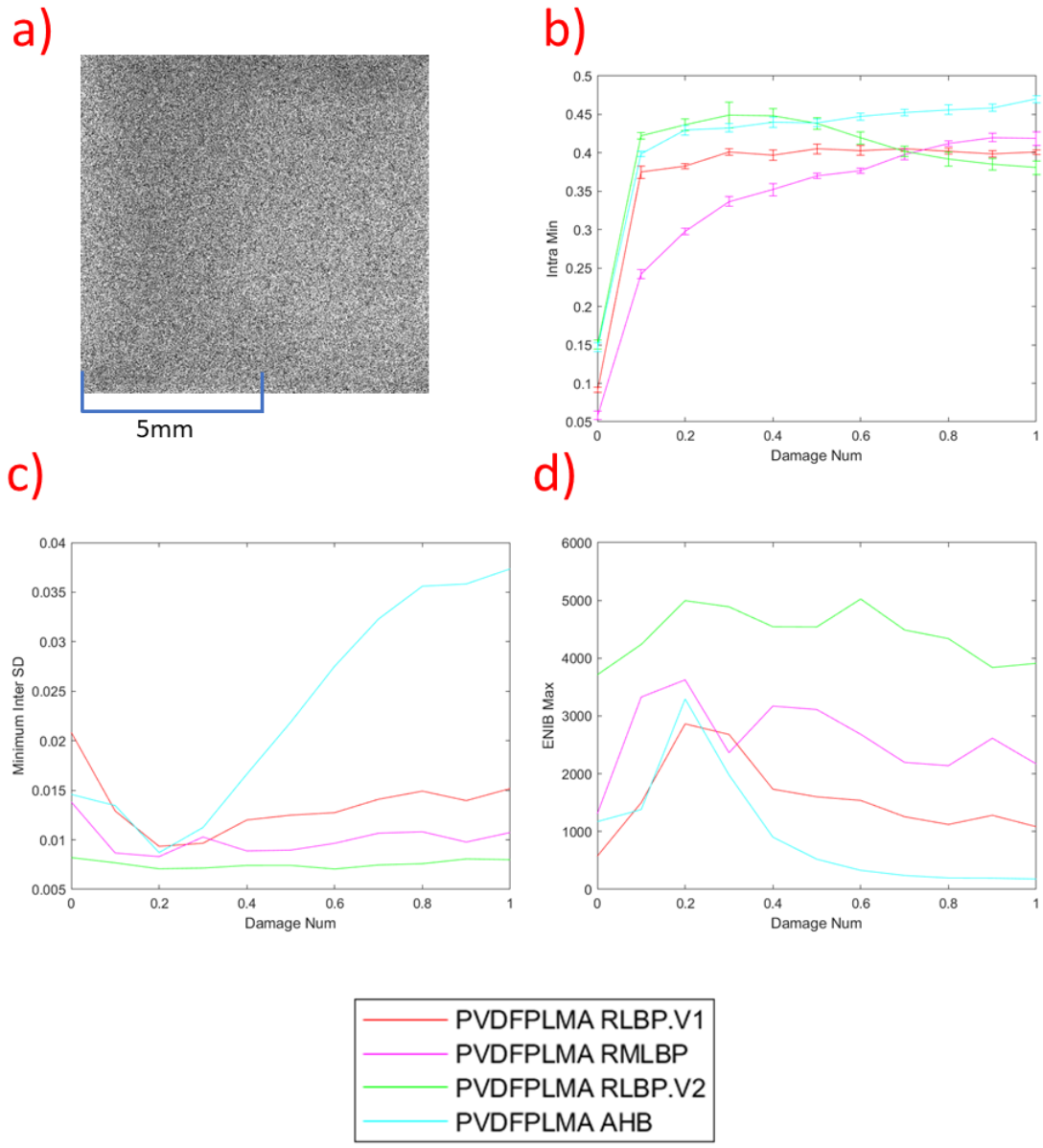

Figure 4.15: a) image of a quantum dot pattern made with InP dots in PVDFPLMA lacquer, noise was then added to the images with a variance value of 0.5. Taken with the system shown in figure 3.1. b) Graph of the minimum intra hamming distance achieved over all R at each increment of noise severity. c) Graph of the minimum inter hamming distance standard deviation achieved over all R at each increment of noise severity. d) Graph of the maximum ENIB achieved over all R at each increment of noise severity.

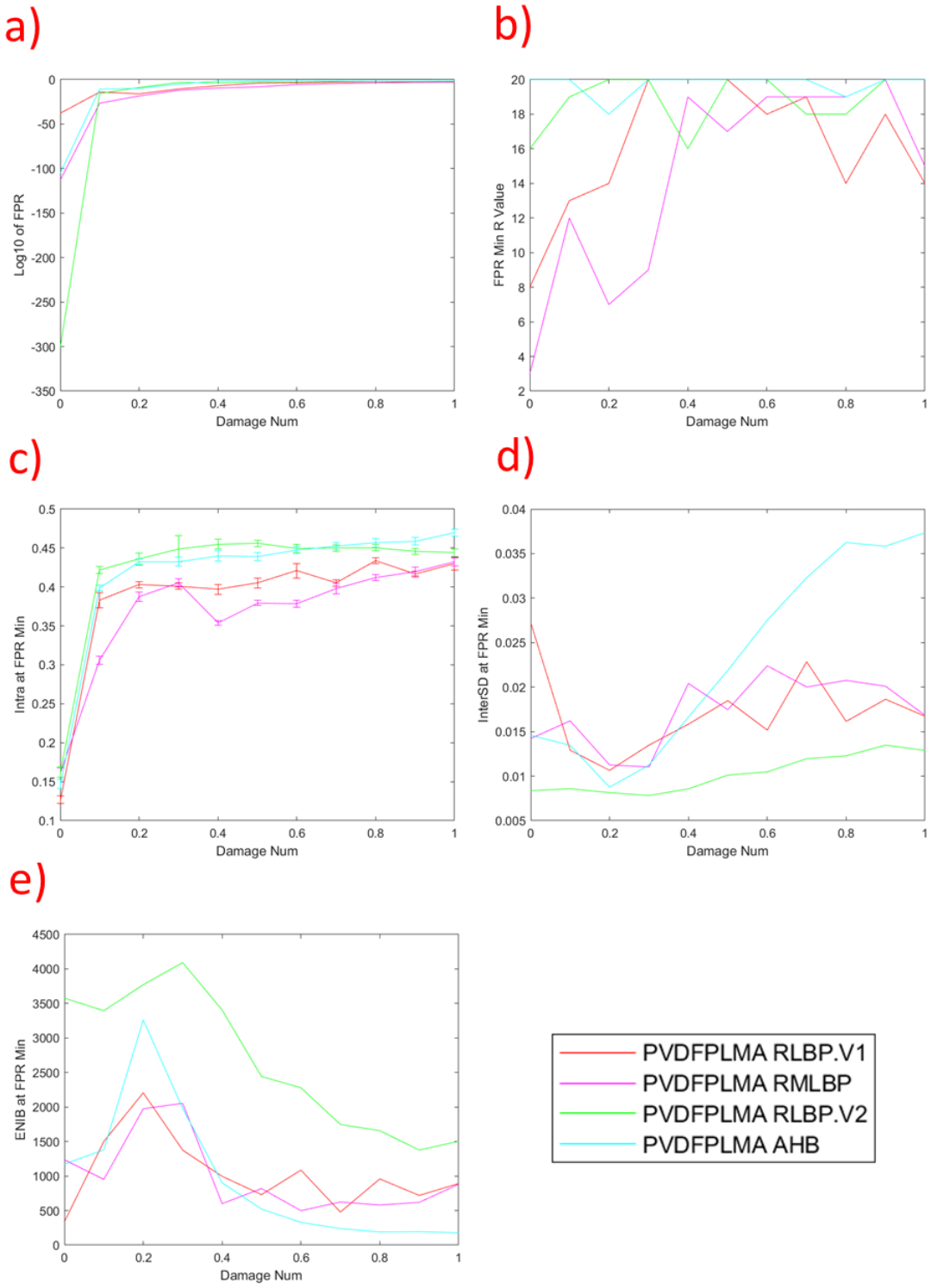

Figure 4.16: a) Graph of log_{10} of the minimum FPR achieved at each increment of noise severity over all R for the PVDFPLMA quantum dot pattern. Missing data points occur when the generated FPR falls below the precision of MATLAB, 10^{-308}. b) Graph of the radius values R where the FPR minimum show in graph a) occurs at each increment of noise severity. c) Graph of the intra hamming distance at the R value where the FPR minimum occurs at each increment of noise severity. d) Graph of the inter hamming distance standard deviation at the R value where the FPR minimum occurs at each increment of noise severity. e) Graph of the ENIB at the R value where the FPR minimum occurs at each increment of noise severity.

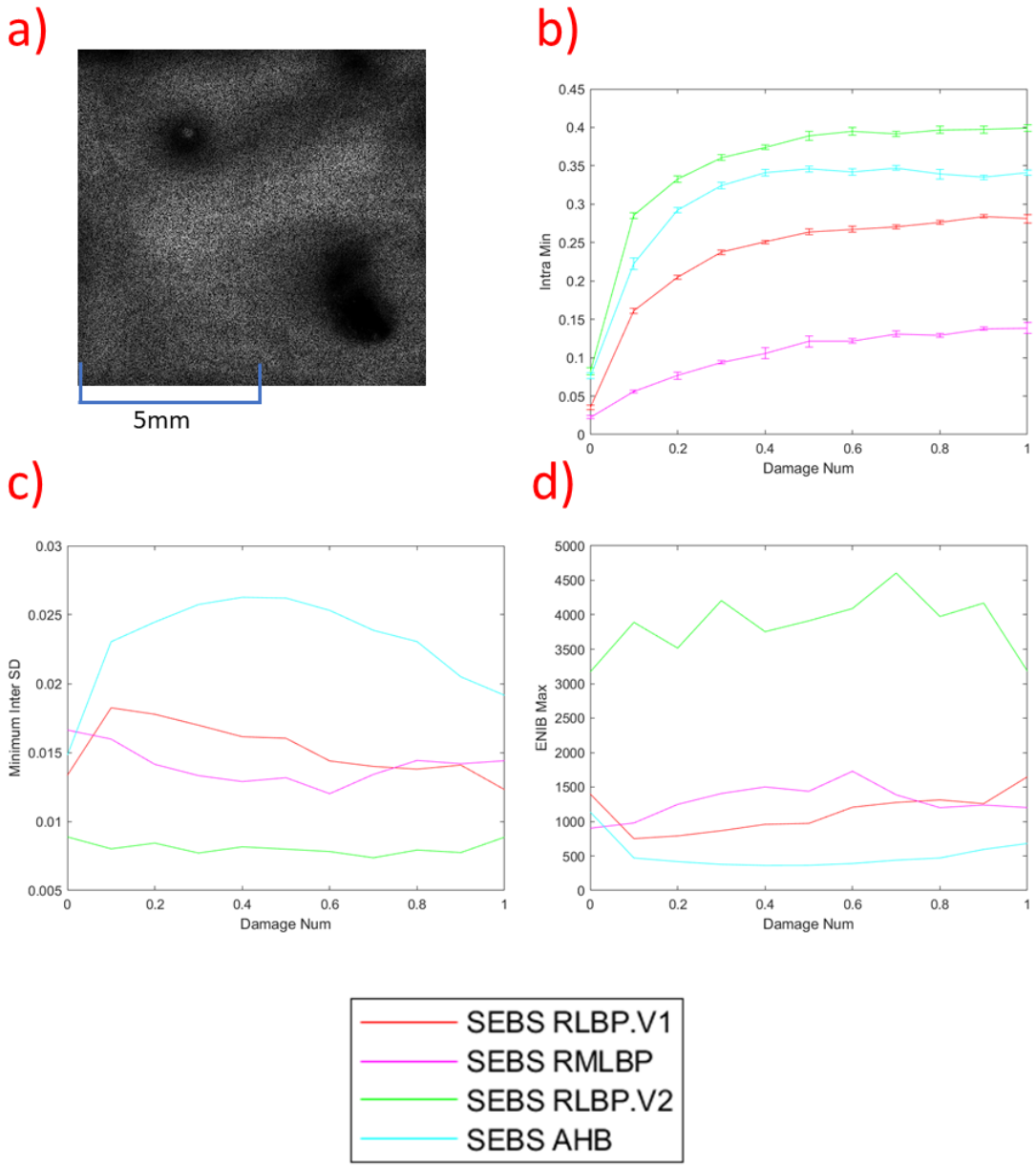

Figure 4.17: a) image of a quantum dot pattern made with InP dots in PVDFPLMA lacquer, noise was then added to the images with a variance value of 0.5. Taken with the system shown in figure 3.1. b) Graph of the minimum intra hamming distance achieved over all R at each increment of noise severity. c) Graph of the minimum inter hamming distance standard deviation achieved over all R at each increment of noise severity. d) Graph of the maximum ENIB achieved over all R at each increment of noise severity.

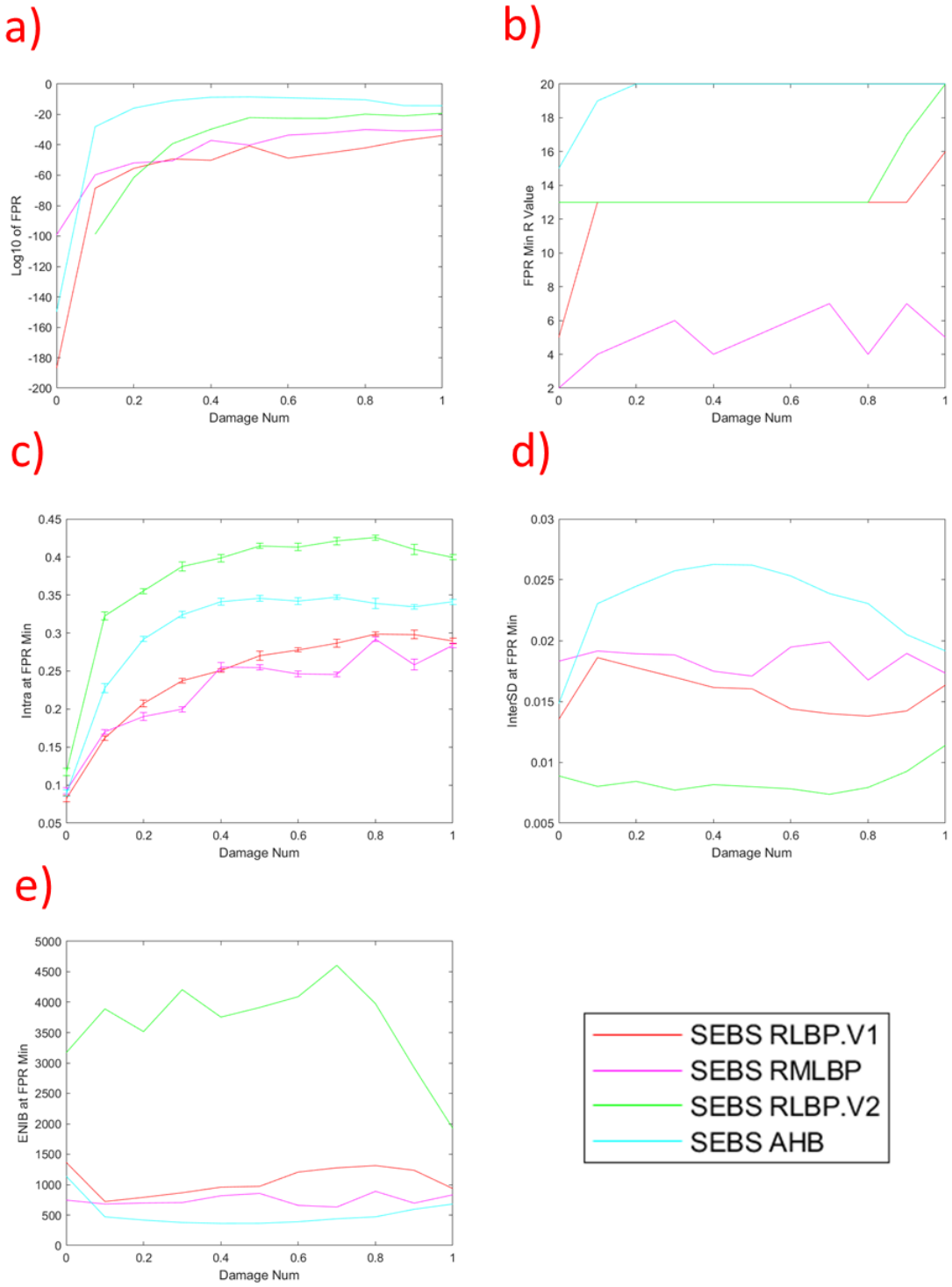

Figure 4.18: a) Graph of log_{10} of the minimum FPR achieved at each increment of noise severity over all R for the SEBS quantum dot pattern. Missing data points occur when the generated FPR falls below the precision of MATLAB, 10^{-308}. b) Graph of the radius values R where the FPR minimum show in graph a) occurs at each increment of noise severity. c) Graph of the intra hamming distance at the R value where the FPR minimum occurs at each increment of noise severity. d) Graph of the inter hamming distance standard deviation at the R value where the FPR minimum occurs at each increment of noise severity. e) Graph of the ENIB at the R value where the FPR minimum occurs at each increment of noise severity.

Noise is a prevalent issue in image capture, every capture device suffers from it. As such when expanding the fingerprinting algorithms to use on more noisy systems than the controlled environment detailed in figure 3.1 a key consideration will be the generation of repeatable fingerprints from noisy images. This is of course best encapsulated by the intra hamming distances in sub figure b of figures 4.13, 4.15 and 4.17. As already discussed the gradient based schemes produce lower intra minima when no damage is applied than their contrast based counterparts. This remains so as the applied noise level is increased. With RLBP.V2 and AHB showing similar sized increases in intra hamming min of 0.279 and 0.271 respectively. RMLBP achieves the lowest increase by a fair margin at 0.207 with RLBP.V1 at 0.249. This shows us that the gradient based schemes are more resistant to the effects of noise in the input image. This will have arisen due to their usage of differences in pixel values rather than absolute values, the direction of gradients is far less affected by noise after all. RMLBP has given significantly better results than the others for two key reasons. For the first, it has improved upon RLBP.V1 owing to the fact that it takes in significantly more data points to produce a single fingerprint value. The extra averaging step resulting in greater robustness to noise. On top of this RMLBP is the only one of the schemes that does not use the central pixel in generating the binary string for the fingerprint bit (including AHB as this compares every pixel to the central pixel). Thus, if the central pixel is noisy it will only affect 1 bit out of the 17-bit binary string of RMLBP. For every other algorithm a noisy central pixel will affect every bit of the string (or kernel). This is further consolidated by the average intra hamming minimum of RMLBP at the highest level of noise tested (a variance of 1) being at 0.245. In comparison the next lowest was RLBP.V1 at 0.302, followed by AHB at 0.359 and RLBP.V2 at 0.372. Thus, on average, RMLBP even at the highest noise levels, produces fingerprints over 12% more similar to if there was no noise at all than RLBP.V2. A point of interest to note however is that unlike the equivalent for the blur damage testing the intra minimum graphs appear to be following a logarithmic curve. Perhaps suggesting a asymptotic value of intra hamming distance they are tending towards. A fact which may allow for the determination of the maximum degree of noise that an algorithm can sustain.

For further discussion and comparison of the algorithms in regards to other figures of merit we must first address AHB's shift in black/white pixel bias with the application of noise. The addition of noise has caused the bias to shift from the maximal entropy case of a 50/50 split of black and white towards one or the other dominating the fingerprint.As it is a contrast based fingerprinting algorithm the sensitivity to the effects of noise is not unexpected as RLBP.V2 also displays this. It is true however, that one would expect the sensitivity to noise to shift the bias closer to the perfect case of an equal split. Thus, making the behaviour of AHB so odd. The changing magnitude of the difference from this optimal value traces a similar path to the changing inter hamming standard deviation. Indicating an increase in larger uniform areas and thus, a decrease in entropy (this can be seen visually in figure 4.12). This effect is not present in the other algorithm's fingerprints and is the origin of the anomalous behaviour of AHB's inter hamming standard deviation (see sub figure d in figures 4.13, 4.15 and 4.17). This effect causes the FPR minimum, and so accuracy of authentication, of AHB to be consistently the highest with all damage values. The exact origin of this behaviour is unknown. Given the difference between the behaviour of AHB with the algorithms that can trace their heritage back to LBP in some way, it is hypothesised that it arises from AHB including every pixel within its perimeter within it's calculation of the final fingerprint bit.

The FPRs shown in figures 4.14a, 4.16a and 4.18a highlight a situation in which the entropy of the fingerprint is less important than its repeatability for accurate authentication. As expected, with increasing damage the minimum achievable FPR also increases. In all cases the major contributor to this is the increasing intra hamming separation between damaged and undamaged fingerprints. With the exception of AHB none of the inter hamming distance standard deviations indicate a significant degree of net change over the noise variance range. Highlighting that it is in fact the intra hamming distance that is dominating here. As can be expected from previous results figures 4.13 to 4.18 show that for the contrast based schemes (excluding AHB for reasons previously discussed) the inter hamming standard deviation remains lower and ENIB higher than that of the gradient based schemes. For noise damage however, the FPR of contrast based schemes is no longer consistently lower than that of gradient based. This suggests that there is a limit to how high the intra hamming distance of the algorithms can get before a higher uniqueness can no longer compensate and the authentication accuracy suffers. As such with noisy capture equipment the contrast based schemes will suffer in regards to authentication despite them outperforming their counterparts by a wide margin with more stable equipment. A final point of interest is that similarly to the intra hamming minima, the FPR minima also tend towards an asymptote with increasing noise, indicating a degree of noise where the FPR will no longer worsen.

The R value at which the FPR minima occurs reveals information on how the algorithms handle increasing noise. In all cases apart from AHB we see an overall net increase in the R value that the FPR minima occurs at. AHB remains almost constantly at the maximum possible value of 20. This indicates that in order to achieve the lowest possible combination of intra hamming distance and inter hamming standard deviation the algorithms are requiring to shift focus to larger and larger scale patterns to reduces the effect of the noise. Figure 4.16b being a clear example of this. AHB's requirement for taking in larger data sets to minimise its intra hamming distance is highlighted clearly as undoubtedly with a larger R range it would find its minimum FPR at a higher R value. This highlights a downside of AHB as larger datasets require more processing time despite not showing appreciable improvements in figures of merit over other the algorithms. It is also important to note that despite intra hamming distances decreasing with increasing R (see figures 4.2 to 4.4) the gradient based schemes display lower intra hamming distances at their FPR minimum. Given the lack of clear improvement in contrast based algorithm FPR minimum with damage greater than zero this would suggest gradient based schemes to be the optimal choice.

In two out of the three tags analysed (CISPMS and SEBS) all of the algorithms meet all of the requirements for figures of merit set out in section 3.3.2 for all tested noise values. CISPMS gives the lowest intra hamming distances and FPR minima. This suggests that the best type of quantum dot texture for accurate authentication, as well as, generating repeatable fingerprints is one with a high level of contrast and discrete features. Logically this makes sense as they allow for the features to be more readily picked out within the noise. PVDFPLMA however highlights an issue with noise and the generation of fingerprints. A uniform pattern lacks the variation in brightness topography for any features to not be smeared out by noise. Each algorithm fails the maximum allowed FPR requirement, RMLBP and RLBP.V1 failed at 0.7 and 0.5 noise variance respectively whereas

AHB and RLBP.V2 failed at 0.4 and 0.3 respectively. Once again bringing focus to the main conclusion of this section. The contrast based schemes show the least robustness against noise. To the degree that it causes the accuracy of their authentication to suffer as a result. RMLBP handles noise the best providing both fingerprints that are the closest to their undamaged counterparts and FPR minima close or better than the contrast based schemes.

4.3 Concluding Remarks

In this chapter it has been demonstrated that it is indeed possible to extract digital fingerprints from QD-PUFs. When authenticating these fingerprints two major factors come into play in regards to the accuracy of authentication, these are the repeatability of the fingerprints (intra hamming distance) and the uniqueness of the fingerprints (inter hamming standard deviation). When the intra hamming distance is low enough the uniqueness of the fingerprints dominates the accuracy of authentication. When the intra hamming distance passes a certain threshold however, accurate authentication is no longer possible even with a high degree of uniqueness. When the upper bound of the intra hamming distribution and the lower bound of the inter distribution start to overlap FPR increases significantly. Examples of this can be seen in figures 4.3c and 4.4c at low R for RLBP.V2. In other words the fingerprints of the same tag must be sufficiently similar to each other before other factors are considered. The determination of this threshold and its dependence of QD-PUF type, algorithm, radius and damage would make for interesting further work.

The trade off that arises in regards to the four algorithms tested (RLBP.V1, RLBP.V2, RMLBP and AHB) is that they produce fingerprints with a high degree of uniqueness or fingerprints that are highly repeatable. The gradient based schemes encode the direction of gradients within the input image which do not change to significant enough degree to give neighbouring pixels different bit values. Thus, they are highly resistant to small scale changes and noise. Giving them a low intra hamming distance. This does however mean they produce fingerprints with large uniform areas with little to no change in them. Thus, limiting their uniqueness.

On the other hand, the contrast based schemes produce lower false positive rates when applied to undamaged images of QD-PUFs. It has also been indicated that such schemes produce fingerprints with a higher level of entropy than their gradient based counterparts. Comparing the value of the central pixel to the immediate surrounding area is much more dependent on the effects of noise and small scale local features. RLBP.V2 being the exemplar of this, as it compares every pixel on its perimeter to the central pixel. Thus, preventing the formation of the large uniform areas and improving fingerprint uniqueness at the cost of repeatability. It should be noted however that the lower intra hamming distance of RMLBP means that its uniqueness can be improved through methods such as XOR de-biasing (see chapter 5). The repeatability is more limited into how it can be improved.

Despite the promise the contrast based schemes show when applied to undamaged QD-PUF images they suffer the most when damage is applied to the input images. The value

of the perimeter pixels is much more likely to change under noise than the direction of the local brightness gradient. RLBP.V2 suffers the most here, its encoding method may allow a high degree of uniqueness but it also compounds the effects of noise. Similarly the contrast based schemes are most affected by the application of blur to the input image. As it smooths out much of the small scale features they are dependant on. Something that the gradient based schemes are not affected by. Thus, the gradient based schemes show the most robustness against both applied blur and noise, their produced fingerprints being closest to their undamaged counterparts. RMLBP's higher number of neighbour points and limited use of the central pixel making it stand out as the most resistant to the effects of noise.

In regards to accuracy of authentication when considering the effects of damage the discussion is less clear cut. With the application of blur RLBP.V2 still produced the lowest FPR owing to its fingerprints high degree of uniqueness. With the application of noise however, the contrast based schemes produced fingerprints with a low enough repeatability that accurate authentication was hampered. Something the gradient based schemes did not suffer as badly from.

The type of QD-PUF used also has an effect on the results obtained. QD-PUF patterns with a higher contrast over the image and discrete clear features allow for lower FPRs and a greater resistance to noise. These same tags however suffer the most with the application of blur, as it easily smears out the once clear features. Tags with a "uniform" pattern that lack any significant variation in brightness topography produce the highest FPRs, their lack of features leading to being more greatly affected by noise and producing more blocky fingerprints. The optimum QD-PUF pattern for use in fingerprinting would therefore be one with larger discrete features than CISPMS and a high degree of contrast.

In terms of optimal use cases we see two distinct categories. If the QD-PUF imaging process will take place in a controlled environment with optimised parameters (noise, exposure, etc) then RLBP.V2 is the best candidate. In its vanilla form it generates the most unique fingerprints with the highest degree of randomness (if de-biasing is not used). The use of specialised equipment would balance out it's lack of robustness to any damage, whereas its uniqueness grants a higher degree of security. Such an example might be using a QD-PUF on a passport in order to determine its authenticity in an airport. On the opposite end of the spectrum is RMLBP which is more suited to public use applications that require the use of non-specialised equipment (such as smartphones) and a lessened security concern. The extra robustness of the algorithm means that it is best suited to dealing with the sub-optimal conditions (such as lower quality imaging apparatus, uncontrolled ambient lighting and user errors) it may find itself used in. For applications such as anti-counterfeiting of luxury items or medication the lessened uniqueness is less of a concern. For matters where the security is a greater concern and the environment can be better controlled (such as dedicated scanning devices in warehouses) XOR de-biasing (see section 5.2) may be used to address this concern.

Chapter 5

NIST Randomness Testing and XOR Debiasing

When discussing matters of authentication it is important to consider factors that may aid an attacker in determining information that would aid them. Although the simulation attack prevention discussed in section 2.2.3 prevents the possibility of a forgery it is still important to limit the information that any not authorised party has of a particular QD-PUF token. As well as this, the uniqueness of each QD-PUF makes creating a replica at the least a fruitless endeavour if not impossible given the effort required. Although at the moment we believe such systems can not be broken it is prudent to still ensure optimal security at all stages within the process. The particular weak link in the authentication process is not the physical QD-PUFs themselves but instead the cryptographic part of the process and the fingerprints themselves.

As described within this chapter the fingerprints bear no encryption of any kind. Given that the fingerprinting algorithms encode structural information of the QD-PUF image it is hypothesised that it may be possible to replicate the original image from a fingerprint. Such a process will likely require the usage of machine learning algorithms and is beyond the scope of this discussion. Such matters are however, well documented[49]. For example Ruhrmair et al[50] successfully attacked five different kinds of electronic PUF using machine learning algorithms. The complexity of PUFs often acts as their strongest defence. Computational processing power is frequently not great enough to attack a PUF successfully using machine learning within the time frame required for an attack to be worthwhile (i.e. within the lifetime of the item the QD-PUF is associated with). This could be a point that sets this matter to rest given the complexity of the QD-PUFs. If not for the fact that it has been demonstrated that machine learning attacks can be enhanced when used in hybrid with other techniques[51]. Thus, there is a very strong case for machine learning being a threat to QD-PUFs, a matter which needs to be addressed.

Although the resizing step within the fingerprint generation process does destroy fine grain information it may not be sufficient to protect against such attacks. This is not the only source of potential information leakage within the fingerprints. As discussed previously the algorithms can lack in entropy, especially at high radii and most notably for the gradient based schemes. As well as this many produced fingerprints lack a white/black pixel bias that is close to a perfectly equal split. Both of these are known as information or entropy leakage[52].

In an optimal situation each bit in the fingerprint is independent of any other, namely the fingerprint is completely random. This means that for a brute force approach to replicate a fingerprint an attacker has at best a 50% chance to correctly guess any bit. When scaled up to the every bit in the 4096 bit fingerprint this gives the attacker the infinitesimally small probability of success of 1 in 10^{1234}. With entropy leakage however at attacker has supplementary information to better guess a bits value and so can drastically reduce these odds[52].

Entropy leakage poses a great issue therefore when considering the usage of fingerprints generated from QD-PUFs in situations outside of a laboratory setting (a problem that has been discussed before for matters such as biometric data[52], but never QD-PUFs). The QD-PUFs themselves are underpinned by the principles of quantum mechanics but the fingerprints themselves may form a weak link in the chain when it comes to cryptographic security. Although the simulation attack prevention discussed in section 2.2.3 may prevent such matters from ever being a concern it is prudent to ensure that every possible avenue of attack is addressed. As such this chapter discusses these issues in greater detail and explores method to solve them in order to provide a complete picture of the security of a QD-PUF authentication process. In order to counteract both the entropy leakage and the potential to replicate the QD-PUF image from the fingerprint we can use post processing methods such as the XOR debiasing discussed in this chapter. This not only destroys structural information in the fingerprint but improves upon the bias of it as well, as shown in section 5.3. Although other techniques do exist that perform debiasing for other types of binary strings[53] this is the first time one has been created that can be applied to fingerprints from QD-PUFs.

5.1 NIST Randomness Test Suite

There are a infinite number of statistical tests that can be used to determine if a string of bits is random or not. The NIST Randomness Test Suite sets out 15 different tests designed to minimise the possibility of a false positive result (type 2 error)[54]. The tests also focus on determining uniformity of the bit string, the scalability of a sequence (whether or not conclusions drawn about the string as a whole can be applied to subsections) and the consistency of the random number generator that produced the string. In this case we will be using our QD-PUFs as a random number generator (RNG) and the fingerprint as the bit string generated from them. Such a series of tests had been performed by Kim et al[30] in the analysis of bit strings generated from their silk PUFs, demonstrating their usefulness in this matter. They have never been applied to QD-PUF fingerprints however. Each test compares the input bit string to an ideally random string for the type of randomness being tested for. Whether or not the input string is random is then determined to a chosen degree of confidence, as per the documentation a confidence of 99% was chosen.

Six of the tests were chosen to be applied to the fingerprints. The reasons why they were chosen are detailed next to their summaries below. Those that were not chosen were not applicable to the fingerprints. The numbering of the tests is kept consistent with that in the official documentation[54].

- Test 1: Frequency (monobit) test. Checks if the bias of the string as a whole is close to the optimal 50/50 split of 1's and 0's (or white and black pixels for a fingerprint). Alongside test 2 below, was chosen to observe the presence of entropy leakage through bias.
- Test 2: Frequency test within a block. Breaks down the string into blocks and analyses the bias within each block. This tests the scalability of the string, even if the global bias is optimal subsections of the string may show heavy bias.
- Test 3: Runs test. This tests for the number of 'runs' within a string of bits. A run is a continual unbroken chain of the same value bit. Optimally a high number of runs is wanted. A low amount would indicate a fingerprint with large uniform areas. Something we have seen in the gradient based schemes.
- Test 6: Discrete Fourier transform test. Applies a discrete Fourier transform to the string in order to observe the presence of periodic patterns and determine is these deviate from the optimum. Chosen as periodic patterns would provide a great degree of information to an attacker, these can occur due to printing artefacts in some QD-PUF creation methods.
- Test 11: Serial test. Determines the frequency of all overlapping m-bit patterns within the string. Periodic or otherwise. For a perfectly random string all patterns should have a equal frequency of occurring. This is of particular interest as the fingerprinting algorithms have certain patterns that are more frequent than others, such as those representing an edge or corner within the image.
- Test 12: Approximate entropy test. Compares the frequency of all overlapping blocks of patterns of consecutive lengths (m and $m+1$) to that of an ideally random string. Useful as a comparison of the entropy of the fingerprints.

To perform the testing an (undamaged) fingerprint at a chosen radius is separated into its individual rows. These rows are then concatenated together in order (the end of row 1 attached to the start of row 2 etc...) to form a 1x4096bit long string. The reduction of dimensions is not a concern as many of the tests are dimensionless. For those that are not, the concern is lifted as if the fingerprint is not random across one dimension it will not be across two.

The string is then subject to each of the tests detailed above. From which it is determined if the string is random according to that test at that radius. 48 fingerprints, each from different QD-PUFs (as discussed in section 3.1), were tested in total at radii from 1 to 20 inclusive. A success rate was determined for each radius by calculating the percentage of fingerprints that passed that particular test. Only RMLBP and RLBP.V2 have been analysed in this section as they display the highest and lowest inter hamming standard deviation (as such the highest and lowest entropy in the fingerprints they produce) respectively.

5.2 XOR de-biasing

As discussed in the beginning of this section there are three key areas of information leakage within fingerprints generated from QD-PUFs. Structural information of the QD-PUF

encoded in the fingerprint, issues surrounding non-optimal bias and a lack of entropy or the presence of large uniform areas within fingerprints. With noiseless cryptographic keys one could use a method such as a hash function[55] in order to correct for this. This is because such a method would map a non-uniformly random string to a uniformly random one. QD-PUF fingerprints (as well as other types of fingerprints) are however too noisy for such a method to be applied. Fuzzy extraction schemes likewise can remove non-uniform entropy but also require helper data[56], something that is not appropriate in this application.

This subsection details a process using the XOR operation to destroy structural information within a fingerprint as well as debias it. Although other de-biasing algorithms such as Von Neumann de-biasing[57] do exist they are not appropriate in this case as they are commonly used in conjunction with a random number generator for encoding a PUFs response. The XOR function however, is well known to debias binary strings and has no information leakage[58], without the need for helper data.

The XOR operation is a logic gate operation commonly used in programming. It takes in two separate bits as its input and outputs a single bit dependant on the input. This output bit will have a value of 1 if the input bits were different values or a value of 0 if they were the same. As such an output of 1 or 0 from an XOR operation has two possible inputs it could have come from (0,1 or 1,0 and 1,1 or 0,0 respectively) with no indication of which it may be. This gives a maximum probability to correctly chose the input combination of 50%. It is because of this property that an XOR operation can take in two biased input strings and will produce a de-biased output as both the possible bits from the XOR operation have an equal probability of occurring. Secondly the XOR operation is the only binary operation that does not leak information[58], hence why it is used in digital ciphers. When taken in tandem with the fact that no helper data is required these properties make the XOR operation highly suitable for use in debiasing QD-PUF fingerprints.

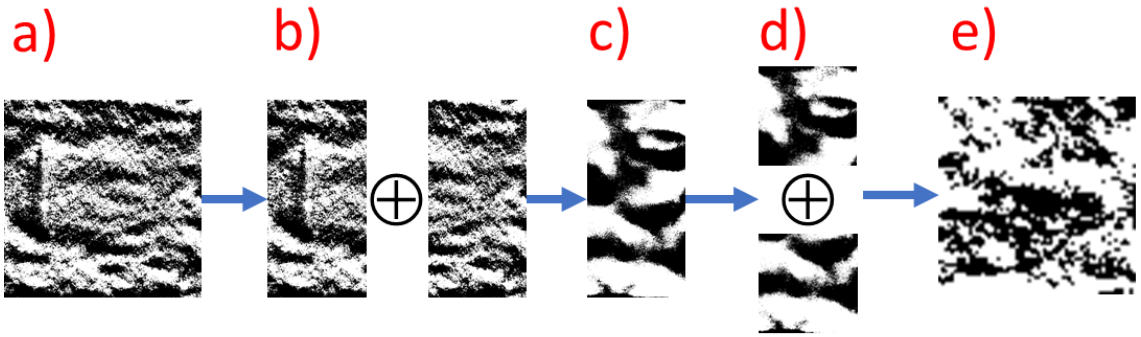

Figure 5.1: Step by step process of applying XOR de-biasing to a fingerprint. a) Resize the 650x650 px fingerprint down to 128x128 px. b) Split this in half vertically to produce two 64x128 px binary patterns. XOR these patterns together to produce a single 64x128 px binary pattern. c) Split the new binary pattern in half horizontally to produce two 64x64 px binary patterns. d) XOR the two 64x64 px binary patterns together to produce a single 64x64 px binary pattern. e) This final pattern is the XOR de-biased fingerprint.

Figure 5.1 details how this can be applied to a fingerprint. Whereas in a non-de-biased fingerprint the 650x650 px binary pattern produced by the algorithm is resized to a 64x64 px fingerprint(see section 3.3) and then is complete, this resizing step is replaced by an additional post-processing sequence. The application of two XOR operation ensures that the bias is optimised. The probability of an attacker guessing all four of the pixels used to generate just a single fingerprint pixel is 12.5%. Therefore any structural information of the QD-PUF cannot be determined accurately from just the de-biased fingerprint alone.

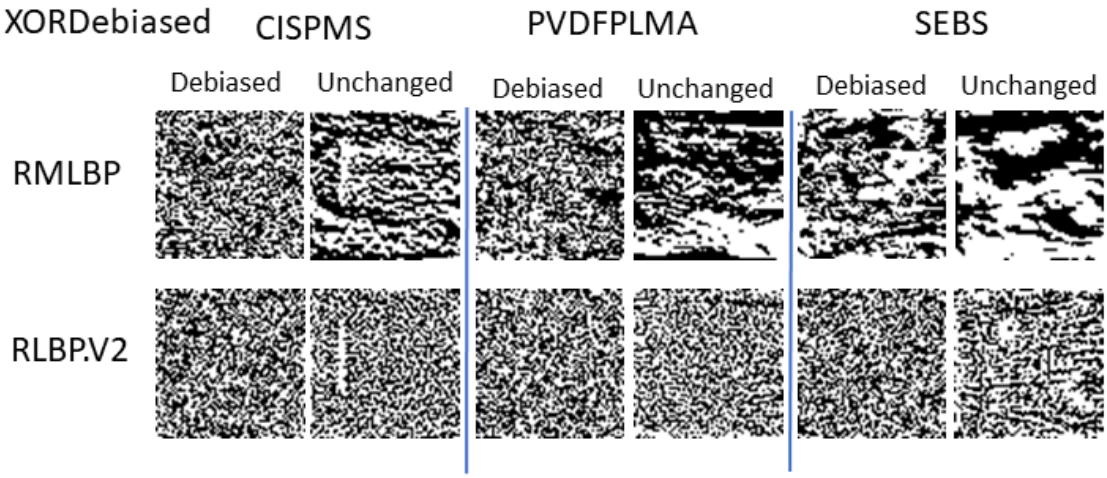

Figure 5.2: Table of example fingerprints generated by the application of an additional XOR de-biasing post-processing step. Rows represent different fingerprinting techniques. Columns represent individual quantum dot patterns, with each column split into the de-biased fingerprint on the left and an unchanged fingerprint on the right. Each fingerprint shown was generated at $R = 10$.

As can be seen from figure 5.2 the XOR de-biasing process drastically alters the appearance of the fingerprints and breaks up large areas of single bit values. Visually none of the structure from the unchanged fingerprint can be discerned. Interestingly SEBS for RMLBP still shows the largest uniform areas, indicating that there is an upper limit to the size of what can be broken down.

For all of the QD-PUFs tested in section 5.1 de-biased fingerprints were generated for both RMLBP and RLBP.V2, at radii of 1 to 20 inclusive. The same testing process for the NIST suite was then applied.

5.3 NIST Results and Discussion

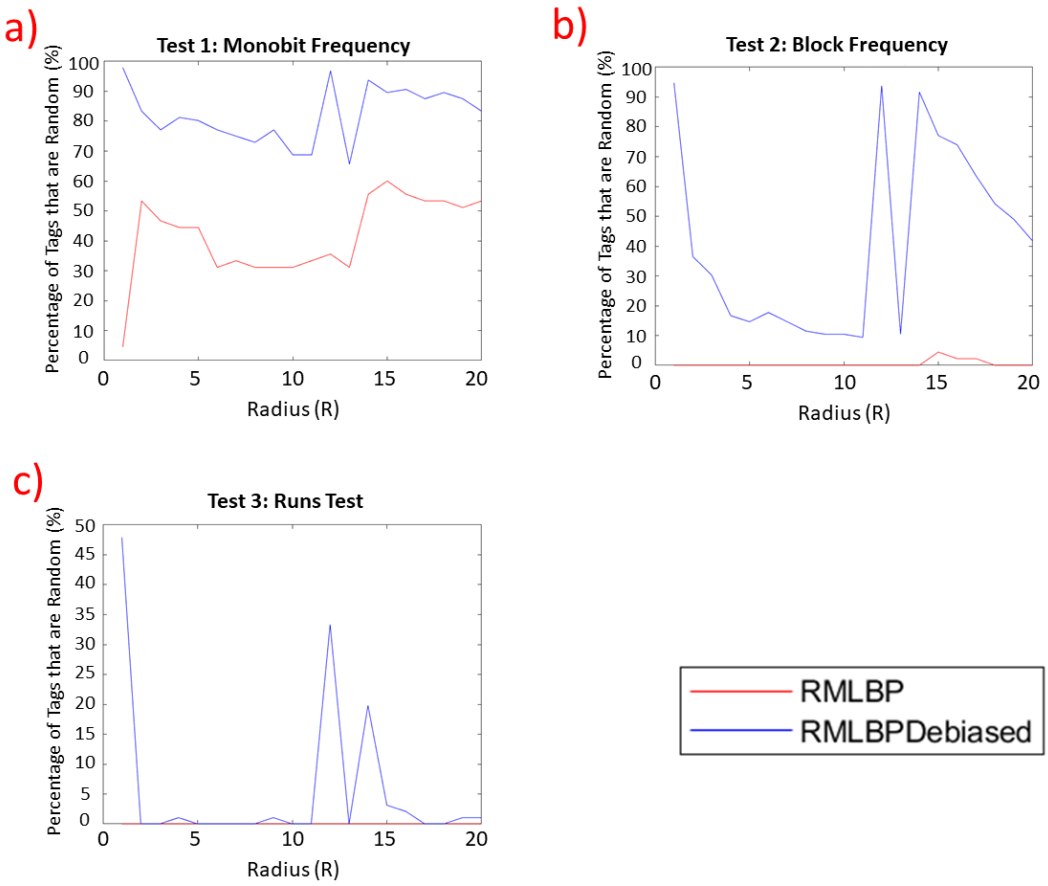

Figure 5.3: Graphs displaying the results of applying the selected NIST randomness suite tests to 48 different fingerprints generated using RMLBP and RMLBP with an XOR de-biasing post processing step. The y-axis of each shows the percentage of the tested QD-PUFs that were deemed to pass the test, this is known as the success rate for the test. a) Success rate of tested fingerprints for test 1 of the NIST randomness test suite (monobit frequency). b) Success rate of tested fingerprints for test 2 of the NIST randomness test suite (block frequency). c) Success rate of tested fingerprints for test 3 of the NIST randomness test suite (runs test). In each case the blue line represents the unchanged fingerprints and the orange the XOR de-biased fingerprints.

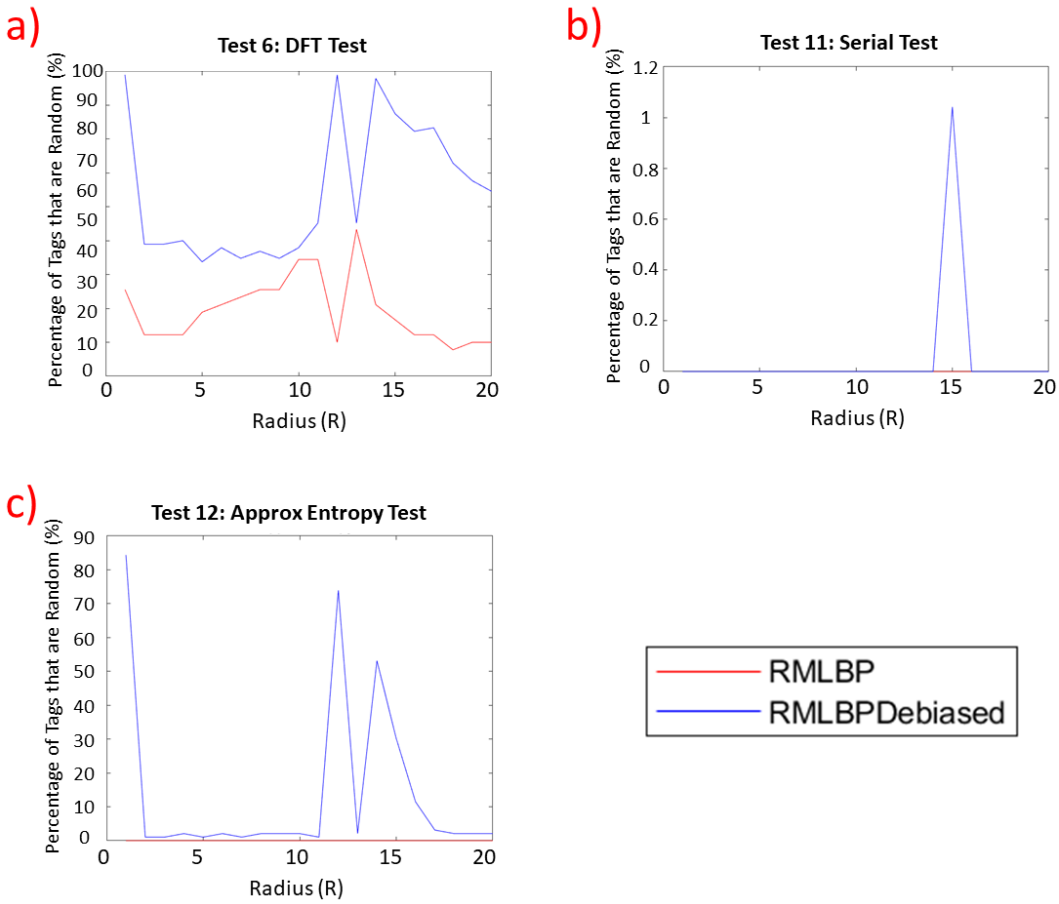

Figure 5.4: Graphs displaying the results of applying the selected NIST randomness suite tests to 48 different fingerprints generated using RMLBP and RMLBP with an XOR de-biasing post processing step. The y-axis of each shows the percentage of the tested QD-PUFs that were deemed to pass the test, this is known as the success rate for the test. a) Success rate of tested fingerprints for test 6 of the NIST randomness test suite (discrete Fourier transform test). b) Success rate of tested fingerprints for test 11 of the NIST randomness test suite (serial test). c) Success rate of tested fingerprints for test 12 of the NIST randomness test suite (approximate entropy test). In each case the blue line represents the unchanged fingerprints and the orange the XOR de-biased fingerprints.

The concerns of a potential for information leakage within RMLBP discussed in the beginning of this section are given light in figures 5.3 and 5.4. As can be seen all of the tests have a low success rate for RMLBP by itself. Indicating that as expected and as discussed throughout chapter 4 the fingerprints from RMLBP, whilst they may be unique, have a low degree of randomness. a and b in figure 5.3 demonstrate the importance of scalability. As we see a significant drop in success rate between the two. The reasoning behind this can be seen visually in RMLBP fingerprints. Although some may achieve optimal bias globally, the large uniform areas prevent this on a local scale. A fact which would greatly aid a brute force attacker.

The only other test in which RMLBP saw any degree of success is the discrete Fourier transform test. Again the large uniform areas likely posed an issue here. Runs of one value or another would be seen as a repeating pattern and so would contribute to a lack

of randomness. It is likely that those with smaller features such as CISPMS would have been the ones to pass this test.

Finally there are the cases of figures 5.3c, 5.4b and 5.4c, wherein RMLBP achieved a 0% success rate at all tested radii. As already covered the production of large uniform areas in RMLBP fingerprints is the cause of this. It comes as no surprise as to why they would cause problems for RMLBP in the Runs Test. For the Serial and Approximate Entropy tests this poses a similar problem. The uniform areas will be seen as repeated patterns of single bit runs thus, reducing the randomness of the fingerprints in the eyes of these tests. Although the gradient encoding method of RMLBP grants high repeatability and robustness it comes at the cost of randomness.

As is immediately clear XOR de-biasing has, at almost all radii, resulted in an improvement in the results of the majority of randomness tests for RMLBP. First and foremost it is important to note that in figure 5.3a the de-biasing aspect of the post-processing step has worked as expected. This shows particular gains in the block frequency test, where the breaking up of the uniform areas has brought local and global bias closer in value (in all cases the variation with radii will be discussed below). Such an improvement can also be noted in the improvement in the DFT test success rate. This supports the concept that the XOR de-biasing is obscuring structure has it has clearly removed periodic patterns from the fingerprint. The fact that either bit has an equal chance of occurring has ensured the output lacks the clear patterns of the input fingerprint. This suggests that in terms of repeatable patterns XOR debiasing has improved the randomness of the RMLBP fingerprints.

The less substantial improvements seen in figures 5.3c and 5.4c supports a hypothesis proposed in section 5.2. Namely that although the XOR de-biasing has broken down large uniform areas, there is a limit to the size of them that can broken down. As can be seen below with RLBP.V2 which lacks the large uniform areas, XOR de-biasing produces much more substantial improvements in these tests. Then there is the serial test which showed only a minuscule 1% improvement at a single radius. Most likely this is an outlier. Certain patterns within the fingerprinting algorithms are more common than others, this would suggest that XOR de-biasing has not sufficiently removed this to be deemed random by this test.

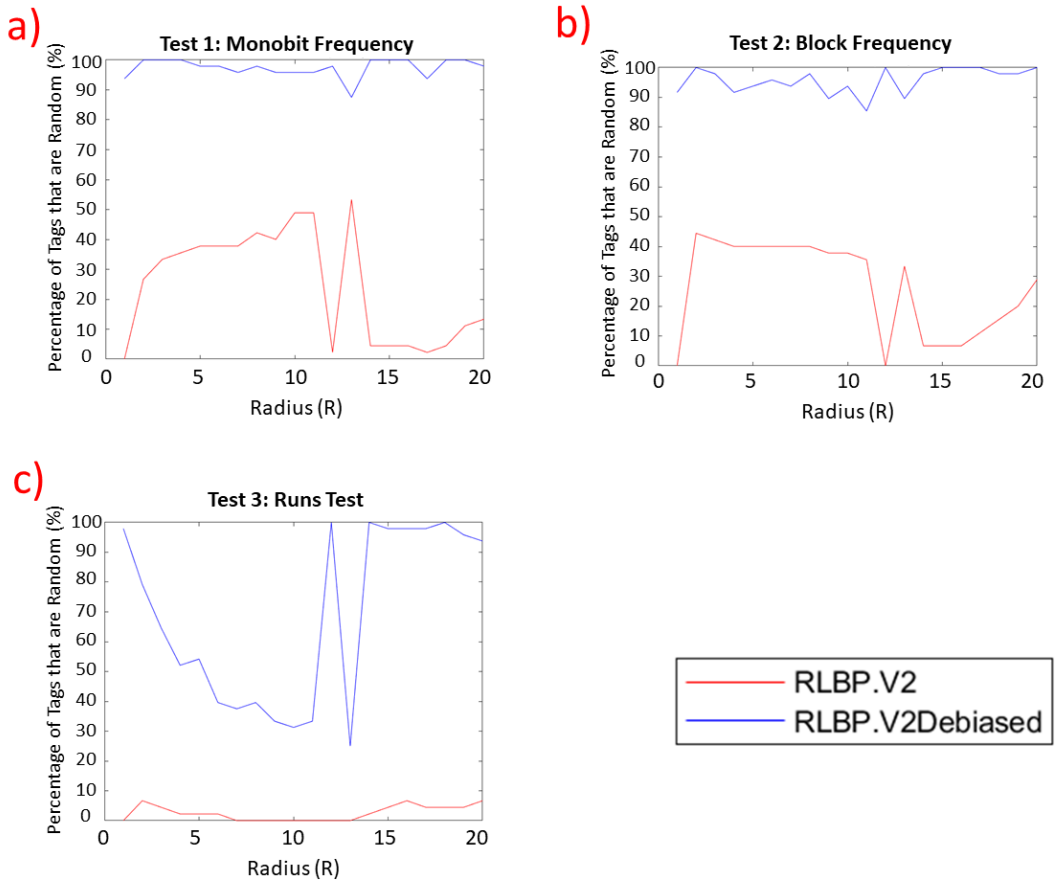

Figure 5.5: Graphs displaying the results of applying the selected NIST randomness suite tests to 48 different fingerprints generated using RLBP.V2 and RLBP.V2 with an XOR de-biasing post processing step. The y-axis of each shows the percentage of the tested QD-PUFs that were deemed to pass the test, this is known as the success rate for the test. a) Success rate of tested fingerprints for test 1 of the NIST randomness test suite (monobit frequency). b) Success rate of tested fingerprints for test 2 of the NIST randomness test suite (block frequency). c) Success rate of tested fingerprints for test 3 of the NIST randomness test suite (runs test). In each case the blue line represents the unchanged fingerprints and the orange the XOR de-biased fingerprints.

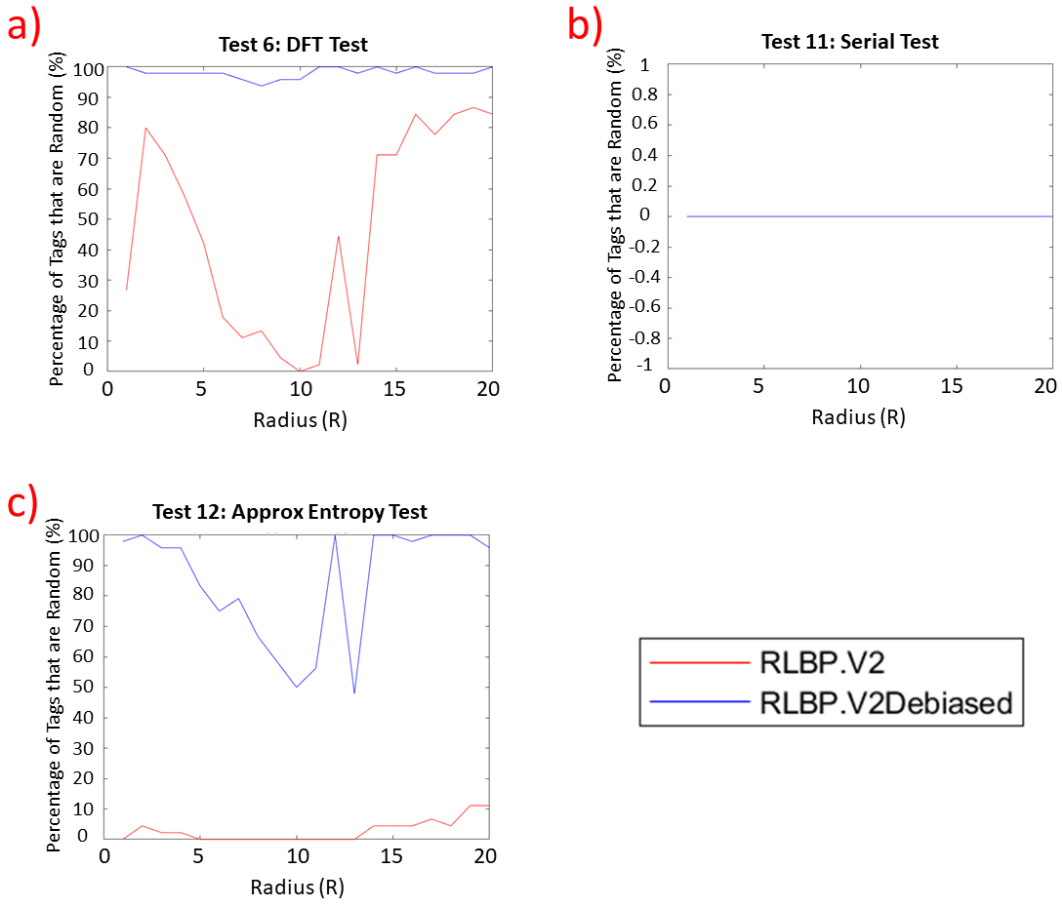

Figure 5.6: Graphs displaying the results of applying the selected NIST randomness suite tests to 48 different fingerprints generated using RLBP.V2 and RLBP.V2 with an XOR de-biasing post processing step. The y-axis of each shows the percentage of the tested QD-PUFs that were deemed to pass the test, this is known as the success rate for the test. a) Success rate of tested fingerprints for test 6 of the NIST randomness test suite (discrete Fourier transform test). b) Success rate of tested fingerprints for test 11 of the NIST randomness test suite (serial test). c) Success rate of tested fingerprints for test 12 of the NIST randomness test suite (approximate entropy test). In each case the blue line represents the unchanged fingerprints and the orange the XOR de-biased fingerprints.

Although RLBP.V2 shows an improvement on the success rates of RMLBP without any de-biasing, figures 5.5 and 5.6 clearly indicate that in all but the DFT test, RLBP.V2 still fails the randomness tests the majority of the time. This is despite RLBP.V2 possessing the highest ENIB and lowest inter standard deviation of the algorithms (in the undamaged case), indicating a higher uniqueness. Supporting the fact once again that although the fingerprints may be highly unique they lack in randomness, a fact that would benefit an attacker.

Although the two algorithms are close in their success rates in the monobit frequency test, RLBP.V2 shows a marked improvement on its gradient based counterpart. This is due to the lack of such blocky single bit areas within the fingerprints of RLBP.V2 gives it an improvement on its local bias. Such improvements are even more significant when we look at figure5.6a. RLBP.V2 achieves success rates in the DFT test that are comparable

to RMLBP with XOR de-biasing. A clear indicator that RLBP.V2 produces fingerprints with less repeated patterns, as to be expected given the finer scale details it can encode. However, it should be noted that another contributing factor to this may be RLBP.V2's higher susceptibility to noise. Randomly distributed noise would break up periodic patterns.

Figures 5.5c, 5.6b and 5.6c display a similar result to RMLBP with low success rates. Each of these can be attributed to the fact that despite the more granular nature of the fingerprints RLBP.V2 produces it still follows the structures within the QD-PUFs. Although such structures are unique they bear clear, repeated structural features. These include things such as edges, corners and flat spaces, each represented by their own arrangement of bits. Each also exists in an orderly fashion in regards to the other, edges must surround a flat area, corners are attached to two edges, for example. This will reduce the randomness of any fingerprint.

The application of XOR de-biasing to RLBP.V2 shows even more substantial improvements to success rates than for RMLBP. As to be expected given the hypothesis that XOR de-biasing works best with fingerprints that lack large uniform areas. In particular figures 5.5a, 5.5b and 5.6a show success rates that on average remain higher than 90%. Indicating that in terms of global and local bias as well as the absence of periodic patterns the majority of RLBP.V2 fingerprints with XOR de-biasing are deemed random. Significantly reducing entropy leakage.

Figures 5.5c and 5.6c still show a significant improvement in success rate with the application of de-biasing but lack the consistent success at all radii. In figures 5.3, 5.4, 5.5 and 5.6 we see this pattern of an initial decrease in success rate, followed by alternating spikes. Although they do occur at similar radii the trend is not exactly the same each time, often showing significant differences. It is also not consistent in which tests it appears in across all of the figures relating to the NIST test results. The origin of this is unknown and would require further testing that is not necessary to the conclusion of this experiment. It is likely however, linked to the size of features within the tested QD-PUFs given the consistent radii it occurs at. Aside from this figures5.5c and 5.6c do achieve success rates above 90% indicating that XOR de-biasing coupled with RLBP.V2 can remove most information leakage at particular radii.

The results of the serial test are again however, lacking in any improvement. Adding further support to the concept that the balancing of the frequency off all overlapping patterns with fingerprints is likely not possible using XOR de-biasing.

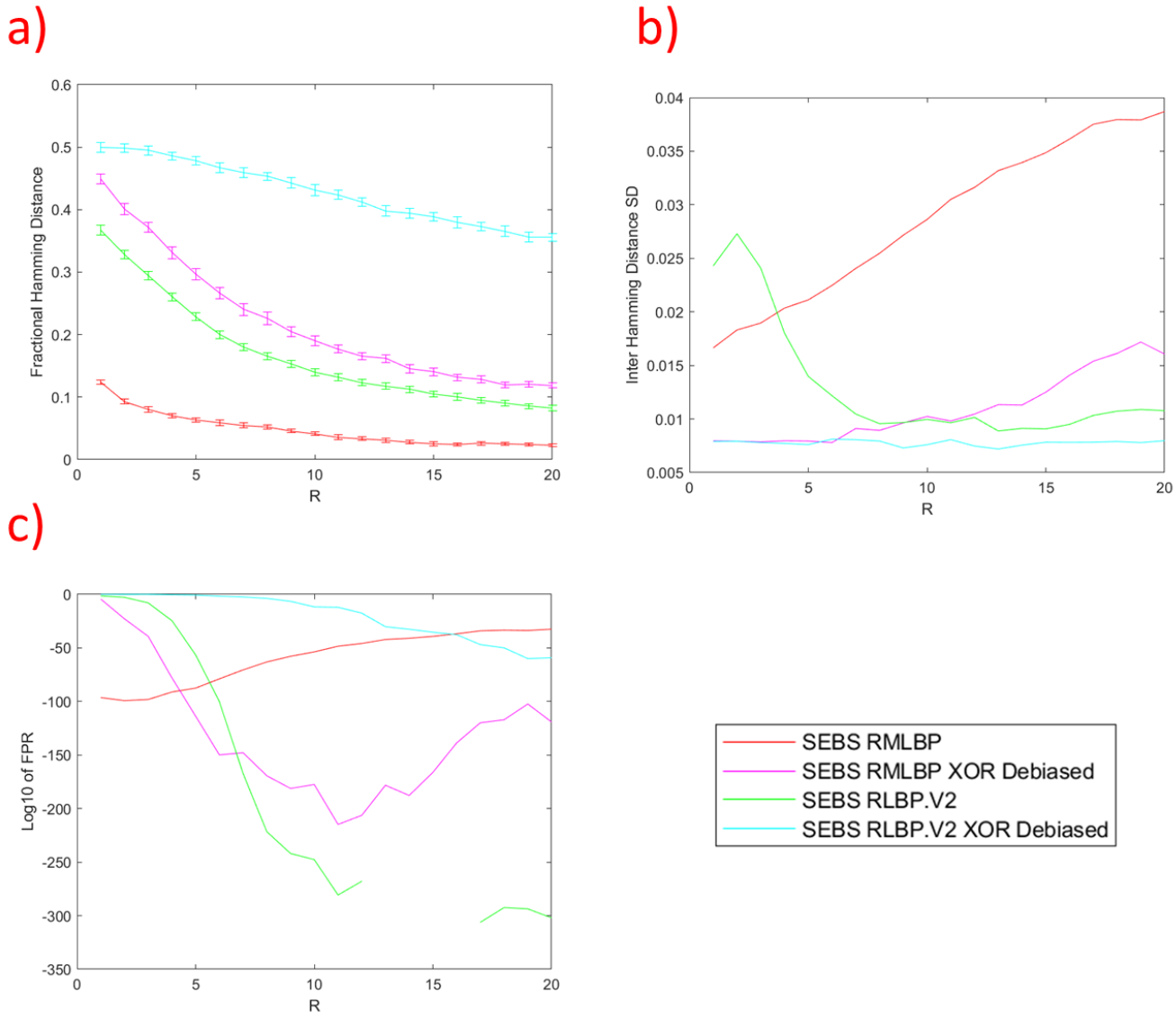

Figure 5.7: Figures of merit of RMLBP, RLBP.V2 and their XOR de-biased counterparts for the SEBS QD-PUF first detailed in section 4.1. a) Fractional intra hamming distance of each of the algorithms with increasing radius. b) Inter hamming standard deviation of each of the algorithms with increasing radius. c) log_{10} of the false positive rate of each of the algorithms with increasing radius.

Finally we address the effect that the de-biasing has on the figures of merit that were discussed in chapter 3. SEBS was chosen of the three QD-PUFs analysed chapter 4 as it lacked the distinct pinprick pattern of CISPMS or the almost lack of features of PVDF-PLMA. Here we can see immediately the drawback of the application of XOR de-biasing. Given that the process involves the combination of four separate pixels it magnifies the effect of any noise within the fingerprint. Although this undoubtedly aids in the addi-

tion of randomness it greatly reduces the repeatability of the fingerprints. This is seen in figure 5.7a with the significant increase in intra hamming distances at all radii. To the extent that at certain radii RLBP.V2 with de-biasing achieves intras of around 0.5, indicating that the repeat fingerprints are entirely unique from one another. RMLBP fairs significantly better owing to its increased robustness against the effects of noise.

Both algorithms do see a reduction in their inter hamming standard deviation. RLBP.V2 with de-biasing achieving the lowest at almost all radii. This may not necessarily be a positive however, although it shows its fingerprints are the most unique, the intra hamming distance values indicate repeats of itself are unique from each other. RMLBP on the other hand shows the greatest difference between its unchanged and de-biased inter standard deviation. This shows that the presence of the large uniform areas was indeed what was hampering the uniqueness of its fingerprints.

Finally this bring us to the FPR of the fingerprints where we see another example of an occasion where the repeatability of fingerprints outweighs their uniqueness for accurate authentication. Similarly to the results seen in section 4.2.3 it does not matter how unique the fingerprints produced are if the intra hamming distance of them is too high. The lack of robustness to noise shown by RLBP.V2 here significantly worsens its FPR, to the point where at low radii it fails the maximum requirement of 10^{-6}. Conversely however, the improvement to the uniqueness of RMLBP has resulted in a significant improvement in FPR. Although the repeatability of its fingerprints has decreased it has not reached the point wherein this hampers accurate authentication.

5.4 Concluding Remarks

To summarise, it has been demonstrated that the issues of information leakage with fingerprints can be addressed. It is clear that information of the original structure of the QD-PUF can be destroyed using the leak proof operation of XOR de-biasing without creating a fingerprint that cannot be accurately authenticated. Thus, removing the possibility of the QD-PUF fingerprints being the weak link in the authentication chain. This however, comes with the caveat that the fingerprinting algorithm used must be highly robust to noise. The nature of XOR means that it does indeed break down prexisting patterns in a manner that cannot be reverse engineered. The process is however highly prone to the effects of noise, as if even one of the bits at any of the stages has been changed due to noise the effect is compounded.

It should also be noted that, at least with the two algorithms tested, there is a trade off between fingerprint repeatability and randomness achievable. As such for the applications of these QD-PUFs discussed in chapter 4 section 4.3, RMLBP is best suited if de-biasing is needed. For applications such as those commonly used in Von Neumann de-biasing where the PUF response is encoded and helper data is required, RLBP.V2's higher achievable randomness would be better suited.

For all further experiments detailed outside of this section XOR de-biasing will not be

applied. This is because it adds another factor to consider when drawing conclusions.

Chapter 6

Addressing QD-PUF Degradation over Time

Chapter 4 demonstrates clearly that QD-PUFs can be used as secure authentication tokens. There are however further considerations when these are used in a practical setting. The foremost of which is the degradation of the quantum dots with time[19]. Covered in further detail in section 2.1.3 oxidization, of the quantum dots causes their emission to decrease. Given that the emission pattern is what the fingerprinting algorithms process this poses an issue with using the QD-PUFs for any long term authentication purposes. For example a QD-PUF used in a passport whose must have emission that remains bright enough to be authenticated for the entire decade long lifespan of the passport. The purpose of this chapter is to address this issue.

The stability of emission of colloidal quantum dots is dependant on their specific chemistry and morphology[19]. In all cases however oxidization on exposure of the CQDs with air causes the emission to decrease[59]. The suspension of the CQDs in a polymer matrix limits exposure to oxygen and thus, improves the emission stability[22]. Section 6.1 details the process of producing the QD-PUFs. Two groups of five different polymers (PMMA, PS, PMS, PVDF and SEBS) were chosen, the latter group consisting of the the same five as the first only with PLMA added as a co-polymer. As the effectiveness of suspension in polymer depends on the oxygen diffusion rate of the polymer and the compatibility with the CQDs, this allows for a wide range to be tested and the effects of blended polymers to be observed. The key stability factors to be tested are the photoluminesence (PL) of the QD-PUF with time as well as any change in the fingerprint with time compared to a fingerprint generated on the day the QD-PUF was made. These results are discussed in section 6.2.

6.1 Degradation methodology

6.1.1 QD-PUF Creation

For this experiment InP/ZnS quantum dots with oleylamine ligands were chosen as the quantum material. These were chosen due to their high quantum yield (the ratio of the number of photons emitted to the number absorbed), at greater than 65%, narrow full width half-maximum of 50 nm, as well as their lower toxicity than cadmium based CQDs[5]. Their maximum emission of 630 nm also allows for easy filtering of the excita-

tion light when the produced QD-PUFs are analysed using the apparatus shown in figure 3.1. As previously discussed these particular CQDs also show a sensitivity to degradation due to oxygen in their photoluminescence[21]. This should give clearer results to interpret.

The creation of the QD-PUFs was performed by Dr Nema Abdelazim (of Lancaster University at the time). In each case solutions of the InP/ZnS CQDs were mixed with the hydrophobic polymers in toluene. Using a micrometre doctor-blade this mixed solution was then applied to a black polyethene substrate. This formed a dry film on the substrate at a thickness of 5μm. Each was then cured in a vacuum oven.

Two groups of five polymers were chosen for testing. The first consisted of Poly(methyl methacrylate) PMMA, Polystyrene PS, Poly(styrene-ethylene-butylene-styrene) SEBS, poly(vinylidene) fluoride PVDF, and Poly 4-methlstyene PMS. These were chosen owing to their optical transparency and their solubility in organic solvents, making them appropriate to mix with the InP/ZnS CQDs[22][5]. To create these QD-PUFs, InP/ZnS CQDs were dissolved in toluene. The chosen polymer was then dissolved in toluene to create two separate solutions. These were then mixed together and followed by sonication for 30 minutes to agitate them in the solution. This produced a CQD and polymer solution with CQD concentration of 80 mgml^{-1}. 300μl of this solution was then placed in the doctor-blade and deposisted onto the substrate to for a 5μm thick, 10mm by 10mm quantum dot pattern. The QD-PUFs were then cured overnight at 60°C in a vacuum oven.

The second group of QD-PUFs made consisted of the same five polymers as in group 1, only with the addition of polylauryl methacrylate (PLMA) as a co-polymer in a 95/5 polymer/co-polymer ratio. This was done as PLMA showed rapid photoluminescence stabilization in preliminary testing. Thus, the two groups would show if the addition of PLMA would improve upon using just a single encapsulation polymer. PLMA was not used by itself however as in the initial testing its high viscosity meant that it took many days to properly cure. The preparation of mixtures for group 2 varied slightly to that of group 1. The process proceeded in the same manner aside from the addition of the co-polymer to the polymer-toluene solution.

6.1.2 QD-PUF Testing

After creation each of the QD-PUFs were stored in open air and in ambient conditions. This ensured that they were subject to conditions similar to if they were in use on a product in a practical setting and so would decay in a similar manner. Periodically the QD-PUFs would be placed in the apparatus shown in section 3.2 and imaged using the process detailed in that section. Exposure values were chosen to maximise the brightness of the image taken without causing any saturation. 25 repeat images of each QD-PUF were taken.

From the first of these a measure of the QD-PUF's photoluminescence was derived at each day they were imaged. The image was cropped to just the area containing quantum material and the average pixel brightness calculated. From this was then subtracted the measured background noise level for the camera and the result calibrated for the exposure the image was taken at. For each QD-PUF this calibrated average pixel brightness

was then plotted against days since the QD-PUF was created with the first measurement taken as soon as the QD-PUF was cured.

For analysis of the fingerprints both RMLBP and RLBP.V2 were chosen. These showed the lowest intra hamming distance and lowest FPR respectively in chapter 4. With RMLBP being the most robust against change to the input image and RLBP.V2 being the least. This also gives an example of a gradient and a contrast based fingerprinting scheme, in order to compare how each handles degrading fingerprints.

For each day that an image was taken fingerprints were generated from each of the repeat images at radii from 1 to 20. For the first day the first two of these fingerprints were used as the challenge fingerprints and the other 23 repeats used as the reference fingerprints to generate the intra hamming distance. The same database of 48 other unique fingerprints as used in chapter 4 were then compared to the challenge fingerprints to generate the inter hamming distance distribution. As in chapter 4 the FPR for each radii was then calculated from these two distributions.

For each day after the first, the first two fingerprints were still used as the challenge fingerprints and still compared to the database of 48 other QD-PUFs to generate the inter hamming distance distribution. For intra hamming distance however the challenge fingerprints were compared to the reference fingerprints from day 1. This gives a measure in the intra hamming distance of how much the fingerprints have changed as the QD-PUF they were generated from degrades. This is reflective of how a QD-PUF authentication system would work, as the reference fingerprints would be generated well before a consumer wishes to authenticate a QD-PUF. The FPR is then calculated as normal.

The minimum FPR and intra hamming distance mean achieved over all radii is then plotted against days since the QD-PUFs creation.

6.2 QD-PUF Degradation Results and Analysis

6.2.1 Group 1

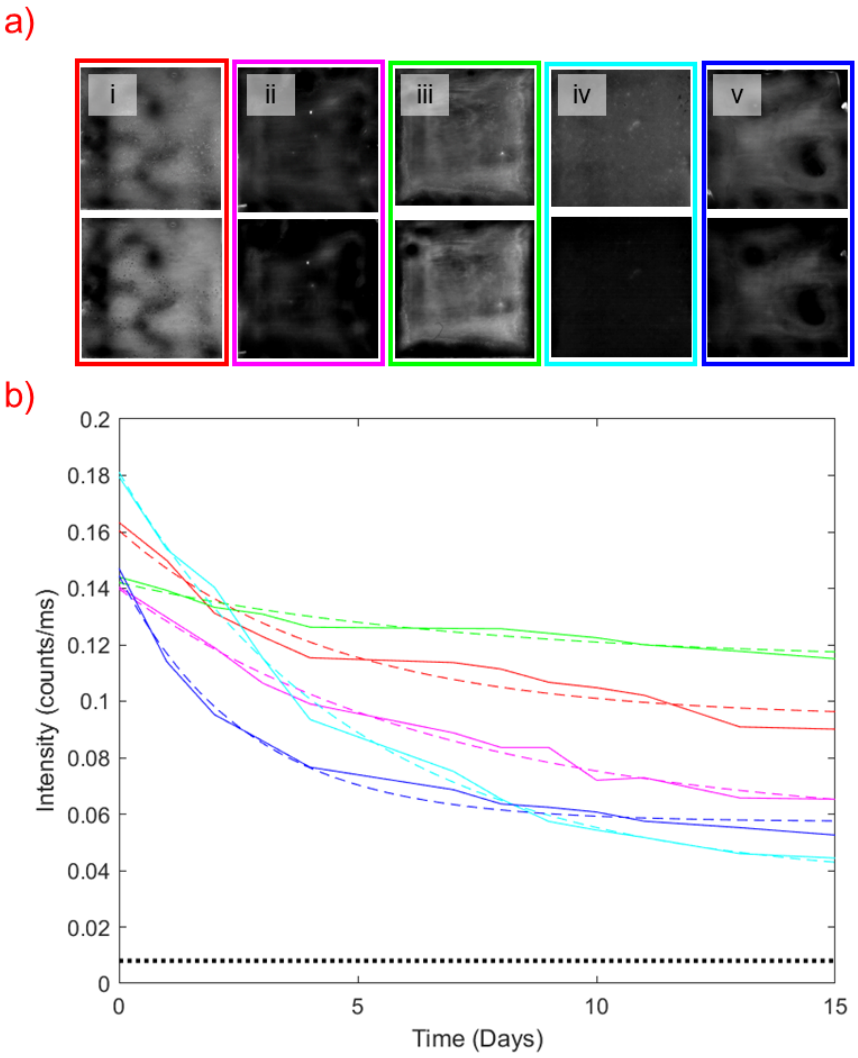

Figure 6.1: a) Top - image of each Group 1 QD-PUF captured on the day they were created using the apparatus detailed in section 3.2. Bottom - image of each QD-PUF captured 15 days after their creation captured under the same conditions. These images have been increased in brightness by 30%, post capture, to aid in comparison for this sub figure only. i-PMMA, ii-PMS, iii-PS, iv-PVDF and v-SEBS. b) A plot showing the average PL intensity of each QD-PUF as a function of time since their creation. The dashed line represents an exponential fit with linear offset that was applied to each data set. The colour of the lines corresponds to the colour surrounding the QD-PUF image in sub-figure a. The black dotted line represents the CCD-sensor's background noise signal.

As expected from the theoretical background covered in section 2.1.3, figure 6.1a clearly shows that the photoluminescence of quantum dots in polymer does indeed degrade with time. Owing to the oxidization mechanism responsible for the degradation of CQDs, an exponential decay fit with linear offset ($y = y_0 + Aexp(R_0 x)$) is appropriate for use to extrapolate the anticipated emission intensity following stabilization after a long period of

time[19]. The values of y_0 garnered from the fits show that for each of the polymers used the photoluminescence will stabilise to a value above the background count of the CCD sensor. The lowest of these being PVDF, the asymptote of which sits at 4.5 times greater than the value of the background count. Indicating that for each of these QD-PUFs we can expect them to keep emitting, when excited, at an intensity great enough to detect for the feasible lifetime of a practical application (e.g. such as several years required for anti-counterfeiting applications).

Of the five polymers tested PS showed both the highest asymptote value for its PL as well as the smallest loss of PL at 20%. Making it clear that it has the best compatibility with the InP/ZnS CQDs and thus, resisted oxidization the most. Conversely PVDF starts with the highest PL but has the lowest value asymptote, losing 80% of its initial PL. This large change in emission intensity indicating that it is far less suited as a polymer matrix in which to embed the CQDs used. Overall this shows us that the use of a matched polymer minimizes ligand loss in the encapsulation process and minimizes oxygen diffusion to the QD surface. As well as this the oxygen diffusion rate of the polymer that the dots are embedded in plays a role in stability. For example, the SEBS triblock co-polymer has higher oxygen diffusion rate than the PS block[60] and in the process gives a greater loss of PL at 60%

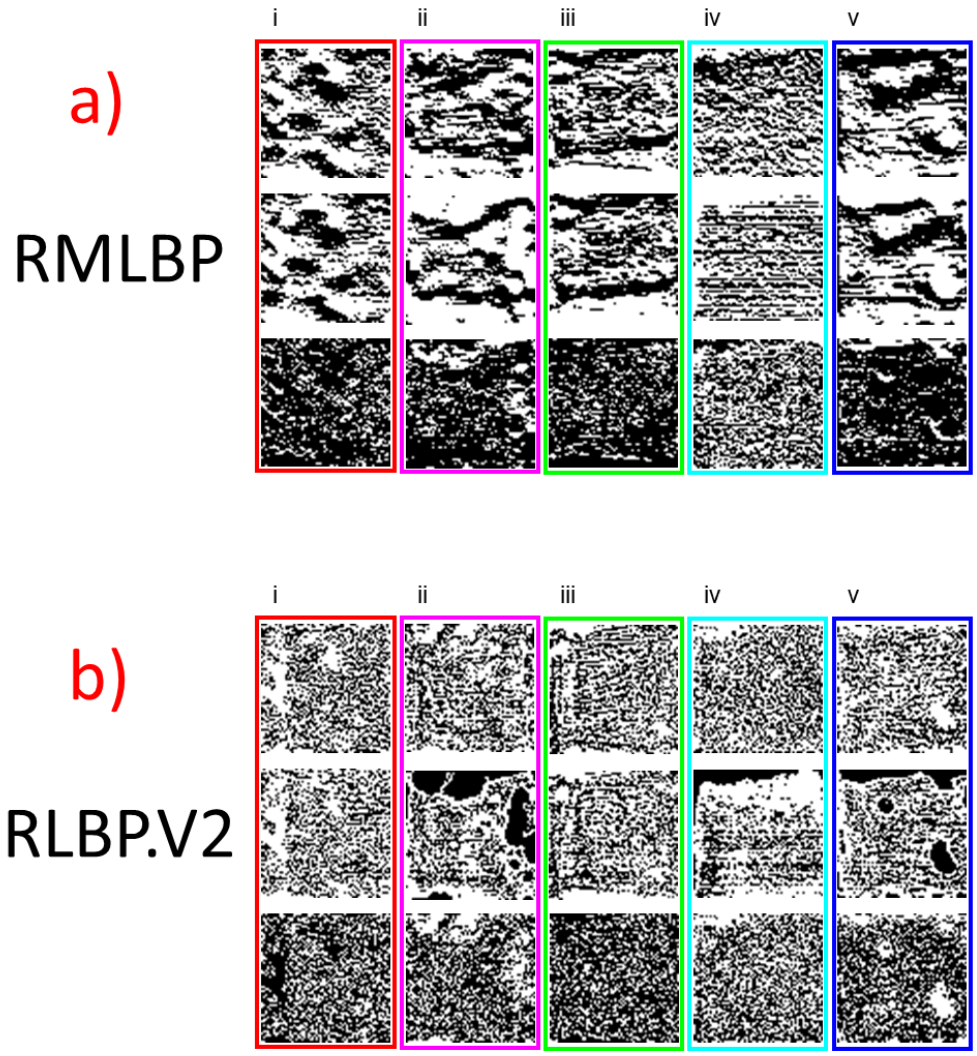

Figure 6.2: For both sub figures the top row represents the fingerprints generated from the Group 1 QD-PUFs on the day of their creation. The middle row represents the fingerprints generated from the same QD-PUF 18 days later. All fingerprints were generated at R=5.The bottom row represents the XOR of the top an bottom row, showing the pixels that are different between the two. i-PMMA, ii-PMS, iii-PS, iv-PVDF and v-SEBS. a) Fingerprints generated using RMLBP. Percentage difference between day 1 and day 18 fingerprints: i-21%, ii-25%, iii-19%, iv-48% and v-20%. b) Fingerprints generated using RLBP.V2. Percentage difference between day 1 and day 18 fingerprints: i-36%, ii-43%, iii-30%, iv-49% and v-40%.

As expected from the work discussed in chapter 4, the fingerprints produced by RMLBP show the characteristic low noise but "blocky" patterns of gradient based fingerprinting schemes. For all of the polymers bar PVDF we see little visual difference between the

fingerprints generated at the two extremes of the available data. As can be seen in figure 6.2 the areas of difference also appear to be randomly distributed (save for a fraction of pixels at the tops of PMS and SEBS). This indicates that for each QD-PUF the change in fingerprints at this radius was owed to a changing signal to noise ratio as PL decreases. This is as opposed to it being due to significant change in the texture of the quantum dot pattern. A fact supported by the lack of any distinct visible change in figure 6.1a. Interestingly, PS shows the least change between the day 1 and day 18 fingerprint at 19% with the lowest PL decrease. PVDF on the other hand shows by far the largest PL decrease and a change in fingerprint almost double that of the next closest at 48%. This would suggest that the change in PL dictates the difference between the fingerprints, if not for the fact that the other three QD-PUFs in group 1 for RMLBP following no discernible link. Suggesting that although PL stability plays a role in this another factor also has an influence. As discussed in chapter 4 this may well be texture of the quantum dot pattern. As it was shown that some are better suited to the effects of increasing noise than others.

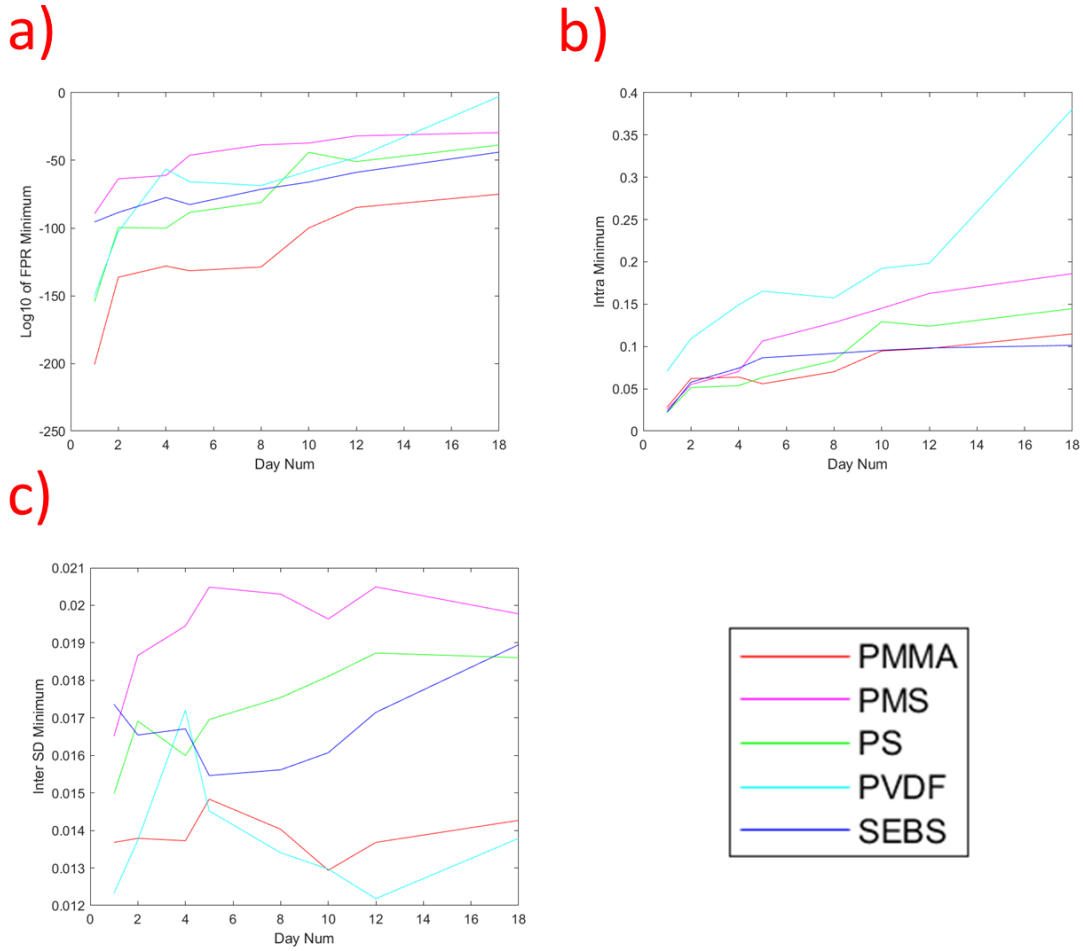

Figure 6.3: a) Graph of the minimum FPR at each day achieved for each of the Group 1 QD-PUFs generated using RMLBP. b) Graph of the minimum intra hamming distance at each day achieved for each of the Group 1 QD-PUFs generated using RMLBP. c) Graph of the minimum inter hamming distance standard deviation at each day achieved for each of the Group 1 QD-PUFs generated using RMLBP. Note: the minimum for each day is the lowest value reached for that figure of merit for radii between 1 and 20. This R value may not be consistent between days or figures of merit. Any values that fell below MATLABs precision of 10^{-308} were set to a value of 10^{-308} for plotting.

As the PL intensity of the QD-PUFs decreases, the signal to noise ratio of the images captured of them will also decrease. As alluded to in analysis of figure 6.2 this is the dominating factor in the changing fingerprints as more days pass from the QD-PUF's creation. It was discussed in section 4.2 that increasing noise in a QD-PUF image does worsen the intra-hamming distances. This is now reflected in a more practical environment in figure 6.3b. With all bar PVDF appearing to increase following a logarithmic curve, tending to some asymptote in the same manner as the PL intensity. This would make sense as when the PL stabilises so too will the signal to noise ratio, resulting in the intra hamming curve flattening out. This is a useful feature to note as this shows that even after an indefinite period of time, any challenge fingerprint generated from a QD-PUF has a maximum possible separation from the reference. Much like with its change in PL, PVDF seems to have behaved anomalously poorly in comparison to the other QD-PUFs, with the data after day 12 showing a sharp increase. This unpredictable

nature and the large PL decay makes PVDF on its own with InP/ZnS CQDs unsuitable for use in the creation of QD-PUFs for long term use.

Another hypothesis raised in the discussion of figure 6.2 was the fact that PL stability is not the only factor influencing fingerprint stability. This is supported here in figure 6.3. There is no correlation between the magnitude of the decrease in PL and the increase in intra hamming distance minimum over the days tested. Despite SEBS and PMS showing the same change in PL of a 60% decrease, SEBS only shows an increase in intra minimum of 0.079 whereas PMS shows double that at 0.161. PS then follows PMS with an intra increase of 0.123, despite showing the least change in PL. This confirms that although a change in PL is what causes the difference in the fingerprints, the magnitude to which this occurs is influenced by another factor entirely. This factor will most likely be the texture of the QD-PUF and its influence on intra hamming distance, especially as the damage is increased however, the texture analysis required to quantitatively study this is beyond the scope of this thesis.

Following the influence of the decreasing signal to noise ratio on the intra hamming distance of the QD-PUFs the change in FPR comes as no surprise. As the challenge fingerprints become more and more dissimilar to their reference counterparts the accuracy of authentication will indeed decrease. In fact, as figure6.3a shows the FPR curves all follow similar trends to their intra counterparts. Supporting the fact that as the QD-PUFs PL stabilises so too does the authentication accuracy. Giving us a definitive value for how high the FPR of a certain QD-PUF will get after a prolonged time has past. Fortunately, (excluding PVDF) the highest value of each of the FPRs is significantly below the maximum limit of 10^{-6}. Once again however, neither the absolute value of the PL nor the magnitude of its change shows any correlation with which QD-PUF gives the lower FPR or the change in FPR over the time tested.

Instead, once again, this appears to be due to the texture and how it influences the fingerprint produced. As we can see in figure6.3c, the ordering of the inter hamming distance standard deviation minima does bear semblance to that of the FPR. Although more rigorous analysis involving accounting for different intra hamming distances is needed to give a definitive answer; this does give proof towards the influence of texture over PL change on the magnitude of the FPR values. It should also be noted that across all five tested QD-PUFs there is no consistency in how the degradation of the QD-PUF affects the uniqueness of the fingerprint produced for RMLBP.

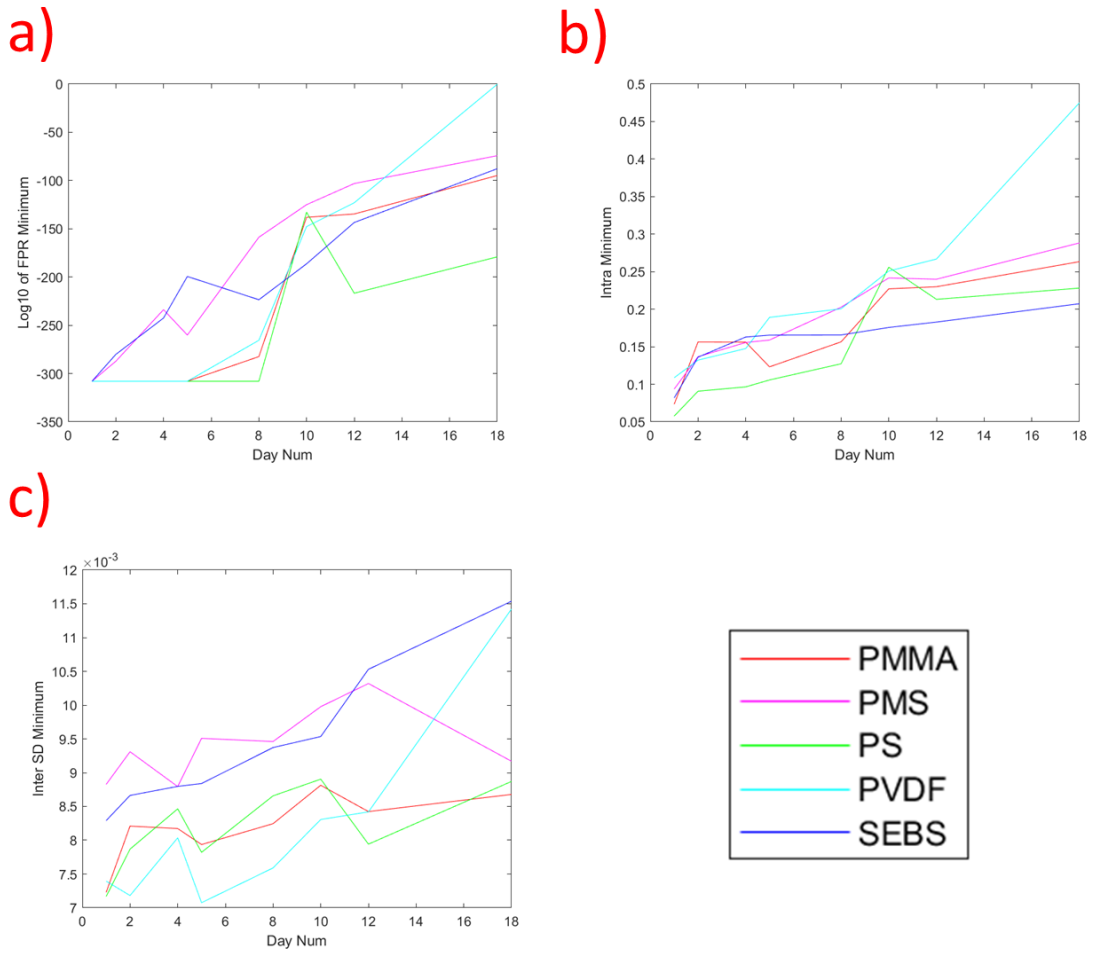

Figure 6.4: a) Graph of the minimum FPR at each day achieved for each of the Group 1 QD-PUFs generated using RLBP.V2. b) Graph of the minimum intra hamming distance at each day achieved for each of the Group 1 QD-PUFs generated using RLBP.V2. c) Graph of the minimum inter hamming distance standard deviation at each day achieved for each of the Group 1 QD-PUFs generated using RLBP.V2. Note: the minimum for each day is the lowest value reached for that figure of merit for radii between 1 and 20. This R value may not be consistent between days or figures of merit. Any values that fell below MATLABs precision of 10^{-308} were set to a value of 10^{-308} for plotting.

Aside from the higher entropy patterns the starkest difference between figures6.2a and b is the change in fingerprints between day 1 and 18. RLBP.V2 being a contrast based fingerprinting scheme is much more sensitive to noise than RMLBP. Thus, the decreasing signal to noise ratio has resulted in an increase in the percentage difference across the board. Another key difference is the fact that features in the day 1 fingerprint appear to have flipped bit value in the day 18 fingerprint (in particular PMS, PVDF and SEBS). This is not due to the quantum dot pattern itself changing, as we can visually confirm that it does not (see figure6.1a) but instead due to the decreasing PL. By comparing to figure6.1a we can see that the areas that change bit value all appear dark on day 1 and appear mostly in the three QD-PUFs with the lowest PL at day 18. As the average PL of the QD-PUFs decreases the change for these dark areas will be much less, they are dark as they contain much lower concentrations of quantum dots. Thus, the relative difference between the values of these areas and their surroundings is not maintained. This is not

an issue for RMLBP as the direction of gradients remains unaltered. For RLBP.V2 which depends on relative difference between areas this has a significant effect. Highlighting a shortfall in using RLBP.V2 for long term QD-PUF authentication. The presence of more randomly arranged pixels however suggests that reduced signal to noise ratio is still the dominating factor in the change.

The increased change in fingerprints over the time the experiment was performed when compared to RMLBP is reflected in figure 6.4b. As expected from RLBP.V2 the initial intra hamming distance values are larger than for RMLBP, as well as this however, the increase in intra hamming distance minimum is also greater. Showing that of the two RLBP.V2's fingerprints are more affected by the degradation of the QD-PUFs PL. Once again there also appears to be no clear correlation between the magnitude of the change in PL and the change in intra hamming distance. With the similarly degrading SEBS and PMS showing a change of 0.125 and 0.194 respectively. The least degrading of PS shows an intra increase of 0.17, the second lowest. Each does follow a similar trend to RMLBP though, with PVDF showing anomalous behaviour. Thus, showing that this was not an artefact of RMLBP and is in fact a physical phenomena. However, the greater change in intra hamming distance suggests that it will stabilise at a higher value, an issue when producing repeatable fingerprints for long term use.

When we look at figure 6.4a we see the advantages of a contrast based scheme such as RLBP.V2 but also potential downfalls. The FPR of RLBP.V2 is consistently lower than that of RMLBP for all but PVDF between day 12 and 18. The origin of this is clear to see in figure 6.4c as the inter hamming standard deviations produced are lower than that of RMLBP. Therefore within the data range tested RLBP.V2 gives more accurate authentication, even when the QD-PUF is degraded. It is when we consider further degradation outside of the tested range that issue begin to occur. A fact that must be considered in light of the fact that the change in FPR is much greater over the time period for RLBP.V2. For example SEBS increases by a factor of 10^{52} for RMLBP but a factor of 10^{220} for RLBP.V2. The data within figure 6.4a is ill suited to a fit for quantitative extrapolation. We can however, consider the fact that we know from chapter 4 that there is a point wherein low inter standard deviation no longer dominates FPR and intra hamming distance becomes more important. If the intra hamming distances of RLBP.V2 flatten out as the PL does then this will not be an issue. This would stabilise the FPR and RLBP.V2 would produce more accurate authentication at any time after the creation of the tag. Making it a very useful tool. If the intra does continue to increase however then the FPR will become worse than that of RMLBP, making RLBP.V2 only a useful tool for short term applications. Further testing is needed to confirm this.

To summarise, all of the QD-PUFs show degradation in their photoluminescence due to oxidization as time passes. There is a clear link between compatibility of the polymers with the CQDs and the stability of the PL. Regardless of the type of fingerprinting algorithm applied however, the PL or change in PL is not the sole factor influencing the fingerprints figures of merit. The likely other factor is the texture of the quantum dot pattern itself and the effect this has on the algorithms handling of noise. RMLBP produces fingerprints that show the least change due to PL degradation but within the time frame tested RLBP.V2 allows for more accurate authentication.

6.2.2 Group 2

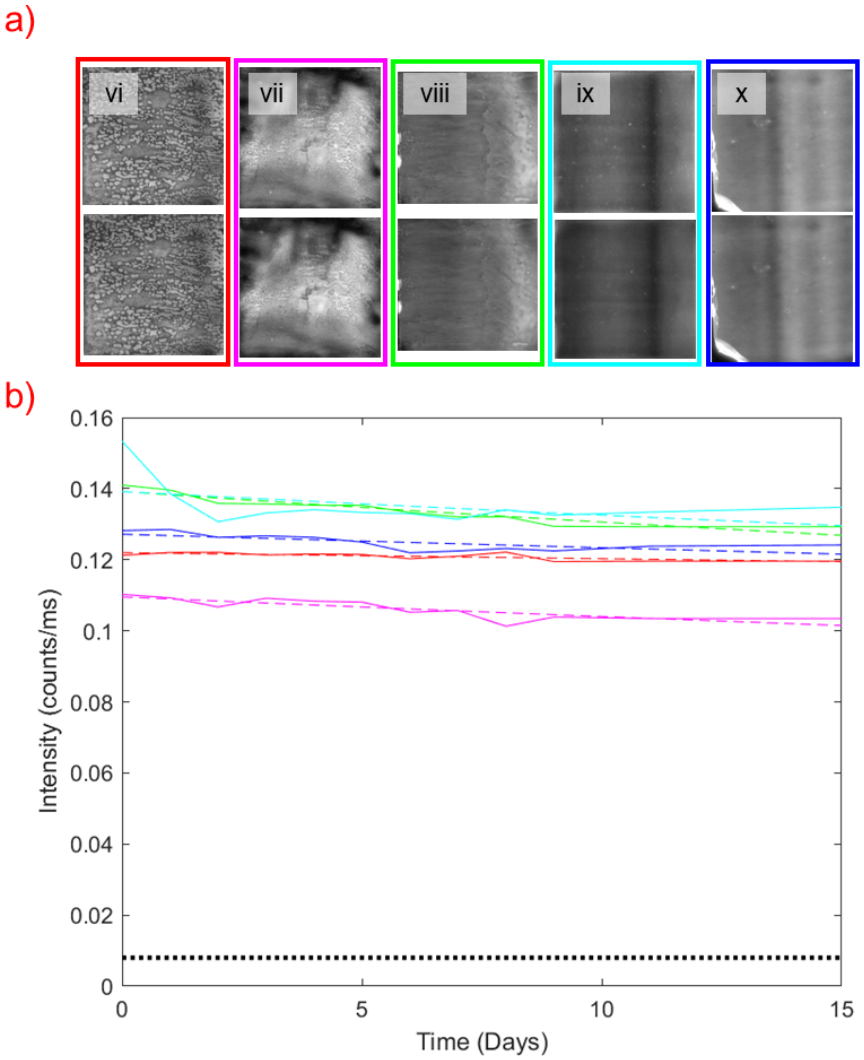

Figure 6.5: a) Top - image of each Group 1 QD-PUF captured on the day they were created using the apparatus detailed in section 3.2. Bottom - image of each QD-PUF captured 15 days after their creation captured under the same conditions. vi-PMMAPLMA, vii-PMSPLMA, viii-PSPLMA, ix-PVDFPLMA and x-SEBSPLMA. b) A plot showing the average PL intensity of each QD-PUF as a function of time since their creation. The dashed line represents an exponential fit with linear offset that was applied to each data set. The colour of the lines corresponds to the colour surrounding the QD-PUF image in sub-figure a. The black dotted line represents the CCD-sensor's background noise signal.

Figure 6.5a shows a clear difference in the textures produced between the quantum dot patterns of Groups 1 (see figure 6.1 and 2). In Group 2 the most obvious difference is the dispersal of the quantum dots as shown by the fact that the proportion of each pattern that consists of dark areas (that lack or have low CQD concentration) is significantly reduced. Large featureless areas are now replaced with more detailed textures, the most obvious example being the difference between PMMA and PMMAPLMA. As

demonstrated in chapter 4, large uniform areas within the patterns leads to worse intra hamming distances as they are more affected by noise. As such, the more apparent texturing should (and indeed does, see figures 6.7b and 6.8b) lead to lower intra hamming distances than their Group 1 counterparts. The presence of such change is likely due to PLMA being, unlike the other polymers, a highly viscous oily liquid, thus allowing for better CQD dispersal[61]. The only concern however is the parallel vertical strips present in PVDFPLMA and SEBSPLMA. These will most likely be printing artefacts and will affect inter hamming standard deviations given the highly non-random nature of them.

Once again the PL data proved a good fit for an exponential decay model. Showing that the PL of the QD-PUFs stabilises to a fixed value given time. With the addition of PLMA however this stabilisation has occurred much quicker and with significantly less loss of PL. The worst performing of Group 2 was PVDFPLMA with a 13% loss of PL between it's starting value and it's asymptote. This outperforms the best of Group 1, PS, which showed a loss of 20%. Indicating that the addition of PLMA has indeed improved upon the photoluminescence stability of the QD-PUFs, this is due it blocking the ambient oxygen from reaching the CQDs surface[60]. It should be noted however that once again the PVDF QD-PUF is the worst performing for PL stability. This shows us that there is a lack of compatibility between PVDF and the CQDs[22]. Finally to give a direct show of performance we can see that even the lowest of the measured photoluminescence, that of PMSPLMA, is still 12.5 times greater than the background count. Giving the worst PL of group 2 a signal to noise ratio 3 times better than the best of Group 1 at stabilisation, despite their initial PL's being lower.

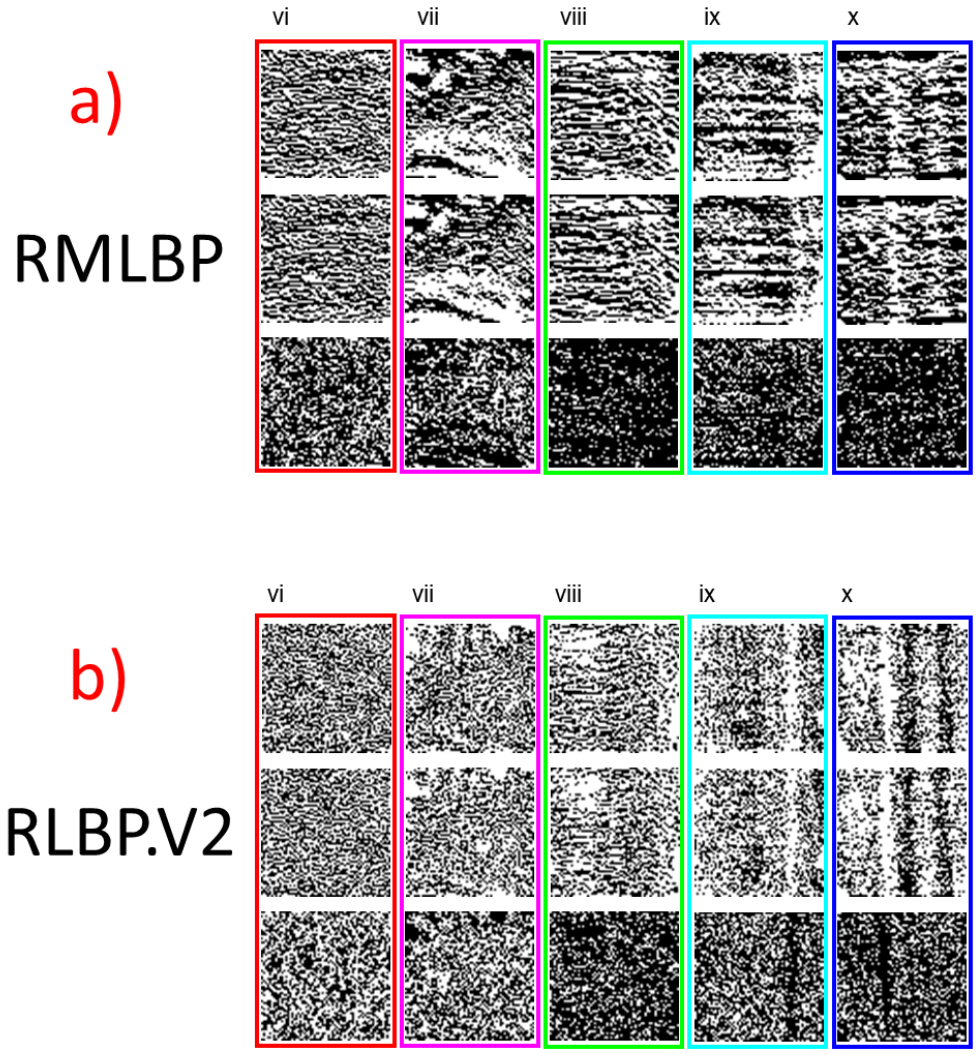

Figure 6.6: For both sub figures the top row represents the fingerprints generated from the Group 1 QD-PUFs on the day of their creation. The middle row represents the fingerprints generated from the same QD-PUF 14 days later. All fingerprints were generated at R=5.The bottom row represents the XOR of the top an bottom row, showing the pixels that are different between the two. vi-PMMAPLMA, vii-PMSPLMA, viii-PSPLMA, ix-PVDFPLMA and x-SEBSPLMA. a) Fingerprints generated using RMLBP. Percentage difference between day 1 and day 14 fingerprints: vi-36%, vii-32%, viii-13%, ix-23% and x-15%. b) Fingerprints generated using RLBP.V2. Percentage difference between day 1 and day 14 fingerprints: vi-51%, vii-48%, viii-24%, ix-36% and x-28%.

Building on the postulation that the addition of PLMA has led to smaller scale detail in the fingerprints we have figure 6.6a. When compared to figure 6.2a we can see that

the fingerprints now show much finer grain patterns. Quantitatively this is supported by the lower inter hamming standard deviations reported in figure 6.7c. PSPLMA, PVDF-PLMA and SEBSPLMA all show relatively low percentage differences between their first and final days (no direct comparison to Group 1 can be drawn here due to lack of data on matching days). However, once again they display no correlation between this difference and change in PL. A feature of commonality that can be drawn with Group 1 for RMLBP however is the lack of any clear features present in the difference maps, showing that any difference is due to noise.

PMMAPLMA and PMSPLMA are both outliers over the entirety of Group 2. This will be addressed here to save further repeating. In all cases the percentage difference between their first and last fingerprints, their intra hamming distances between these two and their FPRs at these values are anomalously high. Namely that they are the only two that have these values higher than their Group 2 counterparts. This is despite in figure 6.6, for both RMLBP and RLBP.V2, their fingerprints appearing almost identical. This has arisen because of a misalignment in the image taken on day 14 of each of these QD-PUFs. It is only a few pixels of horizontal translation but this is enough to significantly worsen the intra hamming distance and percentage change between the fingerprints on day 1 and day 14. For example when we look at the percentage difference between day 1 and day 8 for PMMAPLMA for the same RMLBP radius, we see a percentage difference of 15%. Which is line for what we see for PSPLMA at 12% under the same conditions, thus, highlighting the error.

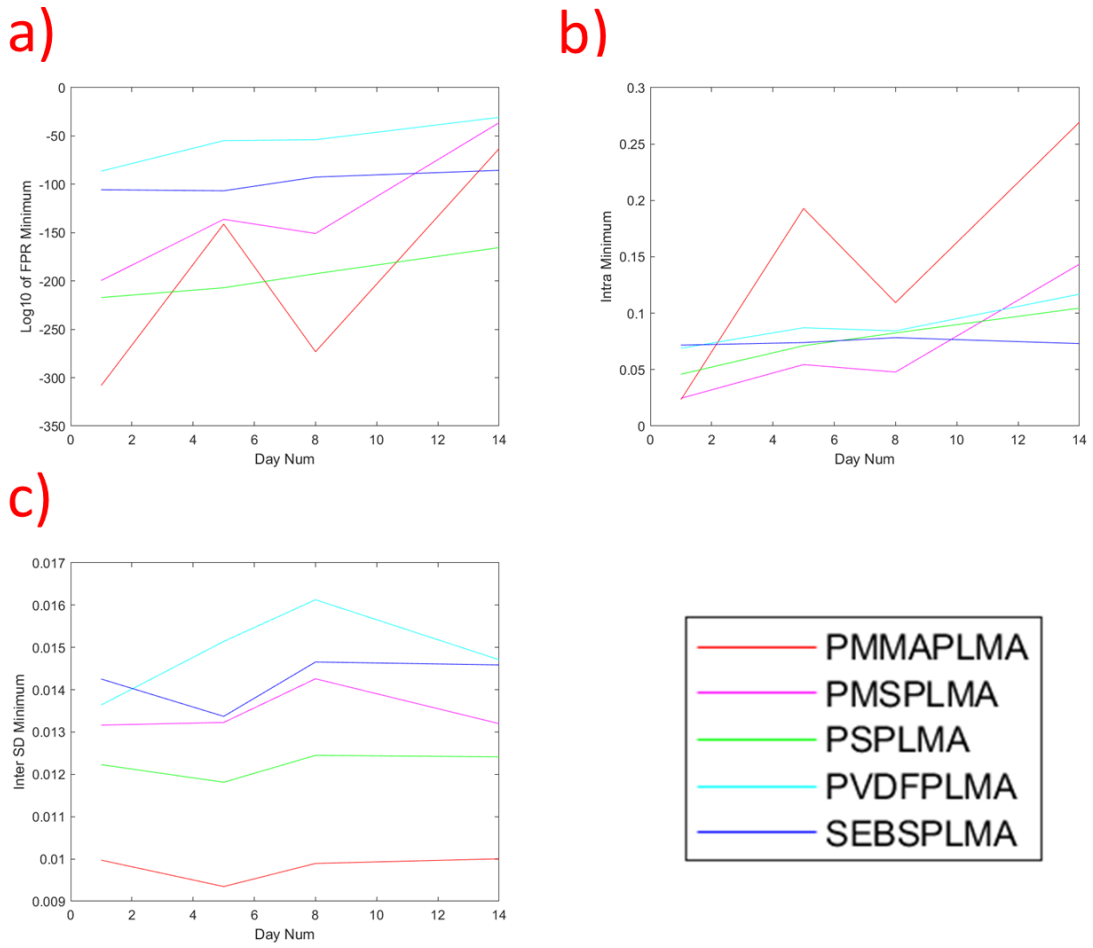

Figure 6.7: a) Graph of the minimum FPR at each day achieved for each of the Group 2 QD-PUFs generated using RMLBP. b) Graph of the minimum intra hamming distance at each day achieved for each of the Group 2 QD-PUFs generated using RMLBP. c) Graph of the minimum inter hamming distance standard deviation at each day achieved for each of the Group 2 QD-PUFs generated using RMLBP. Note: the minimum for each day is the lowest value reached for that figure of merit for radii between 1 and 20. This R value may not be consistent between days or figures of merit. Any values that fell below MATLABs precision of 10^{-308} were set to a value of 10^{-308} for plotting.

As expected, the intra hamming distance of each QD-PUF worsens with time. Albeit, in keeping with the different PL decay, not in the same manner as for Group 1. Although it may be due to requiring more data, there is no longer a clear logarithmic curve that can be fit with a sufficient goodness of fit to this data. Regardless, as already discussed the difference in fingerprints as time progresses bears most semblance to noise, indicating the signal to noise ratio is still the dominating factor. More evidence to show that although changing PL is causing the fingerprints to change it is not the sole contributing factor to the quantitative measures of this is also present here. All of Group 2 show a significantly reduced decay in PL. The fact that the the images taken of them change so little in signal to noise ratio is a key factor in why they show a lessened change in intra hamming distance. PSPLMA gives an intra increase of 0.059, PVDFPLMA gives 0.048 and SEBSPLMA gives 0.001. The significant difference in the decay of their PL curves compared to Group 1 (PSPLMA loses 10% less, PVDFPLMA 67% less and SEBSPLMA

60% less) likely makes the changing signal to noise the dominating factor. When we compare within Group 2 though where the PL loss percentages are much closer in value their is no direct correlation with intra hamming distance change.

With the exception of PMMAPLMA and PMSPLMA for already discussed reasons, we see that this lessened change in intra hamming distance is reflected in the change of authentication accuracy as the QD-PUFs degrade. Overall the QD-PUFs show little appreciable change in their inter hamming distance standard deviation over the time tested, thus making the intra hamming distance the dominant factor. Thus, showing that the increased PL stability leads to being able to accurately use these QD-PUFs in a long term use case scenario.

Despite similarities between Groups 1 and 2 in terms of initial starting intra hamming distance we see that initial FPRs in all cases but PVDFPLMA are lower in Group 2. This stems from the change seen in the texture of the quantum dot patterns, which has in turn lead to lower inter hamming standard deviations for RMLBP. PVDFPLMA shows a higher FPR and inter standard deviation but with a lower intra hamming distance, suggesting a trade off of uniqueness for repeatability. Which given PVDF's much higher intra hamming distance values is easily argued to be an acceptable trade. Overall then this indicates that for RMLBP, the addition of PLMA as a co-polymer is beneficial to authentication accuracy, owing to the effect it has on the quantum dot pattern.

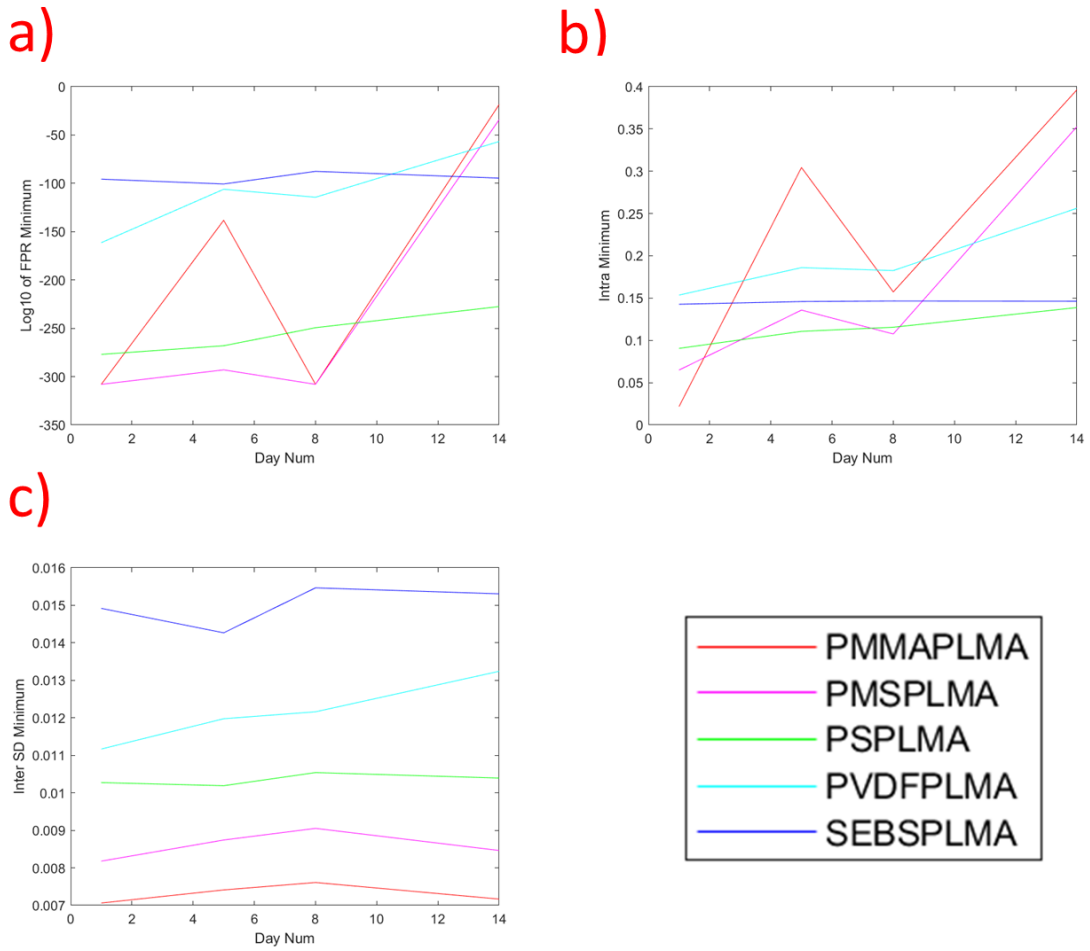

Figure 6.8: a) Graph of the minimum FPR at each day achieved for each of the Group 2 QD-PUFs generated using RLBP.V2. b) Graph of the minimum intra hamming distance at each day achieved for each of the Group 2 QD-PUFs generated using RLBP.V2. c) Graph of the minimum inter hamming distance standard deviation at each day achieved for each of the Group 2 QD-PUFs generated using RLBP.V2. Note: the minimum for each day is the lowest value reached for that figure of merit for radii between 1 and 20. This R value may not be consistent between days or figures of merit. Any values that fell below MATLABs precision of 10^{-308} were set to a value of 10^{-308} for plotting.

For reasons already discussed PMMAPLMA and PMSPLMA will not be covered here in reference to figure 6.6b. The remaining fingerprints generated by RLBP.V2 do show interesting changes over the time frame they were tested however. First of all there is the difference between RMLBP and RLBP.V2, although the percentage differences for RLBP.V2 do show significant improvement they are still much higher than their RMLBP counterparts. Thus, showing that even with a reduced loss of PL, RMLBP will always outperform RLBP.V2 in terms of producing repeatable fingerprints. A fact supported by comparing the intra hamming distances of the two. The fingerprints generated by RLBP.V2 also show clear features created by the vertical lines that originated from printing artefacts in PVDFPLMA and SEBSPLMA. This is to be expected given that RLBP.V2 is a contrast based fingerprinting scheme, it is however an issue as these impose areas of low entropy onto the fingerprint. A fact reflected by the increase in inter standard deviation between these two and their Group 1 variants. In fact SEBSPLMA even displays a higher value than the fingerprints generated by RMLBP. Therefore, highlight

that although in general RLBP.V2 produces higher entropy fingerprints the presence of anything non-random in the quantum dot pattern has a distinct influence on the output.

As expected RLBP.V2 shows a higher set of intra hamming distance values than RMLBP. Interestingly however it also shows in three out of five cases a higher intra hamming distance than Group 1 variants. Only PMMAPLMA and PMSPLMA show a decrease in their initial intra hamming distances. Although this is similar to the scenario with RMLBP the magnitude of the differences is greater, showing around a 1.5 times increase. This would be cause for concern but for the fact that the three whose final intra hamming distance we can comment on (which are also the three that display a higher initial intra) all are lower than the same day for their Group 1 counterparts. The enhanced stability of Group 2 has balanced out the higher noise sensitivity of RLBP.V2 to an extent. Although the initial values may be higher, what is important is the intra hamming distance that they stabilise at.

This is a matter that is reflected in the FPRs for Group 2 (bar the two outliers), each show a higher initial FPR but a lower one at day 14. Showing us that the type of pattern that the addition of PLMA as a co-polymer creates is worse for RLBP.V2 in terms of generating fingerprints for accurate authentication. The enhanced stability however, again provides a useful trade off. As with Group 1 we see that the final PL generated by RLBP.V2 is lower than that of RMLBP. Showing that once again, further data would be useful to confirm if RLBP.V2 stabilises at a lower value. Given the higher PL stability of Group 2 this is more likely and despite the fingerprints showing a lower repeatability this would allow for more accurate authentication than RMLBP.

A matter that is of interest is of SEBSPLMA. Overall when calculating the PL percentage difference it shows, we find that it has a PL decrease of 0%. This is only surpassed over both groups by PMMAPLMA which shows a PL increase of 3% (either as a outcome of a non-optimal fit or due to the lacquer not being properly cured on the first PL measurement). For both RMLBP and RLBP.V2 SEBSPLMA shows the lowest change in figures of merit. Showing an increase in FPR of 20 and 1 orders of magnitude for RMLBP and RLBP.V2 respectively. As well as an increase in intra hamming distance of 0.001 for RMLBP and 0.003 for RLBP.V2. In both cases a mere fraction of the next lowest (0.059 for RMLBP and 0.047 for RLBP.V2). Although the values its figures of merit do not stand out, often being the middle of the pack, they are still well within requirements. Thus, it can be argued that SEBSPLMA is the optimal candidate for the polymer composite with which to produce long term usage QD-PUFs. In such a matter as this stability is more important than performance.

Within Group 2 we have found a universal improvement in the stability of CQDs with the addition of PLMA as a co-polymer. Improvements in PL stability have lead to dividends with the improvement of fingerprint figures of merit. There is however, still no clear link between the magnitude of change in PL and the change seen in such figures of merit. Once again the PVDF containing QD-PUF showed the worst PL stability. This time however SEBSPLMA and PMMAPLMA showed the most stable PL, suggesting an enhanced compatibility with the InP/ZnS CQDs when PLMA is added. Although RLBP.V2 has once again shown lower FPRs than RMLBP and the usage of a QD-PUF like SEBSPLMA should counteract the algorithms noise sensitivity, it should be noted

the conditions in which this data was taken. Compared to many practical settings the apparatus used here was a far more controlled environment. As such if, for example, the images were taken on a mobile phone instead, the extra camera noise may cause a drastic increase in the intra hamming distances generated with RLBP.V2 (as discussed in section 4.2). Thus, limiting it once again to more controlled environments. RMLBP whilst showing lower authentication accuracy would therefore be more useful given its higher degree of robustness.

6.3 Concluding Remarks

The key issue facing QD-PUF being used in long term practical settings is photoluminescence degradation due to oxidization. Within this chapter we have catalogued the photoluminescence behaviour of five different single polymer matrices in which were suspended InP/ZnS colloidal quantum dots. The data gathered from this clearly demonstrated the effect of the oxidization on PL. Though each QD-PUF tested in this group had a PL that stabilised above the background count, each suffered a loss in PL from their initial value. With the lowest loss being the QD-PUF containing PS at 20% and the highest, PVDF, at 80%.

To address the issue of these losses a second group was tested which used the same five polymers only with the addition of PLMA as a co-polymer. PLMA was well suited for this task and indeed reduced the oxidization of the CQDs suspended within it when used as a co-polymer[60]. The worst PL loss in the second group was PVDFPLMA at 13%, lower than even the best of Group 1. PMMAPLMA from Group 2 appeared to gain a 3% increase and SEBSPLMA's PL remained unchanged thus, clearly addressing the issue of PL degradation in long term QD-PUF applications.

The QD-PUFs require fingerprints generating from them in order to be used for authentication purposes. As such the stability of the fingerprints is as important as that of the QD-PUFs PL. In all cases, both Group 1 and 2, there is no link between the accuracy of authentication or the repeatability of fingerprints and PL. To expand further upon this it was shown however that change in these figures of merit was indeed however caused by the changing PL. As the reduction of PL causes the signal to noise ratio of the QD-PUF images to decrease thus, furthering challenge images on later days from their day 1 reference counterparts. The degree to which this occurs however, appears to not solely be affected by the magnitude of the particular QD-PUFs change in PL. Where the change in PL is similar, there is no discernible link between change in PL and change in fingerprint figures of merit (such as comparing within Group 2). When there is a large difference between PL changes (such as between Groups 1 and 2) their does appear to be a correlation. It is hypothesised that the factor that influences this change alongside the PL is the texture of the quantum dot pattern, as it has been shown that this does affect a QD-PUFs robustness against noise. An interesting point of note is that the addition of PLMA as a co-polymer changed the texture of the quantum dot pattern significantly. In most cases adding more fine grain detail. To quantitatively analyse the effects of texture on the robustness would be an interesting topic of further study as one would have to first be able to classify the different textures. Whilst this would be a significant feat of texture analysis it would arguably be worthwhile in order to allow for the comparison of

many different textures.

RMLBP and RLBP.V2 both encode the information within a quantum dot pattern to produce a fingerprint in distinctly different ways. This makes each of them suited best to different use case scenarios than the other. This remains the case when looking at QD-PUF degradation. As expected RMLBP is less affected than RLBP.V2 with the reduction of the signal to noise ratio from the QD-PUF images. When coupled with the reduced degradation of Group 2 (in particular SEBSPLMA) this makes RMLBP well suited for long term authentication applications with QD-PUFs. Although it's authentication accuracy is less than RLBP.V2 it is still well below the required limit and when discussing degradation stability is more important than performance. It is not to say RLBP.V2 is without merit. With the use a a highly stable QD-PUF and controlled imaging environment (such as within a customs office or identity card scanner) its higher entropy fingerprints could be harnessed for higher security applications.

Chapter 7

Behaviour of QD-PUFs Under Varying Wavelengths of Incident Light

Throughout the chapters preceding this one the quantum dot patterns analysed have all been excited with light passed through a short-pass filter. As such, although it does not feature the entire visible spectrum, it still contains a wide bandwidth of wavelengths. Extensive work has also been performed to show that a white light source (such as the flash from a smartphone) can be used to excite the QD-PUF to a degree that a response can be measured[7][6][62]. The key point of commonality here though is only one challenge is being used to excite the QD-PUF and one response is being returned each time. In other words in their current authentication process the QD-PUFs only produce one challenge response pair, making them what is known as a "weak PUF"[31].

This is not to say that weak PUFs are not useful. Strong PUFs which produce many challenge response pairs are generally deemed to be more secure[29], and can be used to generate other cryptographic measures such as encryption keys[32]. Weak PUFs however are useful in anti-counterfeiting as discussed and in cases where a unique identifier is required such as passports[32]. Weak PUFs also tend to be easier to interrogate, requiring less specialised equipment as demonstrated in chapter 4 and Fong et al[6].

This chapter aims to improve upon the security of the QD-PUFs with the demonstration of a process in which the number of challenge response pairs generated is increased, whilst still maintaining the ease of use that the QD-PUFs currently possess. Quantum dots do not possess a linear response to changing wavelength of incident light[12]. As shown in figure 2.3, the absorbance of quantum dots is dependant on the wavelength incident upon them. As has already been discussed in previous chapters the electronic states of quantum dots shift when deposited on to a substrate due to inter cluster interactions. The hypothesis that forms the foundation of this chapter is that if this also affects the photoluminescence excitation spectra (PLE), then the PLE over a whole quantum dot pattern will not be homogeneous. Thus, different areas of the pattern will change in brightness at different rates as the incident wavelength is varied. This will cause the fingerprint generated at different wavelength intervals to appear different, thus allowing for different challenge response pairs. The changing PLE of quantum dots based on the density of CQD clusters is not unfounded as such matters have been demonstrated, such

as in Artemyev et al[12]. It has not been observed before however, how this will affect a quantum dot pattern deposited onto a substrate that possesses a range of different CQD cluster densities. The practical applications of such a phenomena have also not been explored, especially in the form of QD-PUF fingerprints.

This chapter will break down the proposed hypothesis into two parts to provide a thorough testing of it. The first, covered in section 7.2 analyses whether or not the PLE of a quantum dot pattern is indeed inhomogeneous over the entire sample. The second part of the analysis, detailed in section 7.3, then analyses the variation in fingerprints generated at multiple different wavelengths for both RMLBP and RLBP.V2.

7.1 Data Capture and Analysis

In preliminary testing the apparatus detailed in figure 3.1 was used to excite and image the QD-PUF samples. However, the long and short pass filters were replaced by bandpass filters in order to achieve the different singular wavelength excitation light required. However, the light source in that set-up proved to not be powerful enough with most of the output blocked by the bandpass filter. As such instead a microscope was used with the set-up detailed in figure 7.1. This allowed for greater greater illumination of the sample and thus, a measurable signal.

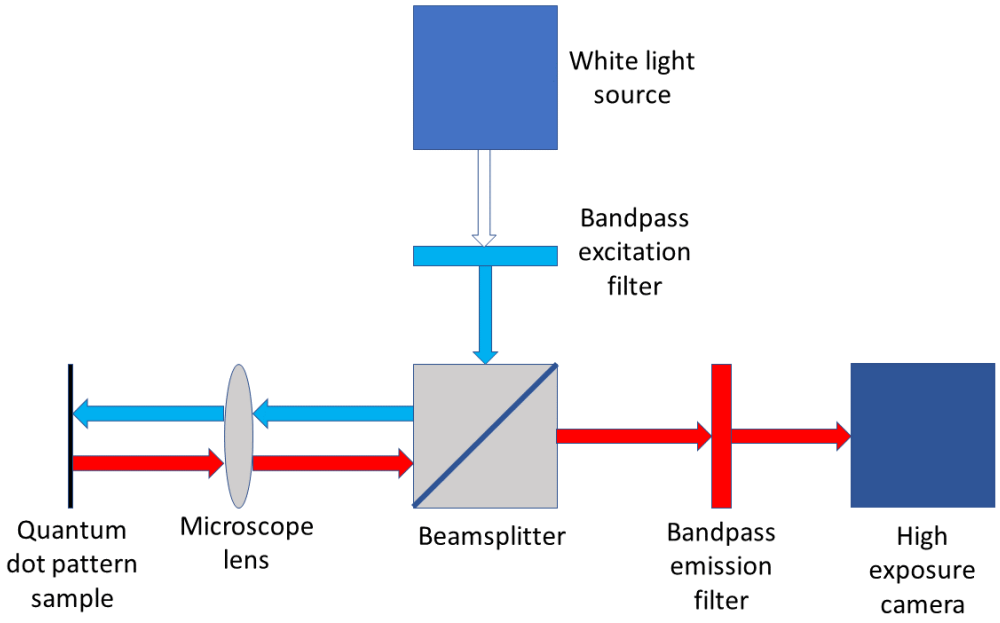

Figure 7.1: Pictorial cross-section of the microscope arrangement used to image the QD-PUFs under different incident wavelengths of light. A bandpass filter is placed in front of the camera with peak transmission as close to the peak emission of the QD-PUF as possible. Varying bandpass filters are then placed in front of the white light source in order to produce excitation light of different wavelengths. Each were chosen such that there is no overlap with the filter in front of the camera. As such only light from the QD-PUF is detected. The magnification of the microscope was set to 10x.

To achieve multiple different excitation wavelengths bandpass filters were used. Although this does not produce a singular wavelength of light, the filters used had a bandwidth of

10 nm to get as close as possible to this. The excitation filters used for the CIS sample were: 440 nm, 480 nm, 510 nm, 530 nm, 550 nm, 580 nm, 600 nm and 620 nm. As the CIS quantum dots have a peak emission at 650 nm, a 650 nm bandpass filter was placed in front of the camera, again with a bandwidth of 10 nm. For the InP/ZnS sample emission intensity has a peak at 625 nm and was lower than that of the CIS QD-PUF. As such as 650 nm bandpass with a 40nm bandwidth was placed in front of the camera instead. Owing to this the 620 nm excitation filter was not used for InPPMMA as it would have resulted in overlap with the camera's filter. It is due to such filters as well that a sample of the substrate of the QD-PUFs was not tested as a control. As the substrate is not photoluminescent and the filter blocks all of the excitation light no signal would have been measured.

The microscope used a ZEISS EC EPIPLAN 10x magnification objective[63] which does not have a uniform transmittance over the wavelengths used (i.e. some wavelengths are absorbed more than others by the lens). As such a mirror was placed where the sample would sit in figure 7.1 and the average pixel brightness of a histogram maximised image calculated for each excitation wavelength. This was then used to calibrate all future images of the samples to remove any effect from the objective.

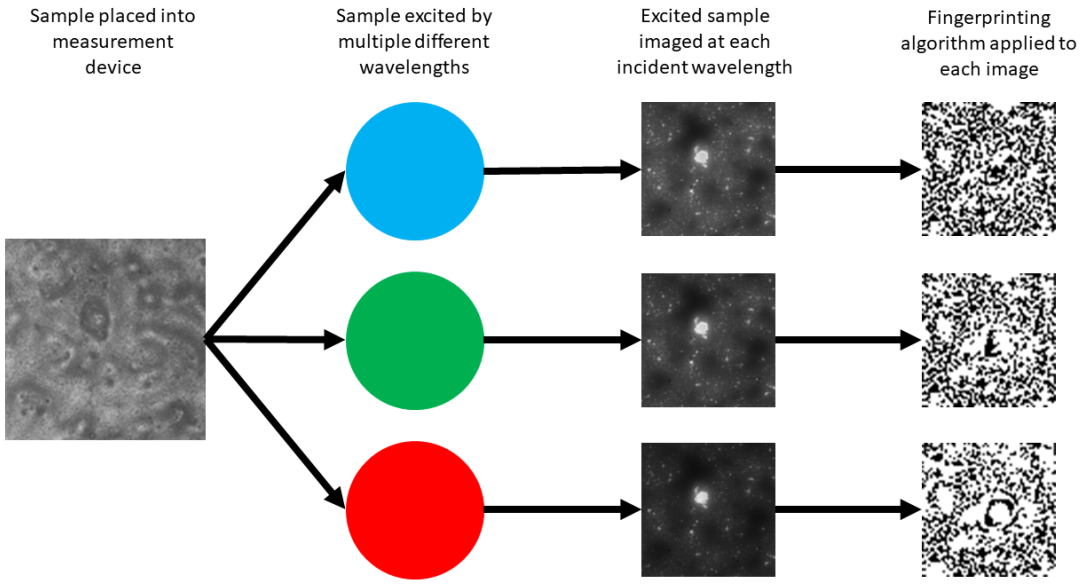

Figure 7.2: Flowchart of the process to generate multiple fingerprints from a single QD-PUF sample. A single sample is placed into the measurement apparatus, the image on the left shows the sample under white light with no filter in front of the camera. The sample is then excited by different wavelengths of incident light and an image captured at each incident wavelength. From this image a fingerprint can then be generated.

As demonstrated by figure 7.2 to capture data a QD-PUF sample was placed within the apparatus, it was then imaged with each of the bandpass filters placed in front of the light source. All imaging was performed in a darkened environment to remove any effects of ambient light. In each case the exposure of the camera used was set such that the intensity histogram of the image spanned the entire available range. For each incident wavelength three repeat images were taken.

For the first part of the analysis the variation of the quantum dots absorption spectra with location on the sample needed to be determined. If we take the brightness of a chosen pixel in the sample image and plot how its brightness varies over each of the progressive images taken at different wavelengths and then apply a fit to it we will get a measure of the absorption spectra of that pixel. Each input image was originally 1000x1000 px in size, this was resized to 900x900 px using the "imresize" function in MATLAB to reduce noise in the image. To the brightness values of each of the pixels the below equation was applied to generate a fitted curve:

$$y = a\,exp\left(-\left(\frac{x-b}{c}\right)^2\right) + d \tag{7.1}$$

The equation itself was chosen as the expected change in the absorption spectra follows an Gaussian decay curve. As the fitting process in MATLAB is an iterative process limits were set on the parameters within the fit equation. These were based on logical reasoning and experience from preliminary testing (e.g. only a could be negative for the curve to have the correct shape and allowing the values to have too large a range led to inaccurate results). The chosen limits were:

- $-1 \leq a \leq 0$, gives the difference between the asymptote and the minima of the curve.
- $0 \leq b \leq 4$, the x-value of the minima of the fit.
- $0 \leq c \leq 4$, gives a measure of the width of the curve.
- $0 \leq d \leq 2$, value of the asymptote of the fit.

As well as this the fits were subject to a pair of goodness of fit tests to ensure that the fitted curves matched well to the data points. The first was a residuals test, the sum of the residuals (the difference between the value of the curve and the measured value) for each point cannot exceed 0.0005. The second was an R^2 test, the R^2 value of the fit must not fall below 0.7. These values were determined empirically by taking a series of random points over several heatmap plots and manually verifying the quality of the fit. The values were chosen to be as strict as possible whilst still allowing for some variation over the heatmap. Any pixel that failed either of these tests had the fit removed and was not included in the final result (shown as a white pixel in the heatmaps in section 7.2). The values of each of the parameters were then plotted in a heatmap for each pixel for each sample tested. If the absorption spectra are indeed inhomogeneous over the quantum dot pattern then the heatmaps will show a change in the value of the fitted parameters. This will also provide insight into what may cause a change in the spectra.

The second part of the analysis focusses on the fingerprints generated at different incident wavelengths. For each sample the same 1000x1000 px area as used in the PLE spectra analysis was used. As per previous chapters the same process was used to generate the fingerprints. RMLBP and RLBP.V2 were used in order to give a comparison between fingerprints generated by the most robust and the most accurate authenticating algorithm respectively. For each sample a fingerprint was generated using each algorithm

at a radius of 10. The fractional hamming distance between each wavelength's fingerprint and the fingerprint generated from the shortest wavelength was then calculated and plotted. This provides a measure of how much the fingerprints vary as wavelength is varied.

7.2 Quantum Dot Pattern PLE Results and Analysis

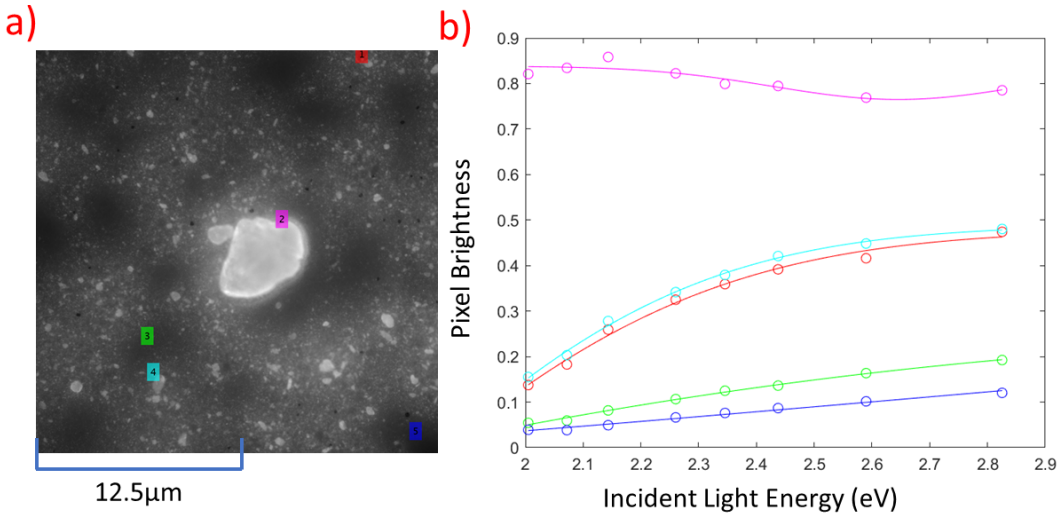

Figure 7.3: a) Image of the CIS QD-PUF sample taken in the apparatus shown in figure 7.1 at 10x magnification. Each number corresponds to a data curve in sub-figure b) and labels the location the data was taken from. b) Pixel brightness of five separate points on the CIS QD-PUF sample with varying incident wavelength of light.

Figure 7.3 serves as a useful first insight into the variation of PLE across a QD-PUF sample, even from just these five point we can clearly see that the PLE does not remain constant over the entire area of the sample. Mirroring findings that we have seen before [12]. It is interesting to note that clearly none of the curves exactly match the shape shown in figure 2.3 but the quality of the fits indicates that they are indeed correct. We can also clearly see that there is consistency in the results found, the two point chosen on QD clusters and the two chosen in low concentration areas show matching curves, despite being widely separated in the image. Furthermore the large central cluster, which appears unlike any other within the image displays a completely different curve. Why these particular variations occur is discussed further on. Overall, this adds a lot of credence to the fact that the measured fits are accurate.

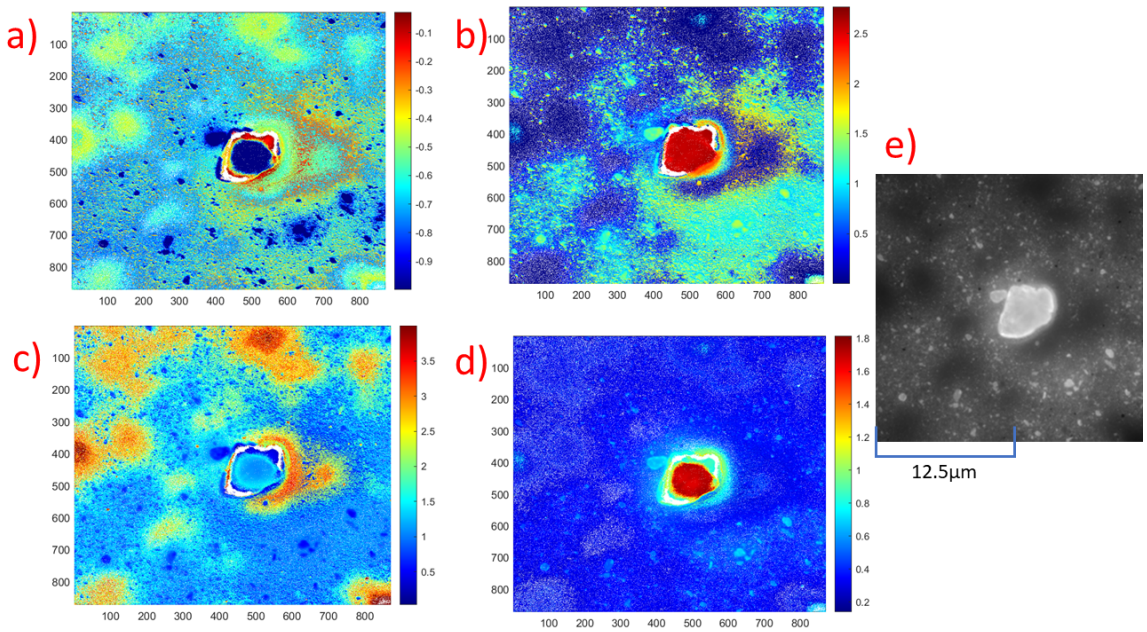

Figure 7.4: a)-d): Heatmaps showing the variation of each of the parameters in equation 7.1 over the area of the QD pattern displayed in sub-figure e). The label of the sub-figure matches to the parameter in equation 7.1 it is displaying. x and y-axis labels are in pixels, the scale is in arbitrary units for a) and d) and in eV for b) and c). This figure displays the results for the CIS sample.

The most obvious result from figure 7.4 builds on the conclusion drawn from figure 7.3b). It is that very clearly none of the parameters are uniform over the entirety of the CIS QD-PUF analysed. Showing that, as predicted, the PLE of CQDs deposited onto a substrate is indeed inhomogeneous. What is most promising is the lack of rejected pixels that can be seen in the heatmaps. This can be seen most clearly in figure 7.4d. This is a clear indicator that the vast majority of the fits applied to each pixel passed the goodness of fit tests. As well as this most pixels sit within the ranges chosen for the parameters indicating that the ranges were suitable. This gives us a great degree of confidence that the fittings applied over the wavelength images for each pixel are indeed accurate.

Further information can be gleaned when we compare the heatmaps to the image of the area of the quantum dot pattern that was analysed. For example we can see in figure 7.4a that the clusters with clear definition in figure 7.4e show a value of a below -0.9. Such as the area within $600 \leq x \leq 700$ and $650 \leq y \leq 750$. The fact that these areas are so clearly defined indicates that this is a physical property of these dense clusters. Conversely areas with a much lower density of quantum dots, such as the area within $100 \leq x \leq 200$ and $300 \leq y \leq 400$, all have consistently the same range of values for a, roughly between -0.4 and -0.5. Physically this result is as expected. As the magnitude of a gives a measure of the range between the fit's maximal asymptote and its minima, lower concentration areas will give a lower value of the magnitude of a. As they lack quantum material they will not show the PLE curve expected and the brightness of these areas will instead remain relatively unaffected by changing incident wavelength. This fact is further supported by figure 7.4c. These low concentration areas show the highest values of c, showing that the curves fitted to them are the flattest in the sample area. As they lack quantum material we would expect the pixel brightness of these areas to remain

unchanged, something this value of c is indeed showing. Further supporting this is that the areas with more disperse concentrations of quantum dots than the distinct clusters have values of a and c that are in-between those of these two extremes. The fact that the concentration of quantum dots is affecting the PLE curve gives one of the reasons as to why the PLE is not uniform over the quantum dot pattern.

In some regards the determined value of b in figure 7.4b is as expected. The low concentration areas show values close to 0. As expected when they have fits that are almost flat. The majority of pixels in more concentrated areas also behave as expected. Due to the shape of the PLE curve for CIS quantum dots (see figure 2.3) it is difficult to determine where the minima of it, and so the value of b, should lie. We do know however, that it must be at a greater wavelength than the maximum wavelength used in the range of excitation filters. That is 620 nm or ∼2eV. As we can see in figure 7.4b the more concentrated areas do have b values below that of 2eV, with most being below 1.5eV. This further supports the accuracy of the fits generated as they are agreeing with expected values. The exception to this is the large central cluster which will be addressed shortly. The exact value of b that certain pixels show however appears to have less of a dependence on the concentration of quantum dots than the other parameters analysed. Whilst more concentrated areas are easily distinguishable from the much darker areas in figure 7.4e in regards to each other the values are far more similar. In fact looking at the area between $500 \leq x \leq 700$ and $500 \leq y \leq 800$ we can see some interesting phenomena. The edges of this area show higher values of b than the middle despite visually appearing to have less quantum material in figure 7.4e. This in of itself is of little consequence if not for the fact that the distinct clusters within this area, of which are a higher concentration of quantum dots than the edge areas, show similar values, distinct from their immediate surroundings. This pattern is repeated elsewhere within the sample and suggests another unknown mechanism is affecting the value of b found. Another factor which is contributing to an inhomogeneous PLE over the sample.

Finally we come to the matter of the anomalously large cluster of quantum dots in the centre of the sample area (roughly within $400 \leq x \leq 600$ and $400 \leq y \leq 550$). As we can first note from figure 7.4d it's brightness asymptote is far greater than that of any other cluster within the sample, unsurprising given that visually it is clearly much brighter than the rest of the sample area image. What is most interesting however, is the fact that the parameters within it do not remain uniform like with other clusters. This is most likely due to its size. The relative diminutive nature of other clusters and the resolution of the image not allowing for us to determine variation within them. It's anomalous size also appears to have led to, or at least allowed for the observation of, properties that do not fit with previous observations. Most notably the values of b and c within it are higher than predicted for dense clusters. Indicating a flatter curve than expected as well as significant blue shift. Although the exact mechanisms behind why this occurs is not known the stark contrast of this cluster with the rest of the sample will prove useful for the generation of fingerprints. A likely proposition will be that it is denser than the other clusters and as such this has caused a change in behaviour. To confirm this however, we would need further analysis to quantify cluster density.

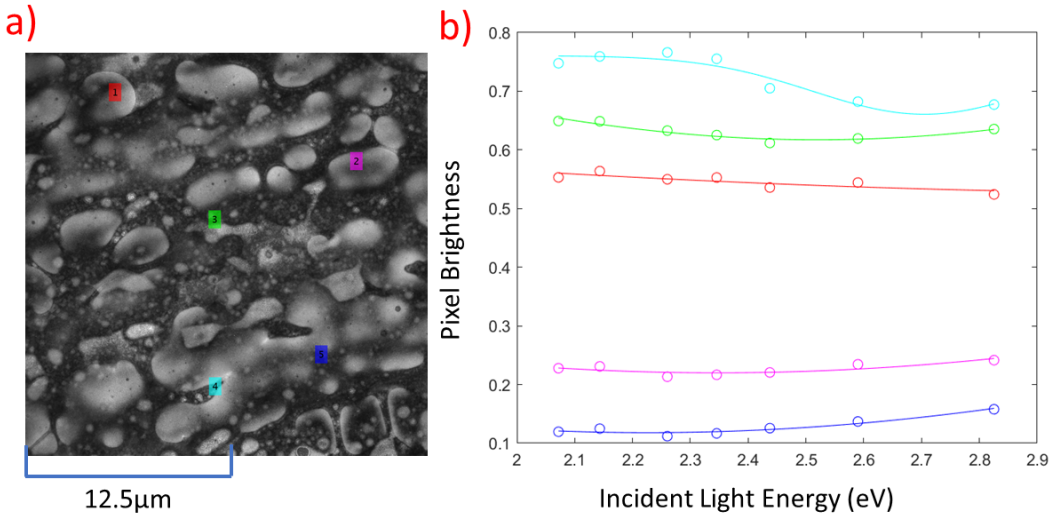

Figure 7.5: a) Image of the InPPMMA QD-PUF sample taken in figure 7.1 at 10x magnification. Each number corresponds to a data curve in sub-figure b) and labels the location the data was taken from. b) Pixel brightness of five separate points on the InPPMMA QD-PUF sample with varying incident wavelength of light.

Figure 7.5 reflects the results seen in figure 7.3. Once again for each of the selected pixels we see that not only do the fits match the data well but there are clear patterns to their shapes. Lines 2 and 5 are each in low concentration areas and is show the same shape curve. Line 4 however, shows a different shape and one that is reminiscent of the predicted PLE curve for InP as shown in figure 2.3. It does display though, a blue shift in the location of its minima from the expected value of 2.24eV. The theorised reasoning for this phenomena is discussed further on. 1 and 3 are also interesting lines to note as, visually, the areas they are measured from are distinctly different and this is reflected in the PLE measured from them.

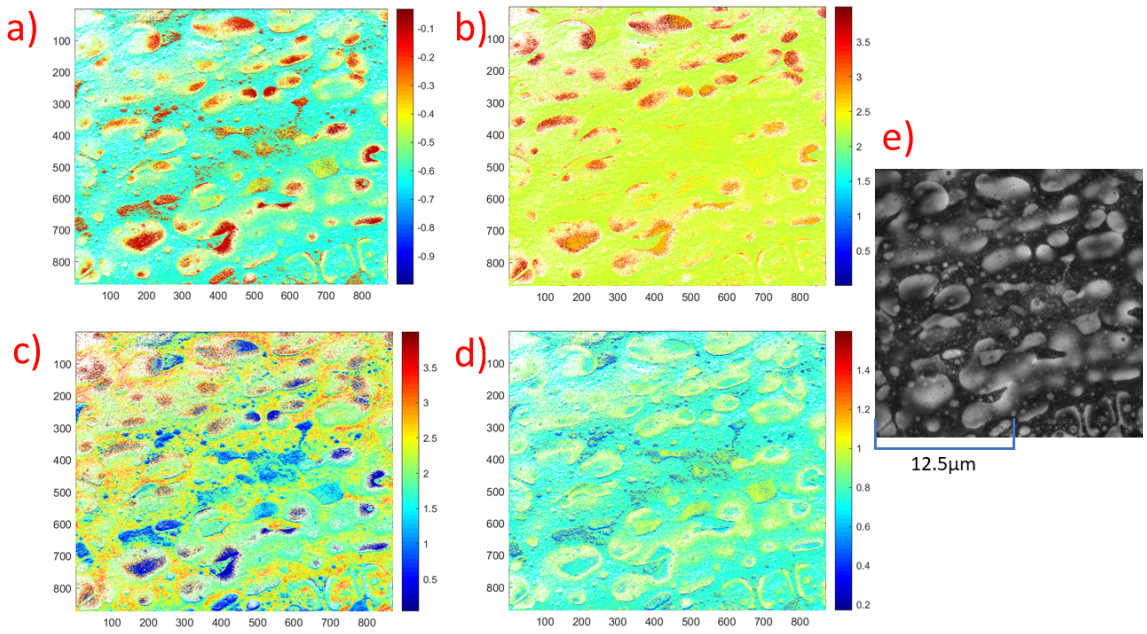

Figure 7.6: a)-d): Heatmaps showing the variation of each of the parameters in equation 7.1 over the area of the QD pattern displayed in sub-figure e). The label of the sub-figure matches to the parameter it is displaying. x and y-axis labels are in pixels, the scale is in arbitrary units for a) and d) and in eV for b) and c). This figure displays the results for the InP sample.

Despite the greatly different PLE spectra the InP sample shows the same overall result as the CIS sample, the PLE of the sample is not homogeneous. Similarly there are also indicators as to the accuracy of the fits that have been applied. Again there have only been a small minority of pixels that failed the goodness of fit tests and the values of the parameters sit within the range with minimal saturation.

In the same manner as the CIS sample we see a clear difference between the areas of higher quantum dot concentration and those with little to no quantum dots present. Unlike the CIS sample however, the areas with a greater concentration show a lower magnitude of a, as can be seen in figure 7.6a. This is not however, contradictory to the results shown in figure 7.4a. As both have very different PLE spectra we would not expect the parameters found in areas of high quantum dot concentration to be the same. Given that the measured PLE for InP, given in figure 2.3, is that of a dip which then increases we would expect the magnitude of the change to be lower than that of CIS which continually decreases. Low concentration areas are more difficult to identify given the more disperse nature of the quantum dot arrangement in the InP sample. We can however, see a clear range of values of a starting with the lower concentration areas at roughly -0.65 and increasing with concentration to -0.15. Indicating, again, the link between the changing parameters and concentration and supporting the concept of an inhomogeneous PLE not just being limited to CIS quantum dots.

The low concentration areas across each of the two samples each show a similar range of values, sitting between -0.45 and -0.65. Whilst this is a fifth of the entire range of a given that higher concentration areas can show a difference of $\sim$0.5 from these areas there is

something to suggest that perhaps this is a consistent range for this parameter over all samples for these areas. Further testing would be needed to confirm this but it could allow for better calibration of the fits by setting the value of low concentration areas. It would also allow for a measure of QD concentration based on the deviation from this value.

To build upon this previous point we can see that in fact there is a link between the distance a pixels a value is from this range of -0.45 to -0.65 and the value of c measured at that pixel. This further supports a point made about CIS, that the higher concentration areas display a lower c value than the lower concentration areas. This is owed to the fact that the lower concentration areas show a much reduced response to the incident light and so would give flat PLE curves with larger c values, as we saw with the CIS sample. Figure 7.6c also provides us with one of the clearest examples of a key difference in the distribution of the PLE variation. The clusters within the CIS sample appear with well defined edges and uniform QD density across them. This is not the case with the InP sample. Even for the structures that appear to have well defined edges and shapes (such as the "dots" scattered throughout the darker areas), closer inspection reveals that internally they are not uniform in QD density. This is reflected in the PLE curves fitted. Take for example the shape between roughly $100 \leq x \leq 250$ and $700 \leq y \leq 750$ in figure 7.6c. It is not easy to match to its counterpart in figure 7.6e as they do not bear the same shape. With the PLE response varying within this grouping of quantum dots. This is certainly not just limited to this area and is repeated across the sample. Further supporting the effects of quantum dot concentration and indicating that the shape and composition of clusters greatly affects how the PLE response is distributed.

One very useful feature of the PLE spectra of the InP quantum dots is the absorption minima at 555 nm or 2.24 eV (as shown in figure 2.3). This distinct dip in the spectra allows us to sanity check the quality of the fits and observe which areas match and which deviate from the expected result. At first glance figure 7.6b seems to indicate that the vast majority of the fits applied to the sample sit close to this value. This is however, misleading. The expected full width half maximum for this absorption dip is $\sim$0.17eV. Comparing between 7.6b and c therefore, we can see that much of the sample matches these two parameters. It appears to be in areas where the QD density is lower, as one would expect as the PLE in figure 2.3 was measured at low concentrations. This greatly supports the accuracy of the this process of extracting PLE spectra from samples on substrates. It also highlights the degree of deviation that we can see from the expected spectra.

Based on the assumption that the more concentrated areas show a values shifted from the centre of the scale and lower c values, it is clear to see that in most cases we see a similar phenomena to CIS, in that these areas appear to be blue-shifted in their value of b compared to less concentrated areas. The repetition of this phenomena across two different quantum dot types would suggest that it is not just a quirk of the fitting process. The exact physical process responsible for this effect is not known. Given its link to quantum dot density however, it could be linked to the effect of ligands on the electronic states within CQDs. More experimentation is needed however to confirm the origin of this effect. Especially as in this sample it does not occur in all occasions that the aforementioned indicators of higher concentration occur. Such as in the central region of the sample we see a higher a value, a lower c value but the value of b is of the expected value.

The only difference between these areas is seen in figure 7.6d with differing values of d.

Throughout this section it has been shown that it is possible to take a measure of the PLE of CQDs deposited onto a substrate. It is also very clear that the PLE spectra of a quantum dot pattern on a substrate does not remain uniform over the entirety of the sample. Variations are introduced through the concentration of quantum dots present and potential other as of yet unknown factors. The distribution of the variation is also highly dependant on the type of CQD being used. As each cluster together in a different manner. In theory this suggests that it is indeed possible to generate differing fingerprints from a single QD-PUF by exciting it using different wavelengths of light.

7.3 Multi-wavelength Fingerprints Results and Analysis

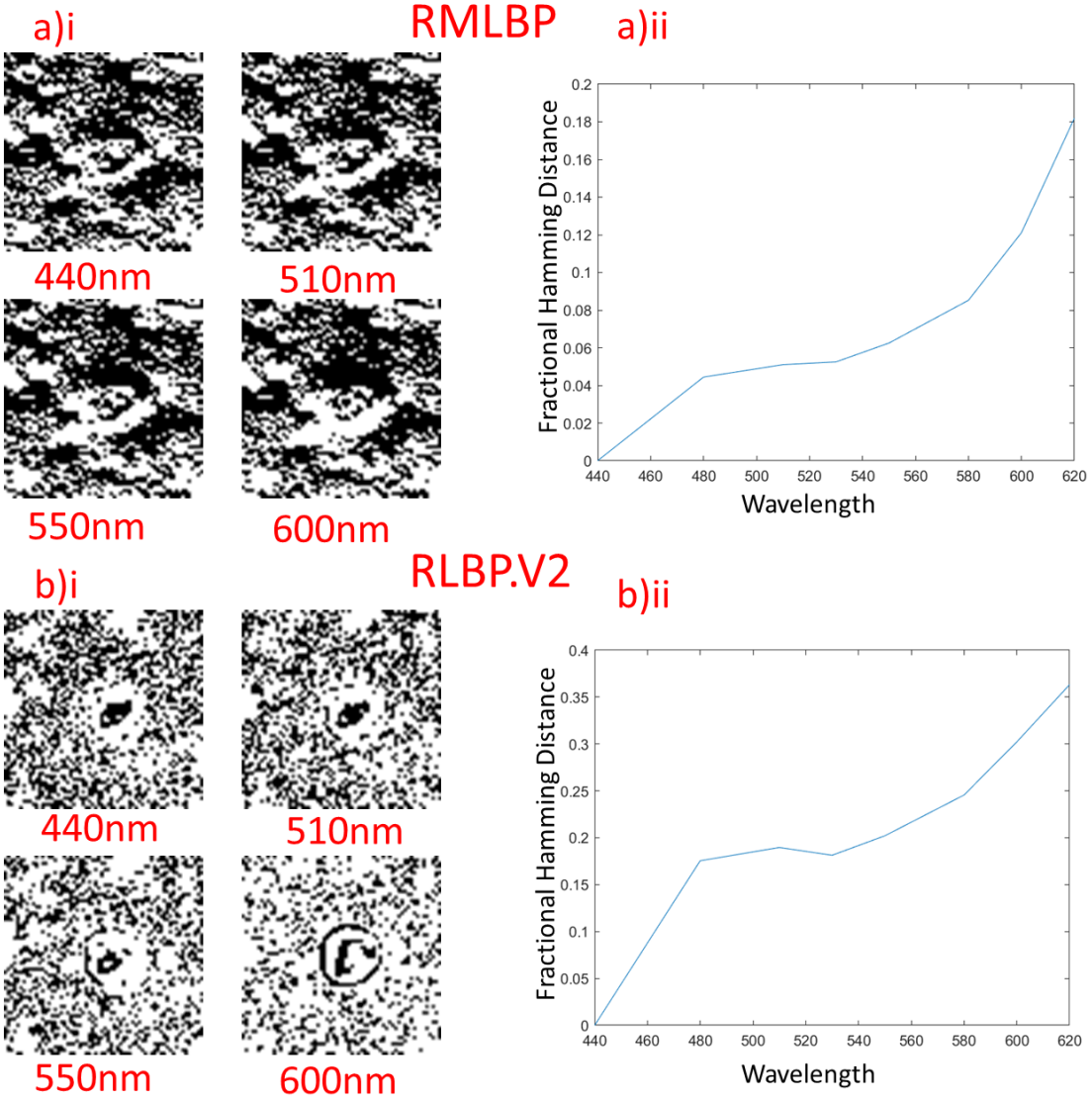

Figure 7.7: Sub-figures labelled a) relate to RMLBP, those labelled b) relate to RLBP.V2. The labelling with Roman numerals is consistent across both algorithms. i - Fingerprints generated at a chosen four of the wavelengths tested. All fingerprints are generated at a radius of 3 and have had the resize step applied to them, making them 64x64 px in size. ii - graph of the fractional hamming distance of the fingerprints generated at each incident wavelength compared to the fingerprint at 440 nm for the CIS sample.

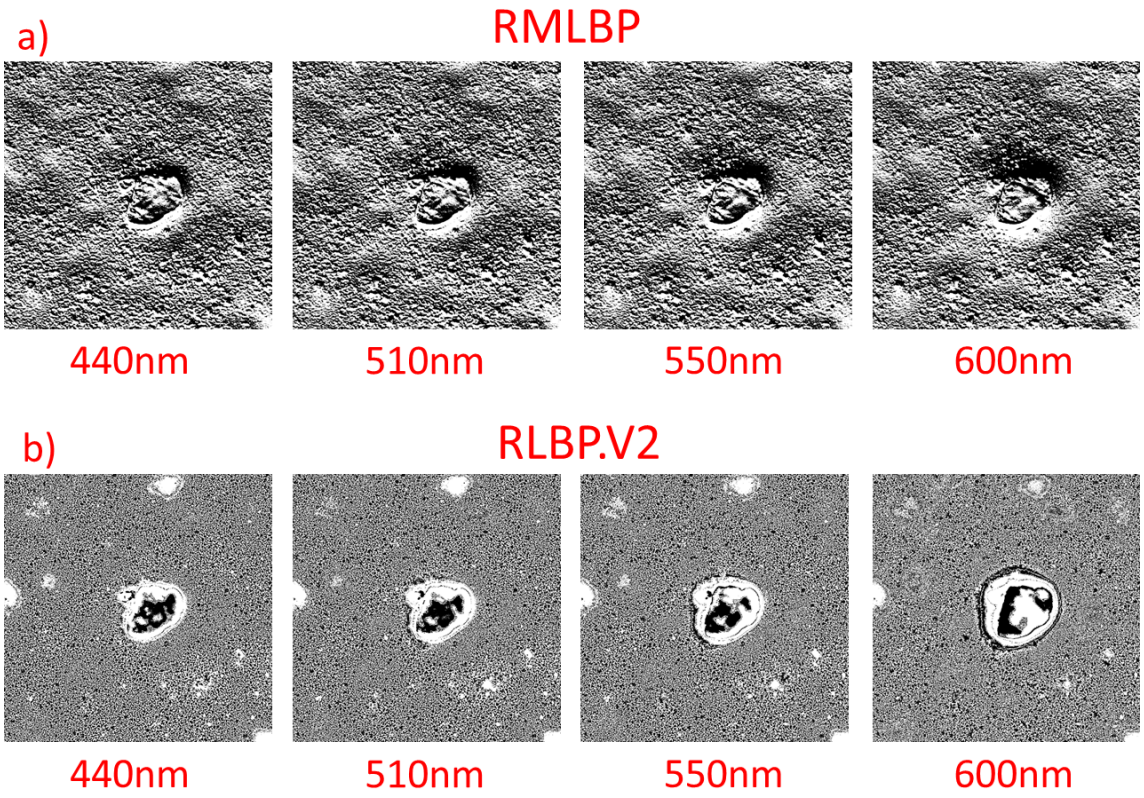

Figure 7.8: Sub-figures labelled a) relate to RMLBP, those labelled b) relate to RLBP.V2. The labelling with Roman numerals is consistent across both algorithms. All fingerprints are generated at a radius of 3 and did not have the resize step applied to them making them 1000x1000 px in size. Each fingerprint was captured at the wavelength labelled beneath it and was generated from the CIS sample.

One of the greatest strengths of RMLBP is the fact that it is robust against small changes in the input image. In this case however it is provably a disadvantage to it. Visually we can see the issue with using RMLBP in the generation of fingerprints at different incident wavelengths in figure 7.7a)i-iv. There is very little change in the fingerprints themselves over the span of the 160 nm wavelength range displayed. The major change is in the central area with smaller areas around the fingerprint also altering in size. This clearly shows that it is primarily only the area around the large central cluster that undergoes any major change. This is reflected in figure 7.8a)i-iv. Where we can see that the only clear variation is in that large central cluster. Thus, the lack of sensitivity in RMLBP makes it unable to determine any significant difference between different wavelength images. The fact that RMLBP determines it's final bit value based on gradient orientation is the reason why this occurs. Such a parameter will likely not change in many cases and will be lost if the radius of the algorithm is larger than the size of the feature that changes.

This is not to say however that with this CIS sample, RMLBP has produced no positive outcomes. It has still demonstrated that variations in the PLE of the input image can be detected, they however have to be large in scale. It also shows that areas with starkly contrasting PLE spectra next to each other produce the most significant change in a fingerprint. To be expected when the fingerprinting algorithms generate their binary strings based on local texture information. A maximum possible difference of 18% of

pixels over the entire range of wavelengths tested is not significant enough to say that multiple challenge response pairs have been generated.

RLBP.V2 on the other hand shows significantly more difference between each of its different wavelength fingerprints. As shown in figure 7.7b)v even the lowest fractional hamming distance from the 440 nm fingerprint is on par with the highest generated by RMLBP. RMLBP's method of encoding the information in the QD-PUF uses the direction of gradients present, highly robust to noise but a property that does not vary as much with incident wavelength. RLBP.V2 on the other hand encodes based on local contrast information compared to the central pixel. Although this is much more sensitive to noise it picks up the changes due to varying PLE much better, twice as good in fact basing it off of the highest hamming distance achieved. Even for the resized fingerprints in figure 7.7b)i-iv we can visually see change as the incident wavelength increases. Though the shift in bias, due to the low concentration areas decreasing in brightness compared to the clusters, would be an issue in regards to inter hamming distance standard deviation during authentication. Although each fingerprint is clearly not a distinct challenge response pair, this has still demonstrated that significantly different fingerprints can be generated from a single QD-PUF.

Figure 7.8b)i-iv gives an interesting texture map of how RLBP.V2 sees the input image as it changes with incident wavelength. It serves as further evidence that the different regions of the sample are not changing uniformly as the wavelength increases. The central cluster clearly undergoes significant and non-uniform change, as reflected by its fit parameters in figure 7.4. The smaller clusters can also be seen along the bottom right and in fact two of the low concentration areas are highlighted as their relative brightness to their surroundings varies. Unfortunately however, this highlights an issue with this process. The majority of this detail is lost in the resize step. Unfortunately though this step is needed in order to make the fingerprints noise free enough for authentication to be viable. Therefore either larger features or greater magnification are needed.

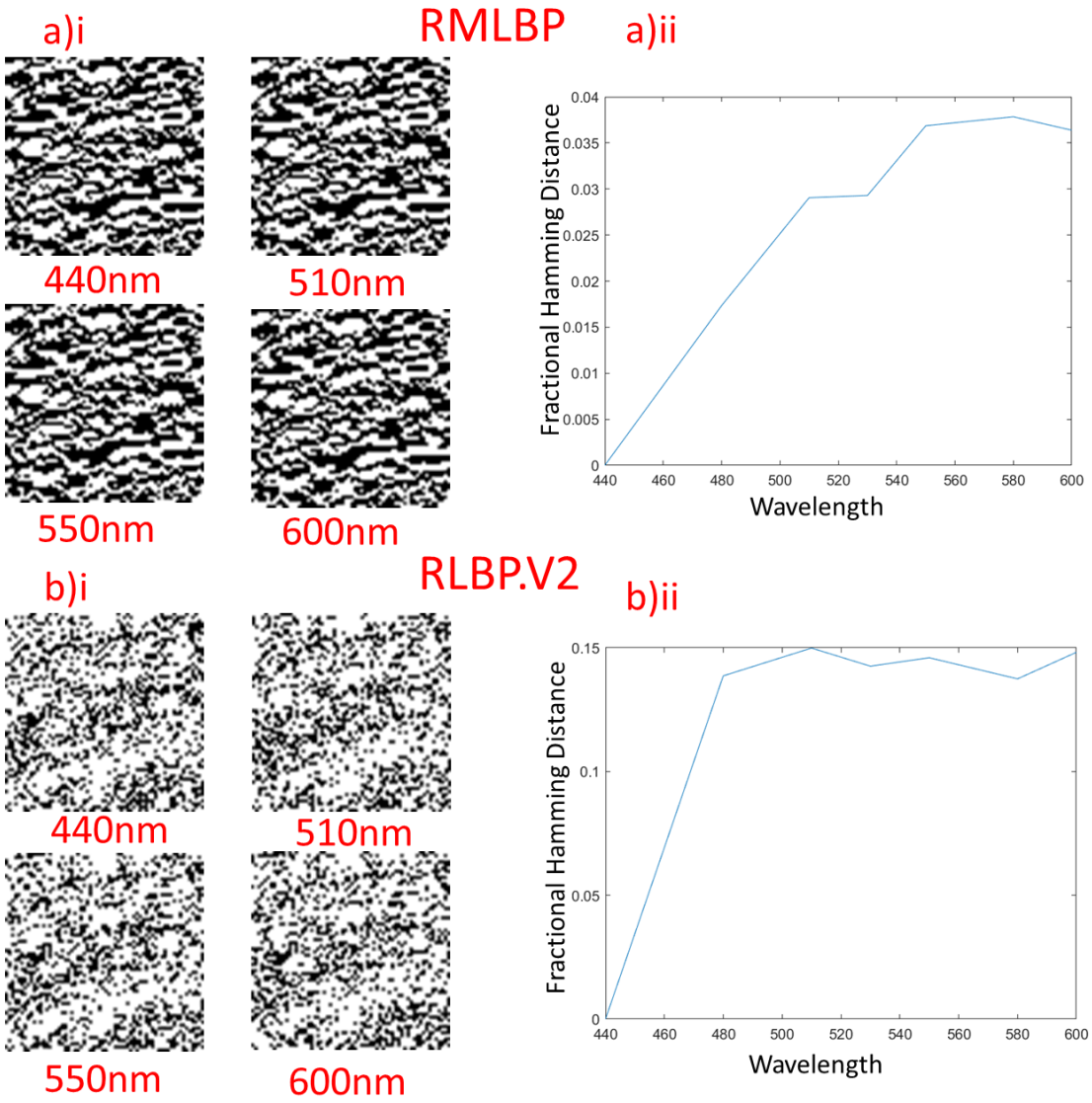

Figure 7.9: Sub-figures labelled a) relate to RMLBP, those labelled b) relate to RLBP.V2. The labelling with Roman numerals is consistent across both algorithms. i - Fingerprints generated at a chosen four of the wavelengths tested. All fingerprints are generated at a radius of 3 and have had the resize step applied to them, making them 64x64 px in size. ii - graph of the fractional hamming distance of the fingerprints generated at each incident wavelength compared to the fingerprint at 440 nm for the InP sample.

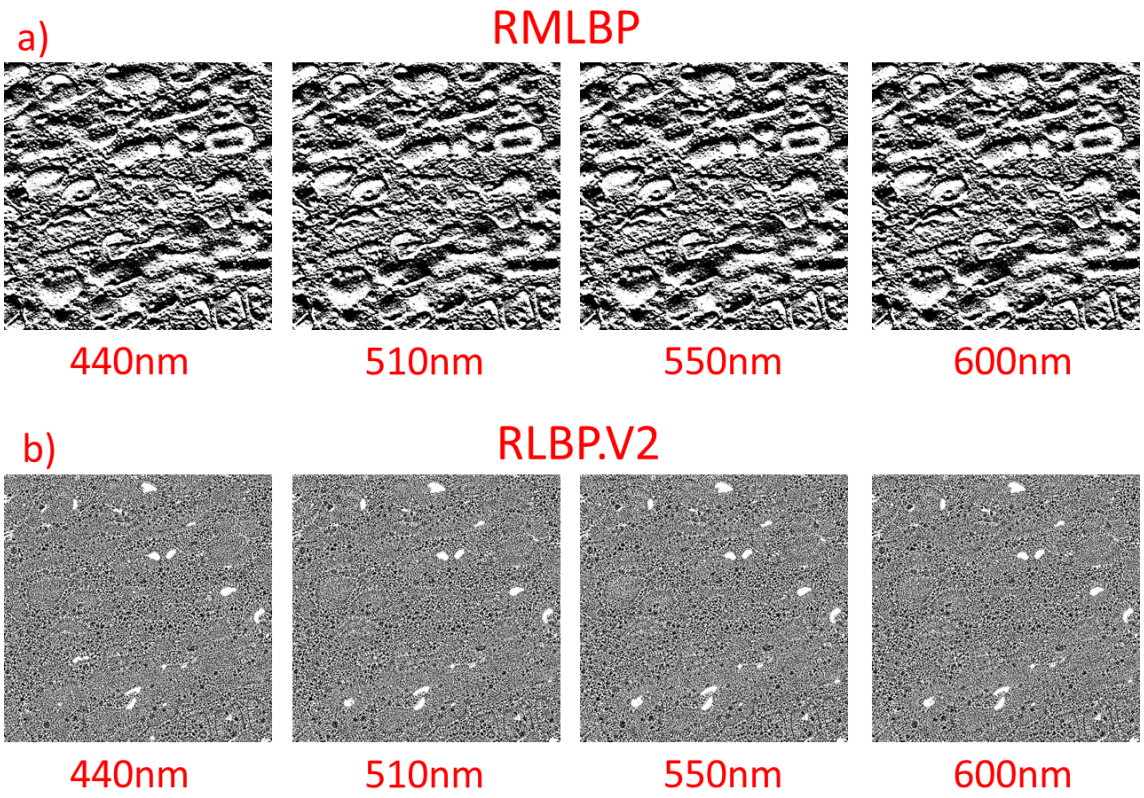

Figure 7.10: Sub-figures labelled a) relate to RMLBP, those labelled b) relate to RLBP.V2. The labelling with Roman numerals is consistent across both algorithms. All fingerprints are generated at a radius of 3 and did not have the resize step applied to them making them 1000x1000 px in size. Each fingerprint was captured at the wavelength labelled beneath it and was generated from the CIS sample.

Given the determination that RMLBP cannot differentiate the minor changes between incident wavelength images as well as its contrast based counterpart and the fact that starkly differing areas of PLE produce the best response in the fingerprint it is of little surprise at the performance shown in figure 7.9a)v. As discussed in section 7.2 InP does not show the clearly defined areas of PLE spectra and instead changes gradually from one value to another. This matter unfortunately means that there is very little variation in its fingerprints generated with RMLBP. With even the highest hamming distance below just 4%. This is not an issue born of the resizing step destroying detail either, as we can see in figure 7.10a)i-iv that there is little to no variation before the resize step is applied. Whilst this is a disappointing result it does confirm two criteria required for differing fingerprints to be generated from a single QD-PUF. There must be large clusters with distinct boundaries and a contrast based fingerprinting algorithm will give the highest variation.

This is a conclusion solidified by figure 7.9b)i-iv. Which gives fractional hamming distances roughly five times greater than that generated by RMLBP. It however does not achieve hamming distances as great as even the lowest as that for the CIS sample. Thus, showing the limited usefulness of a sample such as this for such an application. Looking to figure 7.10b)i-iv we can see that some change has indeed be detected despite the limitations of the sample. The areas that change corresponding with areas of low c, a fact reflected too in the CIS sample, as these areas undergo the most variation over the

tested wavelengths. They are however in this case too small to have any great effect on the resized fingerprints.

From the experiments performed in this section it is clear that the fingerprints generated from QD-PUFs do indeed change when the wavelength of incident light is varied; there are however, some caveats to this. In order for the most change to appear in a fingerprint we require large areas of uniform PLE response (such as the clusters in CIS) set against a highly contrasting background. The latter in its simplest form would be a low concentration area of quantum dots, as these appear to have the largest difference with the higher concentration areas. As the fingerprinting algorithms compare relative brightness levels in the local area, in one manner or another, this would make the local area appear different at each wavelength. On the topic of fingerprinting algorithms it is very clear that the robust nature of RMLBP makes it too insensitive for use in the generation different wavelength fingerprints. A contrast based algorithm such as RLBP.V2 is required in order to pick out the subtle changes in the brightness topography.

7.4 Concluding Remarks

Although it would have been preferable within this chapter to see each QD-PUF produce a distinctly different fingerprint at each wavelength tested it is not to say that this experiment has not yielded useful results. It serves as a proof of concept for the idea of generating multiple CRPs from a single QD-PUF. It has highlighted the limitations of the concept as it stands and the criteria required to improve upon it moving forwards.

The first point that is clear is that as predicted in section 2.1.4, is that the PLE spectra of a quantum dot pattern is not homogeneous. It is also possible to measure the PLE of quantum dots deposited onto a substrate using apparatus such as that show in section 7.1. Although the accuracy of this method would require further experimentation to quantitatively measure; it cannot be denied that this is both a simpler method than what is currently employed and allows for the analysis of the PLE of CQDs outside of solution.

Furthermore, the matter of inhomogeneous PLE raises interesting further experimental avenues. It is not currently completely clear why the deposition of CQDs onto substrate causes a change in the PLE spectra. The current theories surrounding the effects of CQD concentration in clusters and ligand bond altering electronic states require further experimentation to confirm[12]. Such matters are beyond the scope of this paper as the aim was simply to demonstrate the presence of such variation. Another interesting avenue of experimentation would be to optimise the quantum dot pattern to create as clear a change in spectra as possible. It has been made clear that the areas of variation in PLE are small in scale. The InP sample tested gave areas of varying PLE too small to influence a fingerprint generated from an image of the sample. On the other hand the CIS sample with a large central cluster did produce a significant variation in generated fingerprints. The surrounding clusters however, failed to influence the final resized fingerprint to the same extent. Indicating that to generate fingerprints that vary with wavelength a minimum size of features are needed. Further research into what this size is and the effects of magnification would make QD-PUFs suited to this task a reality.

As has been mentioned, fingerprints generated from different wavelength images are different from each other, not to the extent however that they are distinct from each other. They could still however be used in authentication. The user of the QD-PUF would image the sample under different wavelengths. Then requiring that each of them match to a reference fingerprint generated under the same wavelength would add a second layer of security. Although each are only subtly different they are still different. A simulated attack, such as a photograph of a QD-PUF would not respond to the varying incident wavelengths in this manner.

The fingerprints levels of entropy could also be improved upon. By using them as random sources one could apply fuzzy extraction techniques to them[38][64]. This would generate a uniformly random response from the fingerprint that is highly dependant on the input. As such the proximity in hamming distance each wavelength's fingerprint possesses would be immaterial as the outputs from this step would be unique to each other. There are drawbacks to this approach though, as it is highly influenced by noise this may pose practical problems in implementation. An alternative would be the application of a debiasing technique (as detailed in section 5.2), although they do not provide as much separation as fuzzy extractors they are less noise dependant. As such despite the result of this chapter not being as expected a great deal of promise is shown.

Chapter 8

Concluding Remarks and Further Work

8.1 Concluding Remarks

The aim of this thesis was to demonstrate that QD-PUFs could indeed be harnessed using fingerprinting algorithms and to explore what is possible with them. In order to achieve this we first analysed the performance of four fingerprinting algorithms. Two of which employed a gradient based encoding method, the simplistic RLBP.V1 and its successor RMLBP. The other two focused on encoding local contrast information, AHB which was the only pre-existing algorithm used and RLBP.V2. Within chapter 4 all four of these demonstrated that indeed it is possible to digitise QD-PUF's into fingerprints that are suitable for authentication. Each of these however, showed very different performance in doing so. The gradient based schemes give more repeatable fingerprints at the cost of uniqueness, whereas the contrast based ones give more accurate authentication at the cost of stable fingerprints, with RLBP.V2 producing the highest degree of accuracy. Indicating that when no damage is present in the input image, fingerprint entropy produces the better authentication accuracy. Another key influencing factor in the performance of the QD-PUF fingerprints was the texture of the quantum dot pattern itself. Patterns with clear features, showing high degrees of contrast produce fingerprints that authenticate much better.

Furthermore a key factor when testing the algorithms for their performance is their robustness against common image damage, namely noise and blur. Two issues that when QD-PUFs are taken outside of a controlled laboratory environment will become unavoidable. As expected, given their stable fingerprints in the previous experiment, gradient based schemes were far more robust than their contrast based counterparts. Thanks to it taking in more data points than RLBP.V1, RMLBP outperformed the simpler algorithm. With contrast based schemes now authenticating with a lower accuracy than the gradient based ones, showing that there is a limit to just how bad their repeatability can get before their higher entropy fingerprints cannot balance it out.

Overall, this tells us several key factors when harnessing QD-PUFs using fingerprinting algorithms. Firstly there is a trade off between the robustness of the algorithm and the accuracy with which it can correctly authenticate a QD-PUF. This is due to the randomness of the fingerprint produced, a fact supported by the application of the NIST test

suite. Indicating that from an attackers standpoint the gradient based schemes produce fingerprints that have a higher probability to be successfully brute force attacked. The number of data points taken in by the algorithm has a great affect on the robustness of the algorithm and the repeatability of fingerprints produced. As well as this to maximise any gains from the fingerprinting algorithm the QD-PUF being fingerprinted must have a clear, high contrast pattern with distinct features. This therefore, brings forth two stand-out algorithms, RMLBP and RLBP.V2. The former is better suited for use when the imaging environment and apparatus is not optimal but a high degree of security is not as necessary. Such as a QD-PUF attached to a luxury product to be authenticated via smartphone. RLBP.V2 on the other hand may lack the robustness required for more widely used applications but its incredibly low false positive rates in controlled environments and high degree of randomness cannot be ignored. As such it would be suited to applications such as authenticating a QD-PUF embedded in a passport using specialised equipment.

Given that it has been demonstrated that fingerprints can be generated from QD-PUFs the next question is the viability of them for long term use. There is little point after all in a fingerprint which cannot be repeated a period of time after it was first generated due to the QD-PUF degrading. As signal to noise ratio is an influencing factor on a fingerprint and the photoluminesence of QD-PUFs decreases with time due to oxidation this matter must be addressed. It became clear that the addition of the viscous PLMA as a co-polymer greatly reduced the loss of PL due to oxidization. With some hybrid tags such as SEBSPLMA and PMMAPLMA showing little or no loss of PL over an indefinite time period. Addressing the issue of long term QD-PUF usage. To further capitalise on this it is recommended that for long term usage RMLBP is used over RLBP.V2. Its robustness to noise demonstrated in earlier chapters ensured that it was less affected by any change in signal to noise ratio.

As the behaviour of different fingerprinting algorithms as well as the long term applicability of QD-PUFs has been demonstrated the mind naturally turns to how QD-PUFs can be further adapted and improved upon. One such avenue for this is the increasing of the number of challenge response pairs that can be generated from a single QD-PUF. To do this we would need a method to change the quantum dot emission pattern without altering the QD-PUF itself. This concept was demonstrated to in fact be possible, albeit in its current state its applicability is limited. It was indeed shown that quantum dot emission patterns do indeed vary when the wavelength of the light incident upon them is varied. However, the areas of variation were not large enough to cause significant enough difference for each wavelength's fingerprint to be deemed a separate CRP. Clear difference was achieved using a CIS quantum dot sample but an InP/ZnS sample failed to produce any variation in fingerprint. Thus, although the concept has been shown to be indeed possible, further work is needed to bring it to complete fruition.

To summarise it has indeed been shown that the unique nature of QD-PUFs can be harnessed by fingerprinting algorithms for digital authentication purposes. Based on the fingerprinting algorithm used their are a range of use cases they can be applied to and they can remain usable for authentication for an indefinite amount of time. As the last of the experimental chapters showed however, there is as always more to learn.

8.2 Further Work

Throughout this thesis it has been mentioned that the QD-PUFs can be authenticated using a smartphone. This has indeed been demonstrated [7][6] and is a key point of development to bring the QD-PUFs into public use. This however takes a degree of applied knowledge and experimentation which is beyond the scope of what can be discussed here. The application of RMLBP and a QD-PUF such as the CISPMS one used in chapter 4 would be the best manner to approach this. The two of these maximise the repeatability of generated fingerprints and so will counteract the wide ranging environmental factors they will be subject to.

The expansion of QD-PUFs into public use also brings about the question of data security and storage. If they can be used by anyone then everyone must have access to the data of stored reference fingerprints. This is a weakness in the security of the authentication process as discussed in chapter 5. In said chapter a solution was proposed in terms of XOR debiasing which would essentially remove any information from the QD-PUF from the fingerprint. This is not the only solution however, nor was it subject to as rigorous a cryptographic analysis as could be possible. Primarily because the latter could form a thesis of its own. More detailed work into this however would be beneficial and not just to the concept of QD-PUFs. It is highly likely that it would contribute greatly to the field of fuzzy authentication as well as the use of noisy digital signatures as a whole[4].

To further build upon this there is the concept of more rigorous attack testing against not just the fingerprints but QD-PUFs themselves. Although simulation attack prevention can stop many attacks there is still the question of how the bane of many PUFs fares against QD-PUFs, machine learning. Machine learning attacks are being employed to attempt to replicate or at least produce convincing fakes of PUFs[49][50][51]. Such a test has not been applied to QD-PUFs.

As already discussed there is the matter of the generation of more CRPs from a single QD-PUF. In chapter 7 ways of achieving this were discussed. Such as higher magnification or quantum dot patterns with larger features. Overall though this avenue shows promise. Even if distinct CRPs cannot be generated, fingerprints that vary with wavelength still are useful as they can be used as another factor for authentication.

Finally there is the topic of other fingerprinting algorithms. There is a whole plethora of feature mapping[65] and authentication algorithms in existence[66] Many more were tested and created for use in QD-PUFs than were discussed here. Some focus on mapping out key points in an image and authenticating based on their presence in a challenge image. Others binarised based on the presence of features such as edges or corners. The ones chosen here showed more promise than those that were cut. It could be however, that one better performing than those in the preceding chapters exists. Finding or developing it could greatly improve upon QD-PUF fingerprints or it may not. Only time will tell.

Bibliography

[1] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. Physical one-way functions. *Science*, 297, 2002.

[2] Povilas Marcinkevicius, Ibrahim Ethem Bagci, and Nema M. Abdelazim et al. Optically interrogated unique object with simulation attack prevention. In *Design Automation Test in Europe Conference Exhibition*.

[3] Hongrui Cheng, Yongfeng Lu, Dongyan Zhu, Lorenzo Rosa, Fei Han, Mingguo Ma, Wenyue Su, Paul S. Francis, and Yuanhui Zheng. Plasmonic nanopapers: flexible, stable and sensitive multiplex puf tags for unclonable anti-counterfeiting applications. *Nanoscale*, 12(9471), 2020.

[4] Kieran Longmate, Elliott Ball, Edward Dable-Heath, and Robert Young. Signing information in the quantum era. *AVS Quantum Sci*, 2, 2020.

[5] Kieran D Longmate, Nema M Abdelazim, Elliott M Ball, Joonas Majaniemi, and Robert J Young. Improving the longevity of optically-read quantum dot physical unclonable functions. *Sci Rep*, 11(10999):•, • 2021.

[6] Matthew Fong, Chris Woodhead, Nema Abdelazim, Daniel Abreu, Angelo Lamantia, Elliott Ball, Kieran Longmate, David Howarth, Benjamin Robinson, and Phillip; Young Robert Speed. Using intrinsic properties of quantum dots to increase security when uniquely identifying devices. *Sci Rep*, 12(1), 2022.

[7] Elliott M. Ball, Kieran Longmate, Joonas Majaniemi, Angelo Lamantia, Daniel Abreu, Matthew J. Fong, and Robert J. Young. Smartphone-based fingerprint extraction from quantum-optical pufs. *Awaiting Publication*, 2022.

[8] Renkun Chen, Jaeho Lee, Woochul Lee, and Deyu Li. Thermoelectrics of nanowires. *Chem. Rev.*, 119, 2019.

[9] Sergey B. Brichkin and Vladimir F. Razumov. Colloidal quantum dots: synthesis, properties and applications. *Russ. Chem. Rev.*, 85(12), 2016.

[10] Dieter Bimberg and Udo W Pohl. Quantum dots: promises and accomplishments. *Materials Today*, 2011.

[11] L Brus. Electronic wave functions in semiconductor clusters: Experiment and theory. *The Journal of Physical Chemistry*, 90(12), 1986.

[12] M.V. Artemyev, A.I. Bibik, L.I. Gurinovich, S.V. Gaponenko, H. Jaschinski, and U. Woggon. Optical properties of dense and diluted ensembles of semiconductor quantum dots. *phys. stat. sol.*, 224(2), 2001.

[13] Matthew T Frederick, Victor A Amin, and Emily A Weiss. Optical properties of strongly coupled quantum dot ligand systems. *J Am Chem Soc*, 2013.

[14] A Forchel et al. Optical studies of freestanding single ingaas/gaas quantum dots. *Semicond Sci Technol*, 1996.

[15] K Brunner et al. Sharp line photoluminescence and two photon absorption of zero-dimensional biexcitons in a gaas/algaas structure. *Phys Rev Letts*, 1994.

[16] D S Chelma and J Shah. Many body and correlation effects in semiconductors. *Nature*, 2001.

[17] Y Z Hu et al. Biexcitons in semiconductor quantum dots. *Phys Rev Letts*, 1990.

[18] *Principles of Nano-Optics*. Cambridge University Press, 2012.

[19] D A Hines et al. Photoinduced surface oxidation and its effect on the exciton dynamics of cdse quantum dots. *J Phys Chem*, 2012.

[20] Virginia W. Manner, Alexey Y. Koposov, Paul Szymanski, Victor I. Klimov, , and Milan Sykora. Role of solvent oxygen ion pairs in photooxidation of cdse nanocrystal quantum dots. *ACS Nano*, 6(3), 2012.

[21] Joon Hee Jo, Seung Jun Lee, Ho Seok Heo, and Kangtaek Lee. Stability enhancement of inp quantum dot/poly(methyl methacrylate) nanocomposites for light-emitting diode applications by grafting thermoresponsive poly(n-isopropylacrylamide). *J. Mater. Chem. C*, 9, 2021.

[22] Z. Yang, Y. Zhang, J. Liu, J. Ai, S. Lai, Z. Zhao, B. Ye, Y. Ruan, T. Guo, X. Yu, G. Chen, Y. Lin, and X. S. Ultrastable quantum dot composite films under severe environments. *ACS Appl. Mater. Interfaces*, 10, 2018.

[23] Pawel Podemskia, Aleksander Marynskia, Pawel Wyborskia, Artem Berchab, Witold Trzeciakowskib, and Grzegorz Seka. Single dot photoluminescence excitation spectroscopy in the telecommunication spectral range. *Journal of Luminescence*, 212, 2019.

[24] NNCrystal US Corporation. Copper indium sulfide zinc sulfide (cuins2/zns) core/shell quantum dots (cis), `https://nn-labs.com/collections/cadmium-free-quantum-dots/products/copper-indium-sulfide-zinc-sulfide-quantum-dots-cis`.

[25] A. M. White, E. W. Williams, P. Porteous, and C. Hilsum. Applications of photoluminescence excitation spectroscopy to the study of indium gallium phosphide alloys. *J. Phys. D: Appl. Phys.*, 3(9), 1970.

[26] Liu Bing-Can, Pan Xue-Qin, Tian Qiang, and Wu Zheng-Long. Ple spectra analysis of the sub-structure in the absorption spectra of cdses quantum dots. *Chinese Phys*, 15, 2006.

[27] R. Heitz, O. Stier, I. Mukhametzhanov, A. Madhukar, and D. Bimberg. Quantum size effect in self-organized inas/gaas quantum dots. *Phys Rev B*, 62(16), 2000.

[28] M. Rambach, J.Seufert, M. Obert, G. Bacher, A. Forchel, K. Leonardi, T. Passow, and D. Hommel. Excitation spectroscopy on single quantum dots and single pairs of quantum dots. *phys. stat. sol.*, 229, 2002.

[29] Frederik Armknecht, Roel Maesy, Ahmad-Reza Sadeghiz, François-Xavier Standaertx, and Christian Wachsmann. A formal foundation for the security features of physical functions. In *2011 IEEE Symposium on Security and Privacy*, 2011.

[30] Min Seok Kim, Gil Ju Lee, Jung Woo Leem, Seungho Choi, Young L. Kim, and Young Min Song. Revisiting silk: a lens-free optical physical unclonable function. *Nature Communications*, 2022.

[31] Thomas McGrath, Ibrahim E. Bagci, Zhiming M. Wang, Utz Roedig, and Robert J. Young. A puf taxonomy. *Applied Physics Reviews*, 6, 2019.

[32] U. Rührmair and D. E. Holcomb. Pufs at a glance. In *2014 Design, Automation and Test in Europe Conference and Exhibition (DATE)*. IEEE, 2014.

[33] Jeroen Delvaux, Roel Peeters, Dawu Gu, and Ingrid Verbauwhede. A survey on lightweight entity authentication with strong pufs. *ACM Computing Surveys*, 48(2), 2015.

[34] Shahin Tajik, Enrico Dietz, Sven Frohmann, Jean-Pierre Seifert, Dmitry Nedospasov, Clemens Helfmeier, Christian Boit, and Helmar Dittrich. Physical characterization of arbiter pufs. *International Workshop on Cryptographic Hardware and Embedded Systems*, 2014.

[35] J. Roberts, I. E. Bagci, M. A. M. Zawawi, J. Sexton, N. Hulbert, Y. J. Noori, M. P. Young, C. S. Woodhead, M. Missous, M. A. Migliorato, U. Roedig, and R. J. Young. Using quantum confinement to uniquely identify devices. *Sci Rep*, 5, 2015.

[36] G. Dejean and D. Kirovski. Rf-dna: Radio-frequency certificates of authenticity. In *Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems*, 2007.

[37] Chau-Wai Wong and Min Wu. Counterfeit detection using paper puf and mobile cameras. In *2015 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2015.

[38] Yevgeniy Dodis et al. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing.*, 2008.

[39] Joni Saputra and Parman Sukarno. Improving the accuracy of fuzzy vault scheme in fingerprint biometric. In *7th International Conference on Information and Communication Technology (ICoICT)*, 2019.

[40] Jangbae Kim, Je Moon Yun, Jongwook Jung, Hyunjoon Song, Jin-Baek Kim, and Hyotcherl Ihee. Anti-counterfeit nanoscale fingerprints based on randomly distributed nanowires. *Nanotechnology*, 25, 2014.

[41] Alison F. Smith, Paul Patton, and Sara E. Skrabalak. Plasmonic nanoparticles as a physically unclonable function for responsive anti-counterfeit nanofingerprints. *Advanced Functional Materials*, 26(9), 2016.

[42] Henri Gilbert and Helena Handschuh. Security analysis of sha-256 and sisters. In *International Workshop on Selected Areas in Cryptography*, 2003.

[43] Pappu Srinivasa Ravikanth. *Physical One-Way Functions*. PhD thesis, Massachusetts Institute of Technology, 2001.

[44] Edward Bormashenko, Mark Frenkel, Alla Vilk, Irina Legchenkova, Alexander A. Fedorets, Nurken E. Aktaev, Leonid A. Dombrovsky, and Michael Nosonovsky. Characterization of self-assembled 2d patterns with voronoi entropy. *Entropy*, 20, 2018.

[45] T. Ojala, M. Pietikäinen, and D. Harwood. A comparative study of texture measures with classification based on feature distributions. In *Pattern Recognition*.

[46] P. Liang, S. Li, and J. Qin. Multi-resolution local binary patterns for image classification. In *Proceedings of the 2010 International Conference on Wavelet Analysis and Pattern Recognition*.

[47] Mathworks. imgaussfilt, *https://uk.mathworks.com/help/images/ref/imgaussfilt.html*.

[48] Mathworks. imnoise, *https://uk.mathworks.com/help/images/ref/imnoise.html*.

[49] Francesco Regazzonil, Shivam Bhasin, and Amir Ali Pour et al. Machine learning and hardware security: Challenges and opportunities. In *IEEE/ACM International Conference on Computer-Aided Design (ICCAD '20)*, 2020.

[50] Ulrich Ruhrmair, Frank Sehnke, Jan Solter, Gideon Dror, Srinivas Devadas, and Jurgen Schmidhuber. Modeling attacks on physical unclonable functions. In *CCS '10: Proceedings of the 17th ACM conference on Computer and communications security*, 2010.

[51] Xiaolin Xu and Wayne Burleson. Hybrid side-channel/machine-learning attacks on pufs: A new threat? In *2014 Design, Automation and Test in Europe Conference and Exhibition (DATE)*, 2014.

[52] Elena Pagnin, Christos Dimitrakakis, Aysajan Abidin, and Aikaterini Mitrokotsa. On the leakage of information in biometric authentication. In *Progress in Cryptology – INDOCRYPT 2014*, 2014.

[53] S.H. Kwok, Y.L. Ee, G. Chew, K. Zheng, K. Khoo, , and C.H. Tan. Comparison of post-processing techniques for biased random number generators. *Heidelberg: Springer Berlin Heidelberg*, 2011.

[54] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, and San Vo. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical Report Special Publication 800-22 Revision 1a, National Institute of Standards and Technology, 2010.

[55] Rajeev Sobti and G.Geetha. Cryptographic hash functions: A review. *IJCSI International Journal of Computer Science Issues*, 9(2):461–479, 2012.

[56] Roel Maes, Vincent van der Leest, Erik van der Sluis, , and Frans Willems. Secure key generation from biased pufs. In *CHES 2015: Cryptographic Hardware and Embedded Systems*, 2015.

[57] John Von Neumann. Various techniques used in connection with random digits. *Applied Math Series 12. National Bureau of Standards (USA)*, 1951.

[58] Aydin Aysu, Ye Wang, Patrick Schaumont, and Michael Orshansky. A new maskless debiasing method for lightweight physical unclonable functions. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2017.

[59] Michael C. Mancini, Brad A. Kairdolf, Andrew M. Smith, and Shuming Nie. Oxidative quenching and degradation of polymer-encapsulated quantum dots: New insights into the long-term fate and toxicity of nanocrystals in vivo. *J. Am. Chem. Soc.*, 2008.

[60] S. N. Raja, Y. Bekenstein, M. A. Koc, S. Fischer, D. Zhang, L. Lin, R. O. Ritchie, P. Yang, and A. P. Alivisatos. Encapsulation of perovskite nanocrystals into macroscale polymer matrices: Enhanced stability and polarization. *ACS Appl. Mater. Interfaces*, 8, 2016.

[61] H. Becker Y. Xu and, J. Yuan, M. Burkhardt, Y. Zhang, A. Walther, S. Bolisetty, M. Ballauff, and A. H. E. Muller. Double-grafted cylindrical brushes: Synthesis and characterization of poly(lauryl methacrylate) brushes. *Macromol. Chem. Phys.*, 208, 2007.

[62] Feiliang Chen, Qian Li, Mo Li, Feng Huang, Hui Zhang, Jianbin Kang, and Pidong Wang. Unclonable fluorescence behaviors of perovskite quantum dots/chaotic metasurfaces hybrid nanostructures for versatile security primitive. *Chemical Engineering Journal*, 411, 2021.

[63] ZEISS. Objective ec epiplan 10x/0.25 m27, *https://www.microshop.zeiss.com/en/uk/shop/objectives/422040-9902-000/Objective-EC-Epiplan-10x-0.25-M27*.

[64] Ileana Buhan, Jeroen Doumen, Pieter Hartel, and Raymond Veldhuis. Fuzzy extractors for continuous distributions. In *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security*, 2007.

[65] Fabian Wein, Peter D. Dunning, and Julian A. Norato. A review on feature-mapping methods for structural optimization. *Structural and Multidisciplinary Optimization*, 62, 2020.

[66] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain. Biometric cryptosystems: Issues and challenges. In *Proceedings of the IEEE*, volume 92, 2004.