Secure Facial Recognition in the Encrypted Domain using a Local Ternary Pattern Approach

Faraz Ahmad Khan[1], Ahmed Bouridane[1], Said Boussakta[2], Richard Jiang[3], Somaya Almaadeed[4]
[1]*Department of Computer and Information Sciences, Northumbria University, Newcastle upon Tyne, UK*
[2]*School of Engineering, Newcastle University, Newcastle upon Tyne, UK*
[3]*School of Computing and Communication, Lancaster University, Lancaster, UK*
[4]*Department of Computer Science and Engineering, Qatar University, Qatar*

Abstract—Automatic facial recognition is fast becoming a reliable method for identifying individuals. Due to its reliability and unobtrusive nature facial recognition has been widely deployed in law enforcement and civilian application. Recent implementations of facial recognition systems on public cloud computing infrastructures have raised strong concerns regarding an individual's privacy. In this paper, we propose and implement a novel approach for facial recognition in the encrypted domain. This allows for facial recognition to be performed without revealing the actual image unnecessarily as the features stay encrypted at all times. Our proposed system exploits the homomorphic properties of the Paillier cryptosystem and performs Euclidean distance calculations using encrypted data. We propose to represent the images using a radial Local Ternary Pattern approach where a higher than proposed radius is used to extract the image features. Our proposed system has been evaluated using two publicly available datasets and has also been compared against the previously used eigenface approach in the encrypted domain and the obtained results justify the feasibility of the proposed system.

Index Terms—Biometric identification, homomorphic encryption, Paillier cryptosystem, cloud computing, public key distance calculation

I. Introduction

An effective protocol for matching biometric data is a critical part of any facial recognition or verification system. Formally, a biometric recognition system would consist of a database, $\langle v_i, v_j \rangle_{i=1}^{N}$, where v_i represents the biometric data of the subject y_i, and a client who would query the server with a biometric data of a subject, v^0 in order to determine or verify the identity of this subject. Using some distance measure and within a reasonable distance threshold, η the server would return v_{i^*} that would be the closest match to the queried v^0.

The challenge of a facial recognition becomes even more substantial when such systems are implemented in modern cloud computing infrastructures. In such systems, when a third party cloud server is involved it is not advisable to disclose the contents or result of any query request from a client. The challenge, therefore, becomes how to perform facial verification between two parties that are mutually distrusting of each other and that do not wish to reveal the private contents of their images nor do they wish to reveal the verification results.

In a typical setup, the server would store a database of images representing each subject. Since every image represents a face it is therefore necessary to extract identifying features from every image in order to make the task of verification possible. Any client querying the server would also need to extract identifying features from the image that needs to be recognised. Under secure settings the querying image would also need to be encrypted after feature extraction to prevent the server from gaining access to the actual contents of the image. This paper focuses on facial recognition under a privacy preserving protocol. The goal is to perform conventional facial recognition but without disclosing anything about the client or the database stored on the server. This is made possible under the assumption that both parties are *honest-but-curious* (semi-honest model), i.e. both parties would execute their protocol as expected but may learn additional information about the process during the execution of the protocol.

As explained above, in order to perform facial recognition, discriminative features must be extracted from all images before being encrypted. In this paper, Local Ternary Patterns (LTPs) are proposed for the purpose of feature extraction. The LTP technique was first proposed by Tan *et a*l. [1] for facial recognition. This method was an extension of the Local Binary Patterns (LBP) and was proposed to overcome the limitations of light sensitivity of the LBP. After its development by Tan *et al.* the LTP method has also been successfully applied in the field of writer identification [2-3]. Here, we propose to extract the LTP features at a larger radius than what was proposed by [1] as it was observed that at a larger radius more discriminative features are extracted leading to an improved recognition performance accuracy of the system. The improvement brought about by extracting features at a larger radius can be seen from Figure 1.

To perform facial recognition in the encrypted domain a homomorphic encryption scheme must be used. A homomorphic encryption allows for the computations to be performed on the ciphertexts directly, without the use of the decrypted data. Homomorphic encryption schemes can be either partially homomorphic (capable of performing either addition or multiplication) or fully homomorphic (capable of performing addition as well as multiplication). Partially homomorphic schemes (PHE) are much simpler to implement and have a wide range of applications that allow secure computations in the cloud.

(a) (b) (c)

Fig. 1: (a) Original image from the GTF dataset. (b) Positive LTP at radius 15. (c) Negative LTP at radius 15.

In this work, Paillier's homomorphic encryption [4] has been used. Paillier encryption is a public key system which allows anyone to perform the encryption operation as long as they know the public key. However, the decryption can only be performed by a private key that is only known to the trusted party. The scheme is also probabilistic meaning that the same plain text would produce two different ciphertexts.

The proposed system has been evaluated using two publicly available facial databases and the results achieved demonstrate the feasibility of the proposed system. It has also been compared with the previously proposed eigenface approach for secure facial recognition and the results show that the proposed LTP approach outperforms the eigenface approach in terms of accuracy.

The remainder of this paper is organized as follows: Section II reviews the related systems previously proposed in literature. Section III outlines the framework of the proposed approach. Experimental results and discussions are presented in Section IV and finally, the paper is concluded in Section V.

II. Related Work

A prominent paper in this field is the work done by Erkin et al. [5] where they were the first to propose a face recognition method in the encrypted domain and termed the process privacy preserving face recognition. They proposed an eigenface recognition protocol, which allowed comparing Paillier encrypted ciphertexts without exposing any unnecessary details to the server. Their proposed interactive protocol has also been adopted by our proposed system here.

The same work was further improved by Sadeghi et al. [6] where the authors adopted the eigenface approach by combining the homomorphic properties of the Paillier cryptosystem with the efficiency of garbled circuits. This combination allows for a faster response time which is necessary for real world applications but relies on expensive garbled circuits to achieve this. Our proposed system is inspired by their work but is different at the feature representation stage, we propose to use a radial LTP instead of eigenface and have demonstrated improved recognition rates by making this change.

Yuan and Yu [7] also proposed a privacy preserving biometric identification system but used it to encrypt the database on the server and by doing so protected the cloud data against the risk of theft and misuse. Their proposed system achieves efficiency by exploiting the power of cloud computing and pushing almost all computation to the cloud. Biometric identification is performed by generating a credential for the candidate biometric and submitting it the cloud. Which performs all biometric computations in the cloud including a k-NN search and returns the result to the owner.

A secure multi-party biometric identification system was developed by Zhan et al. [8] where the authors proposed a framework that divided the homomorphic computation load among multiple parties. The private data to be stored was partitioned vertically so that every party has its own view of the data but also have access to all the instances involved. A k-nearest neighbour classification was used without disclosing the private actual data to any of the party members involved in the computation.

Evans et al. [9] proposed a practical privacy preserving fingerprint authentication system by combining homomorphic computations with garbled circuits. They proposed a novel back tracking protocol for efficient oblivious information retrieval.

A homomorphic encryption framework to secure a database of face templates was proposed by Boddeti [21]. The system aims to preserve the privacy of users and prevent information leakage from the templates by performing a template matching directly in the encrypted domain. The system was evaluated using various benchmark face datasets (LFW, IJB-A, IJB-B, CASIA) showing attractive performances.

Liu et al. [21] discussed a face recognition in the encrypted domain using the Discrete Fourier Transform and Logistic chaotic map. Recognition is carried out in the encrypted face images to extract the feature vectors where the similarity matching is performed using Normalized Cross Correlation Coefficient of the feature vectors of encrypted face images stored in the feature database.

A facial biometric identification system using homomorphic encryption and operating in the encrypted domain was proposed by Drozdowski et al. [22]. The system fulfils various properties and is useful for biometric template protection applications.

Gomez-Barrero et. al [23] proposed a framework for multi-biometric template protection using a homomorphic probabilistic encryption where only encrypted data is handled in order to achieve a more secure and privacy-preserving system.

K-NN classification under homomorphic encryption was also explored by Nassar et al. [10] where they also adopted the eigenface approach for facial images representation. They experimented and proposed the best tuning parameters that would work for an eigenface based secure recognition system.

III. PROPOSED SYSTEM

The framework of the proposed system is shown in Figure 2. LTP features are extracted from the facial images and stored on the server. Since the server is assumed to work under the *honest-but-curious* model all the feature vectors are stored in an unencrypted form. Encryption will happen during an interactive process when the client requests for a recognition result using an unknown encrypted image. Before the interactive process starts, the client querying the server would also extract LTP features from its query image and then encrypt this feature vector using any homomorphic encryption scheme. Since the client is the only party that would receive the output, any public-key encryption algorithm can be utilized that demonstrates homomorphic properties. As mentioned in Section I, Paillier encryption has been used by us in the proposed system. The encryption stage will generate a public and private key. The client will retain the private key for decryption purposes and send the encrypted feature vector along with the public key to the server. Using this public key, the server is capable of performing encryption on its stored data and perform linear operations on the ciphertexts by exploiting the homomorphic property of the Paillier system. The server will perform an interactive secure distance protocol (explained in Section III-B3) and return to the client a set of encrypted distances. The client would then be able to decrypt these distances using his/her private key and find the closed match corresponding to the minimum distance. If the distance is smaller than a certain threshold, η a match is declared. It is also assumed that all communication between the client and server is over a secure authenticated channel and under this protocol the server, at any stage, does not have any knowledge of the actual contents of the clients query. Even the distances reported by the server are encrypted and only the client can decrypt those results.

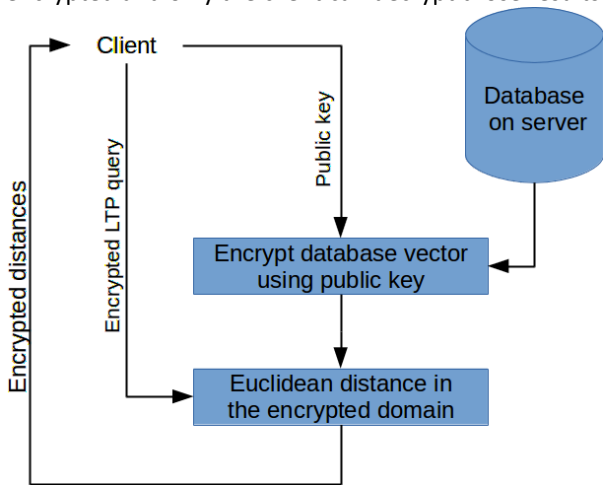

Fig. 2: Framework of the proposed system.

A. Local Ternary Patterns

The Local Ternary Pattern encodes a grayscale image into a three valued code of either -1, 0 or 1 as shown in 1 and 2

$$LTPM, R(x,y) = \sum_{n=0}^{M-1} k'(p_n, p_c, t)2^M$$

Where M is the neighbourhood, R is the radius at which extraction of LTP is performed and t represents the threshold that is specified by the user and k' is given by:

$$k'(p_n, p_c, t) = \begin{cases} 1 & p_n \geq p_c + t \\ 0 & p_c - t \leq p_n < p_c + t \\ -1 & otherwise \end{cases} \quad (2)$$

The threshold, t is utilized by LTP to calculate a tolerance interval between the central pixel and neighbouring pixels represented by p_c and p_n , respectively. The LTP procedure generates a 0 if the intensity of a pixel is between this interval, produces a -1 if the intensity is below this interval and 1 for any values above this interval. For example, as can be seen in Figure 3, for this $3x3$ patch of image the tolerance interval is [29, 35] when a threshold of t = 5 is used for a central pixel of p_c = 34. The neighbouring pixels are set to 0, 1 and -1 for values that lie within, above and below this interval, respectively.

For the sake of simplicity, the authors suggested another variation of the ternary LTP code in [1] by further dividing the acquired LTP code into positive and negative patterns. This divides the ternary LTP code in two binary LBP codes. The splitting of a LTP code into positive and negative LBP codes is also shown in Figure 3.

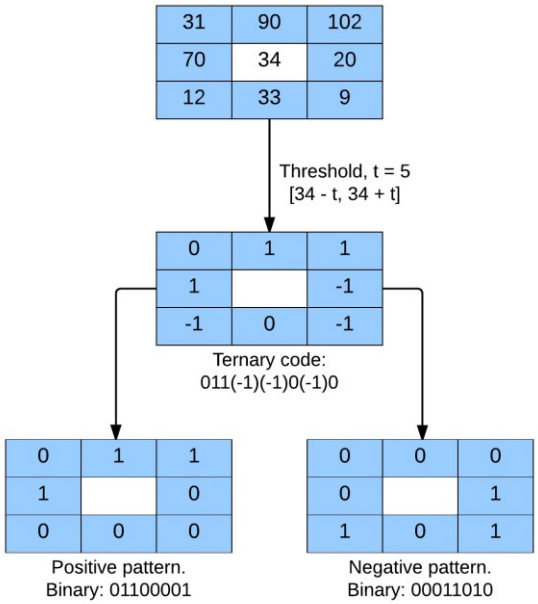

Fig. 3: Demonstration of LTP encoding for a $3x3$ block.

B. The Paillier Cryptosystem

The Paillier cryptosystem [4] is a probabilistic public key encryption scheme that possesses the homomorphic properties of addition, thus it is only partially homomorphic. The security of the Paillier cryptosystem is based upon the *n-th* in $Z^*_{n^2}$. The set $Z^*_{n^2}$ is a set of integers that are smaller than n^2 but are also prime to n^2. In this sub-section the key generation, encryption and decryption processes in the Paillier system are explained, for a detailed analysis of the scheme the reader is referred to the original paper [4].

1) Key Generation: As explained above the setting for key generation is the multiplicative group $Z^*_{n^2}$. The first step of the process is to randomly generate two large prime numbers, p and q that are of equal bit length. p and q must satisfy the condition of $gcd(pq,(p-1)(q-1)) = 1$. Next, n is calculated using $n = pq$ and the Carmichael's function on n, $\lambda(n)$ is calculated using $\lambda = lcm(p-1,q-1)$. A random number g is also selected from the multiplicative group $Z^*_{n^2}$. After selecting g a check must be performed by ensuring that n divides the order of g through the existence of the modular multiplicative inverse, μ:

$$\mu = (L(g^{\lambda}(mod\ n^2)))^{-1}(mod\ n) \quad (3)$$

where L is the quotient of the Euclidean division, given by:

$$L(\mu) = \frac{\mu-1}{n} \quad (4)$$

If this check fails, a different g must be chosen from $Z^*_{n^2}$. However, it should also be noted that simply $g = n+1$ satisfies all the conditions but comes at a cost of larger λ *(*for further clarification how to determine the public and private keys the reader is encouraged to visit reference [4]).

The public encryption key is given by (n,g), whereas the private decryption key is given by (μ,λ). Having calculated the keys, the encryption of a given pixel, p can be performed using

$$E(p) = c_p = g^p.r^n(mod\ n^2) \quad (5)$$

Where r is a random number from $Z^*_{n^2}$ and the pixel $p<n$.

The above ciphertext can be decrypted back into the pixel value using

$$p = L(c^{\lambda}(mod\ n^2)).\mu(mod\ n) \quad (6)$$

2) Homomorphic Properties of Paillier: As mentioned above, the Pailler cryptosystem is additively homomorphic i.e. the product of two pixels $E(p_1)$ and $E(p_2)$ in the encrypted domain will correspond to the sum of the two pixels in the plain text domain.

$$D(E(p_1,r_1).E(p_2,r_2)\ mod n^2) = p_1 + p_2\ mod n \quad (7)$$

D represents a decryption of the ciphertext while E represents an encryption of the plaintext. The multiplication of a ciphertext is also possible with an unencrypted constant. The k-th power of the ciphertext $E(p_1,r_1)$ corresponds to the encryption of the product of k and p_1.

$$D(E(p_1,r_1)^k mod n^2) = k.p_1\ mod n \quad (8)$$

It should be noted that equation 8 does not make the Paillier cryptosystem fully homomorphic as it should be observed that the constant k is unencrypted and in the plaintext domain. Given two encrypted numbers $E(p_1)$ and $E(p_2)$ one cannot get $E(p_1.p_2)$ under Paillier, only $E(p_1 + p_2)$ is possible.

3) Distance Computation in the Encrypted Domain: The simple Euclidean distance or it's square between two vectors, the query LTP vector v^0 and a LTP vector stored on the server v_i for subject i can be calculated using

$$d_i^2 = \sum_{j=1}^{m} \left(v'_j - v_{j,i}\right)^2, i = 1 \dots N \quad (9)$$

where m represents the number of variables in a vector. The above equation can be expanded to

$$d_i^2 = \sum_{j=1}^{m} v'^2_j - \sum_{j=1}^{m} 2v'_j v_{j,i} + \sum_{j=1}^{m} v^2_{j,i} \quad (10)$$

Under the homomorphic property of addition, the three sums of Equation 10 can be considered equivalent to the product of the three elements in the encrypted domain,

$$E(d_i^2) = E\left(\sum_{j=1}^{m} v'^2_j\right) \cdot E\left(-\sum_{j=1}^{m} 2v'_j v_{j,i}\right) \cdot E\left(\sum_{j=1}^{m} v^2_{j,i}\right) \quad (11)$$

The term $E\left(\sum_{j=1}^{m} v'^2_j\right)$ in Equation 11 can be calculated by the server alone by simply encrypting the value $E\left(\sum_{j=1}^{m} v^2_{j,i}\right)$. Similarly, the second term $E\left(-\sum_{j=1}^{m} 2v'_j v_{j,i}\right)$ can also be calculated by the server alone using the homomorphic properties outlined in Section III-B2,

$$E\left(-\sum_{j=1}^{m} 2v'_j v_{j,i}\right) = \left(E\left(\sum_{j=1}^{m} v'_j\right)\right)^{-2v_{j,i}} \quad (12)$$

Finally, the term $E\left(\sum_{j=1}^{m} v^2_{j,i}\right)$ in equation 11 cannot be calculated by the server alone as it would require the involvement of the client by following an interactive protocol as one outlined in [5]. Using this protocol the server sends the value back to the client after blinding it using a uniform random element. Blinding is necessary to protect the privacy of the client making the request. The client decrypts the value, calculates $E\left(\sum_{j=1}^{m} v'^2_j\right)$ in plaintext domain and then send it back to the server after encrypting it again. Note that this interactive protocol needs to be run only once to get all the required results.

4) Minimum Distance: To determine the identity of the client, the feature vector on the sever that is closest to the query vector needs to be determined. After distance computation the server generates a vector of N encrypted distances i.e. $E(d_i)$, $i = 1 \ldots N$. The idea is to determine the smallest distance in this vector and with it the corresponding label of that subject. The distance is then compared to a distance threshold η at the client's side thus ensuring security. If the distance is smaller than the threshold value, only then a match is returned back to the client. The protocol for finding the minimum distance by the server is suggested by [6], and the same protocol is used in the system proposed here.

IV. Experimental Results

Experimental results were carried out to demonstrate the effectiveness of the proposed system in the encrypted domain using two publicly available databases: the AT&T (ORL) face database [6] and the Georgia Tech face database [11]. Both the databases chosen here demonstrate multiple conditions that deviate from normal circumstances. Distortions such as variations in pose, illumination, gestures and occlusions are covered.

AT&T Laboratories at Cambridge University manages the AT&T (ORL) face database. The database is composed of 40 individuals having 10 images per individual. This database covers variations in gestures, expressions, occlusions and angles (facial images taken with a maximum of 20 degrees variation in rotation). The evaluation protocol used for this database is similar to that used previously in literature [12–14] i.e. 70% of images per subject are used for training set while the remaining images are designated as query or test images.

The Georgia Tech face database (GTF) is composed of 50 individuals having 15 images per individual. The GTF database is more challenging than the ORL as it involves a cluttered background and greater variations in pose, illumination and expressions. The evaluation protocol for the GTF database has been kept the same as the ORL, i.e. 70% of images per subject are used for the training set while the rest are used for querying the system.

Radius	Recognition Rate (ORL)	Recognition Rate (GTF)
3	95.83%	78.80%
5	97.50%	80.40%
7	98.33%	81.20%
9	97.50%	85.20%
11	97.50%	84.20%
13	97.50%	84.80%
15	97.50%	86.00%
17	97.50%	85.20%

TABLE I: Recognition rate for varying radii for the ORL and GTF databases.

LTP features are extracted from all images using a higher radius where it was observed that using a radius of 7 produced the most discriminative features resulting in the best accuracy for the ORL database while a radius of 15 proved to work best for the GTF database. The recognition rate under different radii are reported in Table I. During the encryption task each element of this feature vector is encrypted using a key size of 2048 bits (Section III-B1), which is the recommended key size as per NIST recommendations [15]. The performance at this stage can be improved by benefiting from the randomization feature of the Paillier cryptosystem, i.e. a repeated value can be encrypted by simply randomizing an already encrypted value [16].

Table II shows the comparison of the proposed system with some methods previously published in the field using the same datasets and also using the same evaluation protocol that has been used in the works. As can be seen the proposed system outperforms most of the systems on both datasets. The previously published systems shown at the top of Table II operate in plaintext domain and not in the encrypted domain, but were added here for the purpose to demonstrate the effectiveness of the proposed method.

Furthermore, a comparative analysis against the eigenface approach operating in the encrypted domain has been carried out. The eigenface approach is a popular method when performing facial recognition in the encrypted domain and has been shown to be effective in works done by [5], [6], [10]. For the sake of comparison, the eigenface approach has been implemented and used on the two datasets using the exact and same operational conditions as used for the proposed system. As can be seen, the proposed LTP approach (calculated using a large radius) outperforms the eigenface approach by a large margin for both datasets (5% and 11.6% improvement for ORL and GTF databases, respectively). The results achieved demonstrate that the proposed system produces more than acceptable results when dealing with encrypted facial recognition. The various benchmark datasets used have multiple distortions including pose, illuminations, gesture and occlusions. A key feature of the LTP method it that it is capable to extract and process the texture from these multiple distortions by combining the two binary patterns (positive and negative). These positive and negative patterns especially when varying the radius size are capable to capture more distinguishing patterns to improve the recognition.

V. Conclusion

In this paper, we have proposed and implemented a novel approach for facial recognition in the encrypted domain, this allows for facial recognition without revealing the facial images unnecessarily as the images stay encrypted at all times.

Our proposed system exploits the homomorphic properties of the Paillier cryptosystem and performs Euclidean distance.

System	Dataset	Recognition Rate (Top-1)
Naseem et al. [12]	ORL	93.50%
Bansal and Chawla [17]	ORL	93.75%
Xu et al. [18]	ORL	95.00%
Xu et al. [19]	ORL	91.67%
Naseem et al. [12]	GTF	92.57%
Bansal and Chawla [17]	GTF	63.75%
Xu et al. [18]	GTF	74.25%
Xu et al. [19]	GTF	62.20%
Mahalingam and Ricanek [20]	GTF	92.42%
Eigenfaces approach (encrypted) [5], [6], [10]	ORL	93.33%
Proposed system (encrypted)	ORL	**98.33%**
Eigenfaces approach (encrypted) [5], [6], [10]	GTF	74.40%
Proposed system (encrypted)	GTF	**86.00%**

TABLE II: Performance evaluation of the proposed system.

calculations using encrypted ciphertexts. The proposed system has been evaluated on two publicly available datasets showing attractive recognition performances for both databases. We have demonstrated that extracting LTP at a larger than proposed radius captures more descriptive features, we have also demonstrated the effectiveness of the proposed LTP secure distance system over the eigenface approach previously used in literature making a secure facial recognition system more practical for real world applications. The system proposed clearly improves the previously proposed systems for secure Euclidean systems in terms of accuracy achieved. However, the complexity of the proposed system in terms of time is linear to the dataset size. For future work we would like to explore K-d trees at the classification stage to speed up the overall process.

ACKNOWLEDGMENT

This publication was made possible by the NPRP award number 12S-0312-190332 from the Qatar National Research Fund (a member of The Qatar Foundation). The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] X. Tan and B. Triggs, "Enhanced local texture feature sets for face recognition under difficult lighting conditions," *IEEE transactions on image processing*, vol. 19, no. 6, pp. 1635–1650, 2010.

[2] Y. Hannad, I. Siddiqi, and M. E. Y. El Kettani, "Writer identification using texture descriptors of handwritten fragments," *Expert Systems with Applications*, vol. 47, pp. 14–22, 2016.

[3] F. A. Khan, M. A. Tahir, F. Khelifi, and A. Bouridane, "Offline text independent writer identification using ensemble of multi-scale local ternary pattern histograms," in *Visual Information Processing (EUVIP), 2016 6th European Workshop on*. IEEE, 2016, pp. 1–6.

[4] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 1999, pp. 223–238.

[5] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 2009, pp. 235–253.

[6] A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient privacy preserving face recognition," in *International Conference on Information Security and Cryptology*. Springer, 2009, pp. 229–244.

[7] J. Yuan and S. Yu, "Efficient privacy-preserving biometric identification in cloud computing." IEEE, 2013, pp. 2652–2660.

[8] J. Z. Zhan, L. Chang, and S. Matwin, "Privacy preserving k-nearest neighbor classification." *IJ Network Security*, vol. 1, no. 1, pp. 46–51, 2005.

[9] D. Evans, Y. Huang, J. Katz, and L. Malka, "Efficient privacy-preserving biometric identification," 2011.

[10] M. Nassar, N. Wehbe, and B. Al Bouna, "K-nn classification under homomorphic encryption: Application on a labeled eigen faces dataset." IEEE, 2016, pp. 546–552.

[11] GeorgiaTech. (2007) Georgia tech face database. [Online]. Available: http://www.anefian.com/research/face-reco.htm

[12] I. Naseem, R. Togneri, and M. Bennamoun, "Linear regression for face recognition," *IEEE transactions on pattern analysis and machine intelligence*, vol. 32, no. 11, pp. 2106–2112, 2010.

[13] X. Jiang, B. Mandal, and A. Kot, "Eigenfeature regularization and extraction in face recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 30, no. 3, pp. 383–, 2008.

[14] J. Yang, D. Zhang, A. F. Frangi, and J.-y. Yang, "Two-dimensional pca: a new approach to appearance-based face representation and recognition," *IEEE transactions on pattern analysis and machine intelligence*, vol. 26, no. 1, pp. 131–137, 2004.

[15] E. Barker, L. Chen, and D. Moody, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*. US Department of Commerce, National Institute of Standards and Technology, 2014.

[16] Y. Rahulamathavan, R. C.-W. Phan, J. A. Chambers, and D. J. Parish, "Facial expression recognition in the encrypted

domain based on local fisher discriminant analysis," *cognition*, vol. 4, p. 6, 2013.

[17] A. K. Bansal and P. Chawla, "Performance evaluation of face recognition using PCA and N-PCA," International Journal of Computer Applications, vol. 76, no. 8, 2013.

[18] Y. Xu, X. Fang, X. Li, J. Yang, J. You, H. Liu, and S. Teng, "Data uncertainty in face recognition," IEEE transactions on cybernetics, vol. 44, no. 10, pp. 1950–1961, 2014.

[19] Y. Xu, X. Li, J. Yang, Z. Lai, and D. Zhang, "Integrating conventional and inverse representation for face recognition," IEEE transactions on cybernetics, vol. 44, no. 10, pp. 1738–1746, 2014.

[20] G. Mahalingam and K. Ricanek, "Lbp-based periocular recognition on challenging face datasets," EURASIP Journal on Image and Video processing, vol. 2013, no. 1, p. 36, 2013.

[21] C. Liu, J. Li and Y. Duan, "A face image recognition algorithm based on DFT encryption domain," 1st Inter. *Conf on Electronics Instrumentation & Information Systems (EIIS)*, Harbin, 2017, pp. 1-6.

[22] P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf and C. Busch, "On the Application of Homomorphic Encryption to Face Identification," Intern. Conf. of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 2019, pp. 1-5.

[23] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryption," Pattern Recognition, vol. 67, pp. 149–163, 2017.

[24] V. N. Boddeti, "Secure face matching using fully homomorphic encryption," in Intl. Conf. on Biometrics Theory, Applications and Systems (BTAS). IEEE, 2019, pp. 1–10.