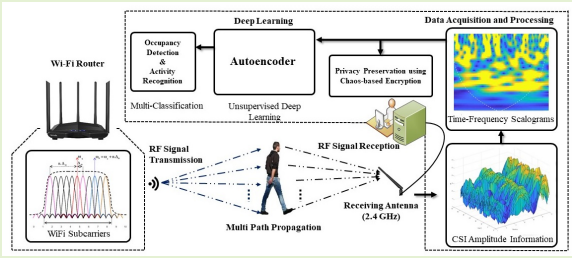
Privacy-Preserving Wandering Behaviour Sensing in Dementia Patients using Modified Logistic and Dynamic Newton Leipnik Maps

Syed Aziz Shah, Jawad Ahmad, Fawad Masood, Syed Yaseen Shah, Haris Pervaiz, William Taylor, Muhammad Ali Imran and Qammer H. Abbasi

***Abstract*— The health status of an elderly person can be identified by examining the additive effects of aging along disease linked to it and can lead to the 'unstable incapacity'. This health status is essentially determined by the apparent decline of independence in Activities of Daily Living (ADLs). Detecting ADLs provide possibilities of improving the home life of elderly people as it can be applied to fall detection systems. . This paper looks at Radar images to detect large scale body movements. Using a publicly available Radar spectogram dataset, Deep Learning and Machine Learning techniques are used for image classification of Walking, Sitting, Standing, Picking up Object, Drinking Water and Falling Radar spectograms. The Machine Learning algorithm used were Random Forest, K Nearest Neighbours and Support Vector Machine. The Deep Learning algorithms used in this paper were Long Short Term Memory, Bi-directional Long Short-Term Memory and Convolutional Neural Network. In addition to using Machine Learning and Deep Learning on the spectograms, data processing techniques such as Principal Component Analysis and Data Augmentation is applied to the spectogram images. The work done in this paper is divided into 4 experiments. The first experiment applies Machine and Deep Learning to the the Raw images data, the second experiment applies Principal Component Analysis to the Raw image Data, the third experiment applies Data Augmentation to the Raw image data and the fourth and final experiment applies Principal Component Analysis and Data Augmentation to the Raw image data. The results obtained in these experiments found that the best results were obtained using the CNN algorithm with Principal Component Analysis and Data Augmentation together to obtain a result of 95.30 % accuracy. Results also showed how Principal Component Analysis was most beneficial when the training data was expanded by augmentation of the available data.**



***Index Terms*— Wandering behavior, wireless sensing, machine learning, human activity, patient monitoring**

I. Introduction

Alzheimer disease (AD) is the most common symptoms experienced by dementia patients that are characterized by cognitive decline [1] . This can be categorized by numerous cognitive deficiencies such as (temporary) loss of memory, decline in physical behaviour and slowing down of critical thinking, specifically deficits in doing Activities of Daily Livings [2]. Detecting AD at infant stage is extremely challenging as several of the symptoms associated with this disease are common with people normal ageing. Presently, there is no method that can intervene the disease-modifying therapy for dementia due to AD, monitoring ADLs of [3] dementia patients can keep track of its progression that would allow for treatment planning and providing better care services for challenges faced due to behavioural symptoms.

Moreover, many new detection and prediction undergoing clinical trials, non-invasive and reproducible physiological symptoms are required to determine and recruit subjects in the preliminary stage of the dementia disease, to continuously monitor progression of AD. In clinical settings, AD detection is obtained using a series of trials and tests including checking family history of the patients, cognitive impairments diagnosis, brain imaging and monitoring techniques. These techniques include Magnetic Resonance Imaging (MRI), Computed Tomography (CT), and Electroencephalogram (EEG) that have been exploited to aid physicians when detecting the specific disease. The EEG comprise electrical signals obtained from two electrodes deployed on subject's scalp's and carry the electrical activity of the brain. The EEG has become one of the most important non-invasive techniques used in clinical settings that help improve our

This work is supported in parts by EPSRC EP/T021020/1 and EP/T021063/1.

Syed Aziz Shah is an Associate Professor at Centre for Intelligent Healthcare, Coventry University, UK (syed.shah@coventry.ac.uk)

Jawad Ahmad is at School of Computing, Edinburgh Napier University, UK. Fawad Masood is associated with Institute of Space Technology, Islamabad, Pakistan. Syed Yaseen Shah is at Glasgow Caledonian University, UK. Haris Pervaiz at Lancaster University, UK. Muhammad Ali Imran, William Taylor and Qammer H. Abbasi are at University of Glasgow, UK.

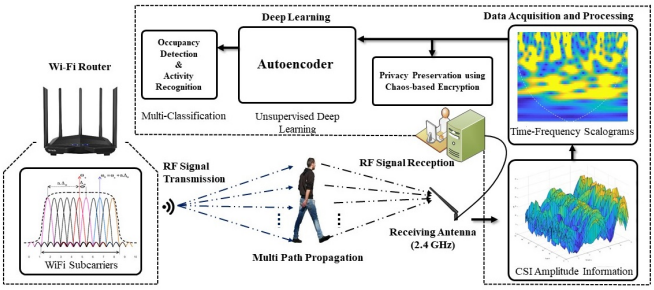


Fig. 1: System architecture of intelligent healthcare system for wandering behaviour detection.

understanding of neural activity and complexity, for the detection of dysfunctional brain slots.

The wireless technologies that include Global Positioning System (GPS), Global System for Mobile Communications (GSM) are extensively used for safety and security purposes. Recently. these technologies have also been applied in intelligent healthcare systems for locating elderly dementia patient moving out from indoor environment. Moreover, state-of-the-art healthcare devices, generally use vision-based and auditory-based signals to deliver patients several sorts of daily reminders [4]. A sensor-based system enables the dementia patients to live safely. These sensors include movement detection systems, non-invasive fall detectors and vital sign monitoring. These device can record the patients ADLs along their daily routine habits [5] and identity behavioral abnormalities. Numerous researchers have designed electronic games, specially made for dementia patients [6]. These games enable the patients' minds to be alert, aware and to examine the degree of progression of the disease and can be used by care-givers to evaluate AD and identify this condition at an early stage. Similar work was done in articles such as [7] that used radio frequency identification (RFID) to develop a an indoor safety care unit prevent dementia patients from entering hazardous or restricted zones. The aforementioned technologies use dedicated devices and most of them has be deployed on person's body.

The received signal indicator (RSI) recorded using radio-frequency (RF) technology such as Wi-Fi signals has been used to localize people in indoor environment [8]–[10]. However, the RSI data suffers from instability as it is highly susceptible to external noise and inconsistencies that make it infeasible for monitoring dementia patients. On the contrary, the recently used wireless channel state information (CSI) obtained from Wi-Fi technology deliver multiple frequency carriers that can be used to detect ADLs of an elderly person. The main advantage of using channel state information over received signal strength indicator the former presents multiple frequency subcarriers over a certain frequency band. Where each body movements induces a unique on each of the frequency channel that can be used to used monitor different human activities by examining the amplitude information. Also, due to multipath fading, if some of the subcarriers are not received, still the remaining can be used to detect any movement in indoor settings. The CSI information used are robust against external interference, noise and can detect intricate movement in line-of-sight and non-line of sight. On the other hand, the RSSI data suffers coarse-grain information and are highly susceptible to noise, as it only depends on single frequency carrier.

The Wi-Fi sensing present numerous advantages over other techniques such as radar, one of the notable ones is that the former can detect any movement in line-of-sight and non-line-of-sight. However, the latter use directional electromagnetic beam, hence any activity in non-line-of-sight goes undetected. Leveraging channel state information instead of received signal strength indicator the CSI provides multiple frequency subcarriers over a certain frequency band. Where each body movements induces a unique on each of the frequency channel that can be used to used monitor different human activities by examining the amplitude information. Also, due to multipath fading, if some of the subcarriers are not received, still the remaining can be used to detect any movement in indoor settings. The CSI information used are robust against external interference, noise and can detect intricate movement in line-of-sight and non-line of sight. On the other hand, the RSSI data suffers coarse-grain information and are highly susceptible to noise, as it only depends on single frequency carrier. The system would work in outdoor environment as well as long as Wi-Fi transmitter and the wireless devices used operating at 2.4 GHz are used.

Using novel encryption scheme and securing patient data is due to the fact that nearly one thousand patient data breaches occurred in 2018, among the most notable one was when more than 193 million personal records were exposed to fraud and identity theft. The top three breaches of data security were from the health care industry. The largest medical and healthcare patient data breach was recorded in healthcare insurance company namely, Anthem. The breach exposed the patients personal records — including names, birth dates, Social Security numbers, home addresses and other personal info of 78.8 million current and former members and employees of Anthem. [11]

Furthermore, privacy-preserving intelligent healthcare system in conjunction with self-adaptive access control is of upmost importance. The idea is to make sure that the safety and security of patients' data, actualize access control for in emergency and normal cases. The datasets produced files generated by the patient monitoring systems are encrypted and shared a centralized system that can be safely shared among caregivers belonging to various healthcare sectors using multi-domain access policy and procedures. The conventional data set access schemes enable authorized people to decrypt particular subject's sensitive healthcare record , however it also adversely affects the first-response treatment as the life of a certain patient is threatened due to the onsite care-provider not allowed to access healthcare historical data.

In this context, we propose a novel, privacy-preserving, non-invasive intelligent healthcare system for wandering behaviour in dementia patient. This system alerts the care-givers regarding the daily routine activities of the patients and notify in case of the subject leaving the area of interest (experiencing

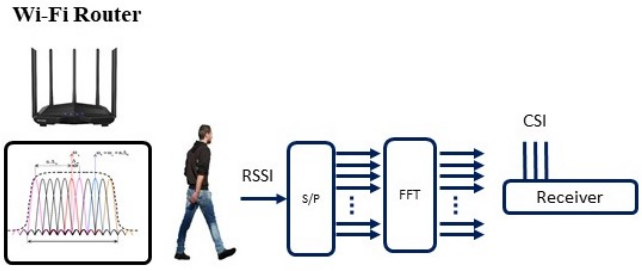


Fig. 2: Time to frequency domain using CSI data stream.

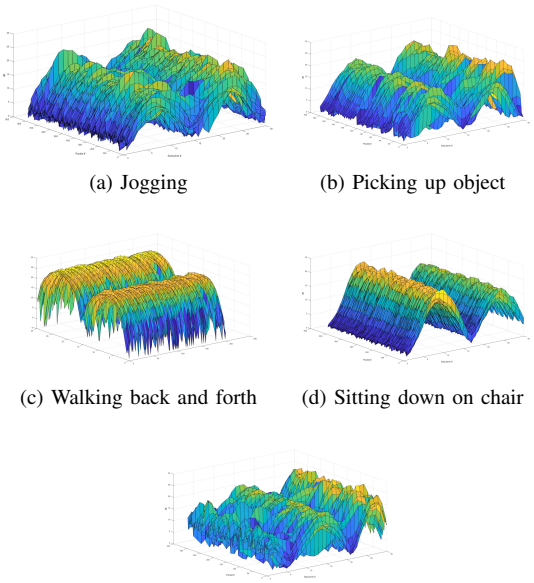
wandering behaviour) while preserving privacy of the subject. This system exploits low-cost small wireless devices such as off-the-shelf Wi-Fi router, network interface card and an omnidirectional antenna operating at 2.4 GHz. In addition, we have implemented two independent modules namely: (i). Deep Learning for wandering behaviour detection (leaving the area) and (ii). Modified Logistic and Dynamic Newton Leipnik maps for scalogram encryption.

II. Non-Invasive Wireless Sensing for Wandering Behaviour Monitoring

The two of the most commonly used techniques of Wi-Fi sensing namely the RSI and CSI are applicable for numerous applications and can potentially monitor large-scale and small-scale body movements such as activities of daily living and vital signs monitoring including chest movement and heart rate. The RSI data only provide plain RF signal strength in the form of wireless signal propagation, due to that the data collected is extremely inconsistent and inadequate for monitoring physical activities . Yu et al., [12] presented persons monitoring system based on RSI data that delivered an overall accuracy of more than 70%. On the hand, the CSI data recorded using wireless devices deliver fine-grained measurement using multiple sub-carriers. The proposed system architecture based on Wi-Fi technology driven by deep learning and image encryption is presented in Fig. 1.

The Wi-Fi signals retrieved through IEEE 802.11 a/a/ac use Orthogonal Frequency Division Multiplexing (OFDM) scheme that efficiently mitigates the multi-path fading effect induced in indoor environment cause by physical objects act as obstructions such as furniture, people in surrounding, walls, ceiling and floor. In OFDM scheme, the frequency carrier is split into several sub-frequency channels. The RF signals operating at S-Band (2.4 GHz) recorded, are primarily pass-band signals and are transformed into base-band (message) signals. These subcarriers are converted into the frequency domain using serial-to-parallel converter on Wi-Fi signals and Fast Fourier Transform (FFT) is then applied on all data as shown in Fig. 2.

Small wireless device operating at S-Band such as Intel 5300 NIC was used to record CSI data stream from OFDM subcarriers. An open-source NIC wireless sensing device



(a) Jogging (b) Picking up object

(c) Walking back and forth (d) Sitting down on chair

(e) Leaving room

Fig. 3: Variances of amplitude information obtained from raw CSI data.

drivers that measure the CSI data for all 30 available subcarriers delivering fine-resolution wireless channel characteristics that include reflection, refraction and shadowing effect known as multi-path fading effect.

Let H_i denote the CSI packets for i^{th} frequency channel, carrying variances of amplitude information [13], denoted as:

$$\mathbf{H_i} = \|H^i\| e^{j\angle H_n} \tag{1}$$

Here $|H_i|$ and $\angle H_i$ deliver the variations of CSI amplitude and phase information for i^{th} subcarrier, respectively. The phase information recorded for individual subcarrier $i, \angle H_i$ is written as [14]

$$\mathbf{H_i} = \angle H_i + (\lambda_p + \lambda_s) m_i + \lambda_c + \beta + Z, \tag{2}$$

subcaption

Where β is the CSI data packets phase offset for i^th frequency subcarrier and m_i is the subcarrier index. The internal noise of off-the-shelf NIC is expressed as Z, and λ_p, λ_s, and λ_c are the phase errors, sample subcarrier offset and central frequency offset, respectively. The raw channel state information is sufficient to extract meaningful information for occupancy monitoring due to the random noise present in Wi-Fi signals. We have only used amplitude information for five activities of daily living activities and wandering behaviour due to short-term memory loss, resulting in patient going out of indoor environment when as shown in Fig. 4.

This system will work and detect activities of daily living and identify critical event such as wandering behavior within Wi-Fi signal range. In normal in-home environment, Wi-Fi signals are available almost everywhere, hence the proposed system is feasible solution.

A. Wi-Fi Signal Acquisition and Data Processing

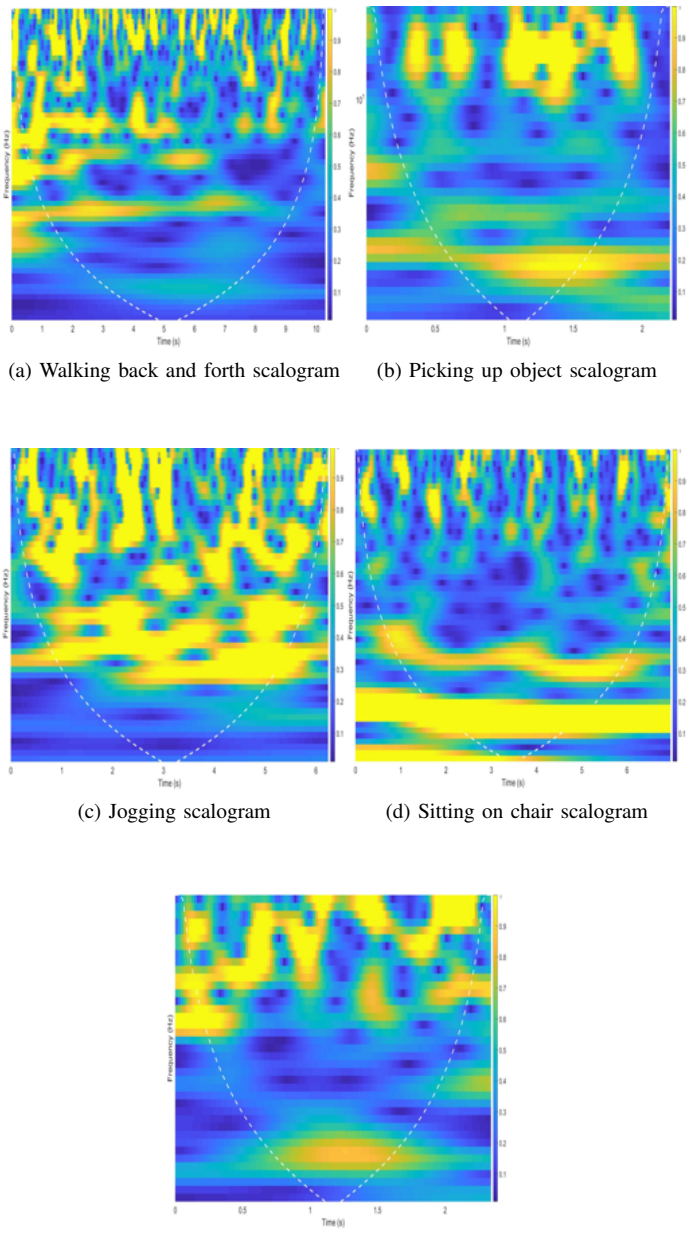
The raw CSI data received using off-the-shelf NIC was connected through wireless medium to a Wi-Fi router operating at 2.4 GHz is discussed in detailed as follows.The data packets were obtained with multiple orthogonal frequency subcarriers from the Internet Control Messages Protocol (ICMP) data stream. In theory, the total volume of raw data are exactly same as compared to the ICMP packets. However, after thorough examination, the CSI data were slightly less than its counterpart . In order to synchronize the sub carrier of the data stream, we have applied linear transformation algorithm on raw data. In principle, the OFDM frequency channels should comprise of independent datasets. Nonetheless, in practice, the adjacent sub carriers consist of similar data. To identify wandering behaviour in dementia patients and to extract distinct information from each OFDM sub carrier, we apply principal component analysis (PCA) to retrieve unique data sets for each recording. The raw CSI data packets can be accommodated into different independent components. This system requires only one transmitter that is Wi-Fi router, radiating electromagnetic waves in all directions and an omni-directional receiving antenna.This system requires only one transmitter that is Wi-Fi router, radiating electromagnetic waves in all directions and an omni-directional receiving antenna. Human activities including normal and abnormal behavior occurring in line-of-sight (between transmitter and receiver) and non-light-sight can easily be detected using proposed system. The optimum operating frequency is the unlicensed band – 2.4 GHz. Primary aim of using omni-directional antennas lies in the fact that they can detect any movement when patient is performing activities within line-of-sight and non-line-of-sight. However, the directional antennas will only detect movements within line-of-sight only. Human activities including normal and abnormal behavior occurring in line-of-sight (between transmitter and receiver) and non-light-sight can easily be detected using proposed system. The optimum operating frequency is the unlicensed band (2.4 GHz).

This system will work and detect activities of daily living and identify critical event such as wandering behavior within Wi-Fi signal range. In normal in-home environment, Wi-Fi signals are available almost everywhere, hence the proposed system is feasible solution.

A total of 20 volunteers took part in the experimental campaign with age range from 45 to 70 years.

B. Scalogram for Detecting ADLs and Wandering Behaviour

The multiresolution scalograms presentign time-frequency information are generated from raw CSI data and are used to detect the wandering behaviour in dementia patient, implying when subject goes out of the room. The scalograms are energy density functions generated by applying Continuous Wavelet Transform (CWT) on all raw CSI data packets. The energy density function $E(t, f)$ can be produced from variances of amplitude information of the CWT function $C_d(t, f)$ using squaring function on discrete datasets. The time-frequency observations are received the CWT function $C_c(t, s)$ of an



(a) Walking back and forth scalogram (b) Picking up object scalogram

(c) Jogging scalogram (d) Sitting on chair scalogram

(e) Wander behaviour (Leaving room) scalogram

Fig. 4: Scalograms obtained from CSI data for ADLs and wandering behaviour.

RF signals denoted as $x(t)$, representing time duraction as t and scale factor s that is expressed as follows:

$$C_c(t, s) = \int_{-\infty}^{+\infty} x(v) \frac{1}{\sqrt{s}} \psi(\frac{v-t}{s}) dv \tag{3}$$

Here $\psi(\frac{v-t}{s})$ is the dilation of the wavelet $\psi(t)$. The term $v - t = \tau$ is marginalize to the actual value of term s, written as a function of subcarrier f ,described mathematically as , $s = g_1(w) = g_2(f)$. The CWT of RF waveform for variances of CSI amplitude information are denoted as:

$$C_c(t, f) = \int_{-\infty}^{+\infty} x(t + kT)\psi(kT, f)d\tau \tag{4}$$

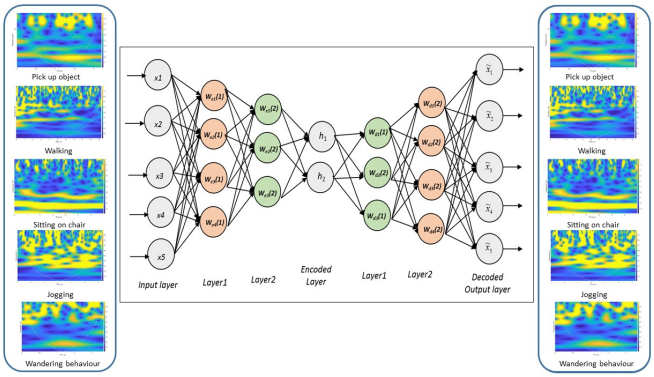


Fig. 5: Unsupervised deep autoencoder used classifying ADLs.

Where $x(KT)$ consist of CSI data samples having a time period $T = 1/F$, here F describes the sampling frequency. The CW of a discrete RF signal can be obtained by substituting the equation $x(kT)$ with expression $CSI^{SC}(kT)$, denoted as follows:

$$C_d(t,f) = T\sum_k CSI^{SC}x(t+kT)\psi(kT,f)d\tau \tag{5}$$

The value of f (as in following equation) is set as 50 Hz, that acts as the sampling frequency of the CSI amplitude data and the time T is set to 0.05 seconds. We have used the mother or the "morse" wavelet. The time-frequency information $E(t,f)$ can further mathematically written as follows :

$$E = C_d(t,f) \times C_d^*(t,f) \tag{6}$$

$$E = T^2\sum_{k1}\sum_{k2} CSI^{SC}x(t+k_1T) \\ CSI^{SC^*}x(t+k_2T)\psi(k_1T,f)\psi^*(k_2T,f) \tag{7}$$

The continuous wavelet transform scalograms present high-resolution analysis that are inherently independent of size of time window that result in distinct dilation of mother wavelet. The scalograms provide adequate variances in the context of of amplitude information when the patient is experiencing wandering behaviour and deliver course-grain resolution as it uses slim time window size at RF frequencies. Moreover, the scalogram can potentially predict fine-grained time-frequency features in Wi-Fi signals due to large time window at lower frequencies. The scalograms presented in Fig. **??** are generated using logarithmic scale of frequency domain.

C. Autoencoder for Scalogram Classification

One of the major challenges academics and researchers face is the availability of small datasets made up from radio frequency signals obtained for healthcare applications. These arise due to ethical approval issues and limited number of subjects and volunteers available. In order to achieve our objectives with restricted datasets, we have applied the unsupervised algorithm called autoencoder network that provide the best performance when exposed with limited number of training samples. The autoencoder algorithm deliver input data at the output as presented in Fig. 5. For instance, for input value x, the objective of this classifier is to find out a optimized model namely, $hw(x) \approx x$. This unsupervised algorithm was designed to initialize the weights and biases of an autoencoder that was highly robust and time efficient when a small number of training samples provided (as in our case). The autoencoder uses data processing (pre-training) by encoding and decoding the given data, respectively. It also calculates a nonlinear mapping on input value x, denoted as:

$$z_i = \sigma(\hat{W}e_i + \tilde{b}) \tag{8}$$

Here $\hat{W}$ and $\tilde{b}$ are weights and biases, respectively. The autoencoder classifier tries to reduce the error rate by minimizing the following values:

$$J(\theta) = \frac{1}{N}\sum_{i=1}^{N}(x_i - z_i)^2 \tag{9}$$

To get optimum performance from the network, the cost function with a sparsity parameter is applied, in order to put the network to learn the correlation when distinct inputs data are provided. The cost function can be mathematically written as follows:

$$gmin_{(\theta)}J(\theta) = \frac{1}{N}\sum_{i=1}^{N}(x_i - z_i)^2 + \beta\sum_{i=1}^{N}KL(p||p_l) \tag{10}$$

Here h indicate the total number of hidden neurons in autoender, β is the sparsity proportion and KL denote Kullback-Leibler divergence that can be described as:

$$KL(p||p_l) = p\log(\frac{p}{p_j}) + (1-p)\log(\frac{1-p}{1-p_j}) \tag{11}$$

For training and test autoencoder algorithm, the data used for unbalanced that was acquiried using Wi-Fi sensing in terms of channel state information. For training and test autoencoder algorithm, the data used for unbalanced that was acquiried using Wi-Fi sensing in terms of channel state information.

III. The Proposed Encryption Scheme

The main reason behind applying novel encryption scheme and securing patient data is due to the fact that nearly one thousand patient data breaches occurred in 2018, among the most notable one was when more than 193 million personal records were exposed to fraud and identity theft. The top three breaches of data security were from the health care industry. The largest medical and healthcare patient data breach was recorded in healthcare insurance company namely, Anthem. The breach exposed the patients personal records — including names, birth dates, Social Security numbers, home addresses and other personal info — of 78.8 million current and former members and employees of Anthem.

Preservation of privacy in healthcare and patient monitoring has emerged as an absolute prerequisite for exchanging

confidential information in terms of data analysis, validation, and sharing with care-takes, nurses or doctors. In this context, the scalograms collected from Wi-Fi signals are encrypted using modified Logistic and Dynamic Newton Leipnik maps. The step-by-step method of encryption of the scalogram data is given in Fig. 7 in details. The two fundamental steps that are important for the encryption process are, i.e., confusion and diffusion can see from Fig. 7 that are deployed for protecting preserving privacy of patients from eavesdroppers. The basic schematic chart of an image encryption is shown in Fig. 6. The schematic chart shows that two components are necessary to complete a cryptosystems (i) Key and (ii) Secure algorithm. The most important is a private key in case of symmetric key encryption, i.e., the key is used to secure the original content. The second important component is a secure algorithm that is designed to encrypt digital images using a private key.

1) Logistic Chaotic Map: The Logistic chaotic map (LCM) or logistic polynomial mapping (LPM) of degree two is one of the extensively employed discrete chaotic maps that was designed by Belgium born Pierre Francois Verhulst [15]. The non-linear chaotic map was reported in the year 1976 when it was studied by one of the notable biologists Robert May in his paper. The simple non-linear one-dimensional discrete map is sufficiently adopted as a researched map for the generation of robust cryptosystems and hybrid systems for image encryption. Mathematically the chaotic map can be defined as:

$$x_{n+1} = r(x_n)(1 - x_n) \tag{12}$$

whereas in the aforementioned Eq. 12, the sequence of random numbers are generated at its conventional state, i.e., when the initial conditions are set. The initial condition $x_n \in [0, 1]$. The control parameter r generates random numbers when r is risen from 0 to 3.54. The range of $r \in [3.54, 4]$ is the specific chaotic range, which generates maximum randomness. The system produces no more random sequences fording a value of 4.

2) Gaussian Map: The chaotic Gauss map, which is also known as the Gaussian's map or mouse map, is the real interval chaotic non-linear iterative map. The Gaussian's map is extensively utilized for image encryption applications due to its more favorable chaotic properties suitable for image security. The map is defined as:

$$x_{n+1} = exp(-\alpha(x_n)^2) mod 1 \tag{13}$$

whereas, in the preceding Eq. 13, $\alpha \in [4.7, 17]$, and $c \in [-1, 1]$. The system is developed using Gaussian noise function (GNF) employing mathematical assumptions. The system is considered insufficient due to its insignificant range. The chaotic range having its control parameter c containing chaotic randomness should be high for any dynamic system; thus, the system can work more efficiently in hybrid systems.

3) Logistic Gaussian System: Logistic Gaussian system (LOGAS) is developed by [16] by the combination of two chaotic maps to increase randomness in the proposed technique. The system is defined as:

$$X_{n+1} = (-(r - 33)x_n(1 - x_n) + ((r + 37)/4) + exp(-\alpha(x_n)^2) mod 1 \tag{14}$$

whereas in the Eq, as mentioned earlier 14, $x_n \in [0, 1]$, $r \in [0, 5]$ and $\alpha \in [4.7, 17]$. The specific range of $[0, 5]$ is examined, which is generated by the combined effect of two chaotic maps. As a result, chaotic characteristics are increased, thus produced good chaotic sequences with its maximum Lyapunov exponent is achieved with the condition is set to $\lambda \in 2.5$.

A. Dynamic Newton Leipnik System

The paper [17] described a various number of fractional derivative equations with its dynamical behavior. The Caputo type of fractional derivative shows better dynamical behavior as corresponded to others. The system is appropriated for image encryption which is defined in [18] and [19].

$$D_x^a y(x) = J^{m-a} y^{(m)}(x), \quad \alpha > 0 \tag{15}$$

whereas, in the above Eq. 15, $m = \alpha$ is the output value, which is in the fractional form that is moreover rounded to its most approaching integer value. The derivative of order y is calculated using the m^{th} derivative of integer m.

$$J^\beta z(x) = \frac{1}{\Gamma(\beta)} \int_0^x (x - t)^{\beta - 1} z(t) \mathrm{d}t \tag{16}$$

In the proceeding Eq. 16, is Riemann-Liouville integral operator have the order $\beta > 0$ and $\Gamma(\beta)$ is gamma function.

Several researchers employed the subsequent equalization that is defined as:

$$D^x y(x) = \frac{\mathrm{d}^m}{\mathrm{d}x^m} J^{m-x} y(x) \tag{17}$$

The three-state variables are utilized for the generation of a secure system based on non-linear differential equations. Newton Leipnik dynamical system (NLDS) is defined as [18] and [19]:

$$\begin{cases} \dot{x} = -ax + y + 10yz \\ \dot{y} = -x - 0.4y + 5xz \\ \dot{z} = bz - 5xy \end{cases} \tag{18}$$

whereas the preceding equation exhibits that x, y, and z are three observed state variables while a and b are positive parameters. The two strange attractors are generated appropriating the following conditions, which are as follows. The value of (a,b) = (0.4, 0.175) with its starting conditions $(0.349, 0, -0.16)$ and $(0.349, 0, -0.18)$. The system is defined as in [18] and [19].

The standard derivative has superseded the fractional-order derivative of the Newton-Leipnik system, which is defined as:

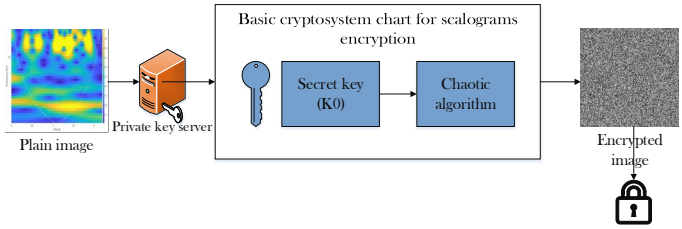


Fig. 6: Basic schematic chart of scalogram image encryption process.

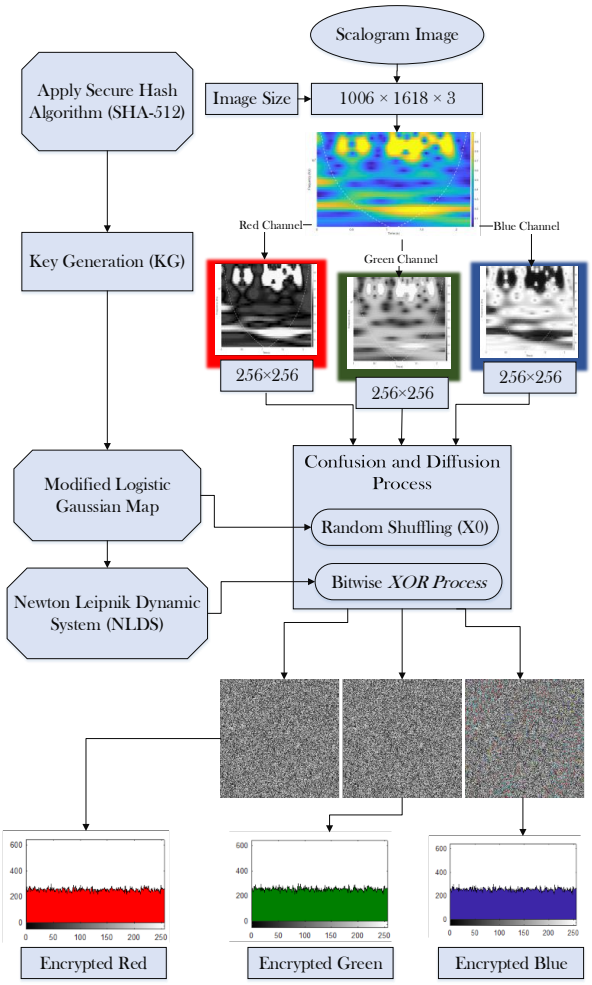


Fig. 7: Flowchart of the encryption process.

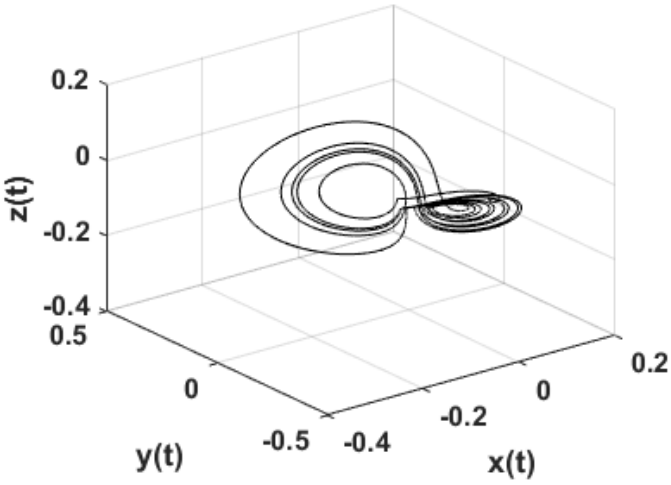


Fig. 8: Dynamic Newton leipnik system with its maximum randomness state.

$$\begin{cases} \frac{d^{e} i_{x}}{d^{m}} = -ax + y + 10yz \\ \frac{d^{2} 2y}{dr^{*}} = -x - 0.4y + 5xz \\ \frac{d^{Gx}}{dx^{g}} = bz - 5xy \end{cases} \tag{19}$$

The generated Leipnik attractor is shown in above Fig. 8 when the value of $\alpha = 0.95$. Newton Leipnik system has several advantages over the traditional chaotic systems:

1) Newton Leipnik displays strange attractors based on initial conditions.

2) The chaotic system based on Newton Leipnik is completely random which is evident from a number of parameters such as positive Lyapunov exponents, recurrence analysis and peak-to-peak dynamics.

3) Based on parametric values, Newton-Leipnik system provides more than one strange attractors and hence it can provide more randomness.

4) The random values produced via Newton Leipnik is dependent on initial conditions as well as on parameter condition of the systems. Only changing the parametric value can produce different chaotic values.

5) Various statistical parameters such as chi-square, frequency and correlation tests prove the security and robustness of Newton Leipnik system.

6) Newton Leipnik system can generate chaotic motions, transient chaos and periodic motions.

B. Encryption Steps

1: Plain scalogram image of walking back and forth image is considered during the experiments with a size of $1006 \times 1618 \times 3$ in the proposed cryptosystem.

2: The scalogram image is further resized to $256 \times 256 \times 3$ dimension and is subsequently divided into its respective three layers of red layer, green layer, and blue layer, as shown in Fig. 9.

3: In the third step, the secure key is generated using a hash function through SHA-512.

4: We utilized modified chaotic maps that are designed using two simple maps, i.e., logistic map and Gaussian map are

TABLE I: Evaluation of the scheme through a number of security parameters.

Security Parameter	Original pick up scalogram	Encrypted pickup scalogram	Original walking scalogram	Encrypted scalogram
$Corr\ Coff$ (H)	0.9713	0.0001	0.9414	0.0011
$Corr\ Coff$ (V)	0.9547	-0.0001	0.9120	0.0004
$Corr\ Coff$ (D)	0.9807	0.0001	0.9676	0.0016
MSE	NA	8.1977×10^{03}	NA	7.9453×10^{03}
$PSNR(db)$	NA	26.3094	NA	26.6319
NAE	NA	0.9583	NA	0.4751
MAE	NA	154	NA	152
NCC	NA	1	NA	1
SC	NA	1.4047	NA	1.2791
AD	NA	53.4560	NA	48.4724
MD	NA	255	NA	255
$Entropy$	7.1364	7.79980	7.2461	7.9980
$Entropy(R)$	6.6181	7.79971	6.6437	7.9970
$Entropy(G)$	6.6702	7.79968	7.0246	7.9967
$Entropy(B)$	6.7184	7.79970	6.8107	7.9973
$Key\ Sensitivity$	NA	99.4311%	NA	99.6735%
$NPCR$	NA	99.4362 %	NA	99.6575%
$UACI$	NA	33.2151	NA	33.4512
$Contrast$	1.6186	10.0731	1.6889	10.5830
$Homogeneity$	0.8059	0.4228	0.7866	0.3944
$Energy$	0.1067	0.0197	0.1405	0.0162

TABLE II: Optimized parameters for autoencoder - (scalograms/ Wi-Fi Sensing)

#	Width	Depth	Accuracy
1	20	1	81.3
2	50	1	80.1
3	100	2	81.5
4	50-100	2	82.2
5	150-200	3	83.4
6	**50-100-200**	**3**	**94.2**
7	10-25-50-100	4	86.2
8	15-30-60-200	4	85.0
9	30-60-120-240	5	84.6
10	40-80-240-300	5	83.2
11	15-30-45-90-200-400	6	84.3
12	50-100-200-400-800	6	85.5

discussed earlier.

5: The modified logistic Gaussian system is practiced to shuffle the entire pixels of each channel at its initial stage that completed the confusion stage.

6: The extra layer of security is achieved when the random sequences are injected into another non-linear system, i.e., Newton Leipnik Dynamic System (NLDS). The high random sequence of chaotic hybrid maps is bit-wise XOR for each channel.

7: Finally, the three split layers are encrypted employing secure Hash (SHA-512), modified logistic Gaussian map (LOGAS), and Newton leipnik dynamic system (NLDS).

8: The histogram of each channel is shown in Fig. 16, 10, and 12. The up and down pixels, as shown in Fig. 10 describes that information is exposed to the attacker while Fig. 12, with its uniform pattern of pixels, exhibits that the examination of pixels learning is improbable; thus, the secure cryptosystem is achieved using the proposed technique.

C. CONFUSION AND DIFFUSION PROCESS

In 1949, Claude Shannon [20] introduced the combined effect of confusion of diffusion. The duo connected property increased the overall security of the system. The property of confusion has permuted the entire pixels of an image;

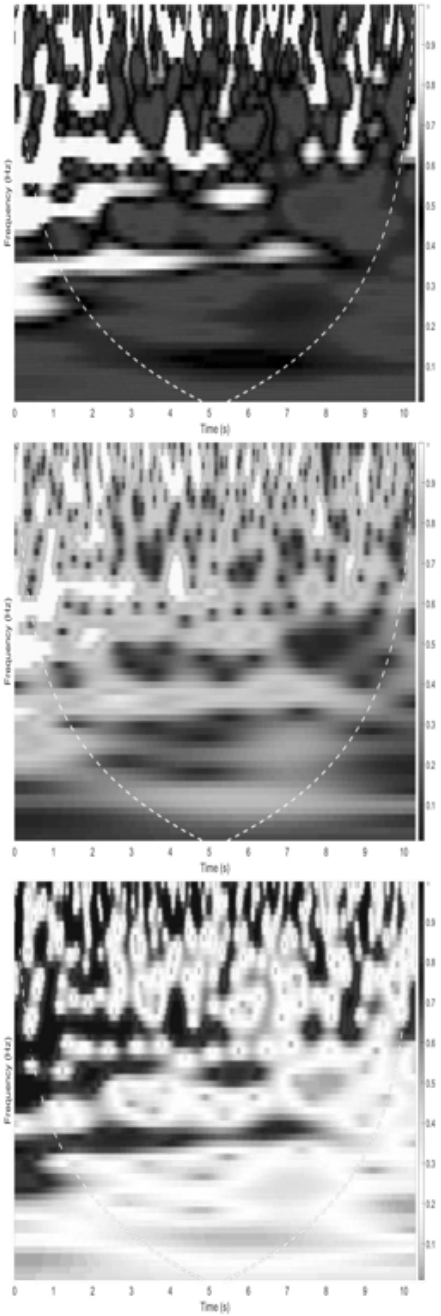


Fig. 9: Plain three layers (red, green, blue) of walking back and forth scenario.

subsequently, the process of diffusion process has substituted the original image pixels, i.e., the entire pixels are distorted and actual value of the pixel is changed as shown in Fig. 16 which ensures that each pixel value is changed from its original value. The uniform distribution of pixels also ensured that the proposed cryptosystem is generating highly random sequences for the better diffusion process. The proposed cryptosystem is also applied to various scenarios, e.g., picking up the object, jogging, sitting on the chair, and wander behavior (leaving room). The plain images are shown in Fig. 4, while the respective encrypted channels using the property of confusion and diffusion, as shown in Fig. 17. The image security test

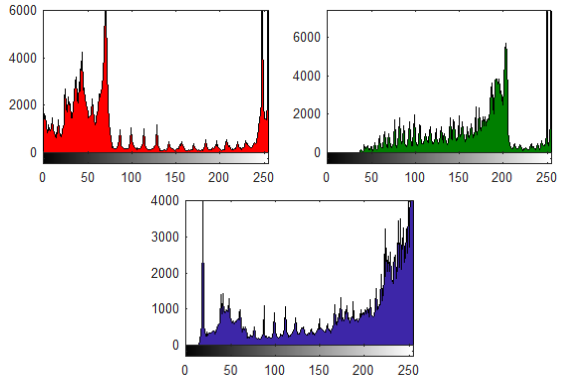


Fig. 10: Histogram of plain three layers (red, green, blue) of walking back and forth scenario.

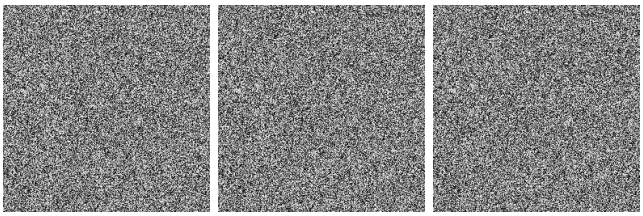


Fig. 11: Encrypted three layers (red, green, blue) of walking back and forth scenario.

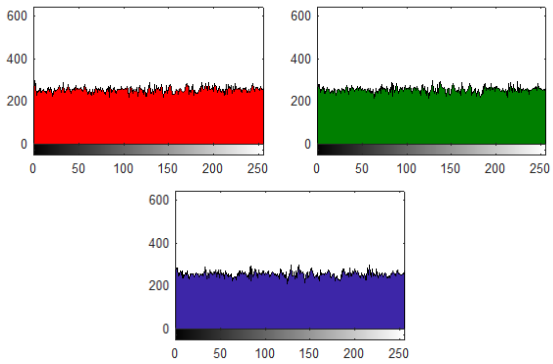


Fig. 12: Histogram of encrypted three layers (red, green, blue) of walking back and forth scenario.

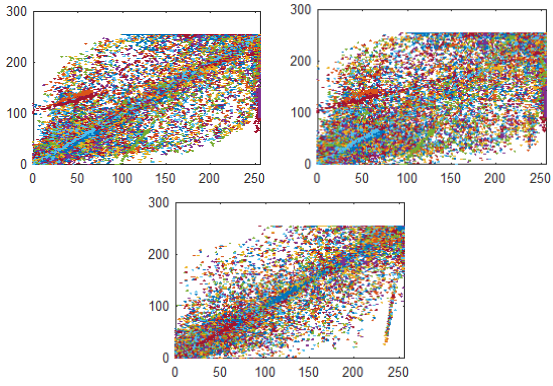


Fig. 13: Plain image correlation coefficient of three directions (horizontal, diagonal, vertical) for walking back and forth scenario.

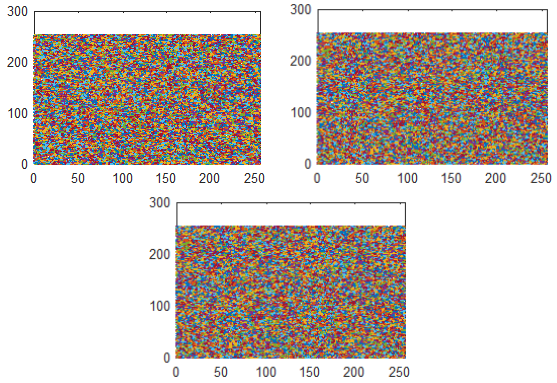
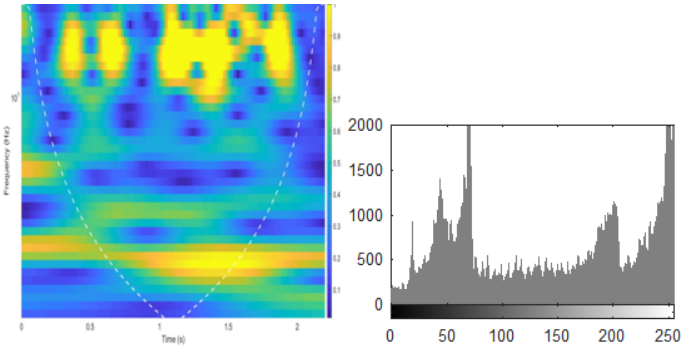


Fig. 14: Encrypted image correlation coefficient of three directions (horizontal, diagonal, vertical) for walking back and forth scenario.



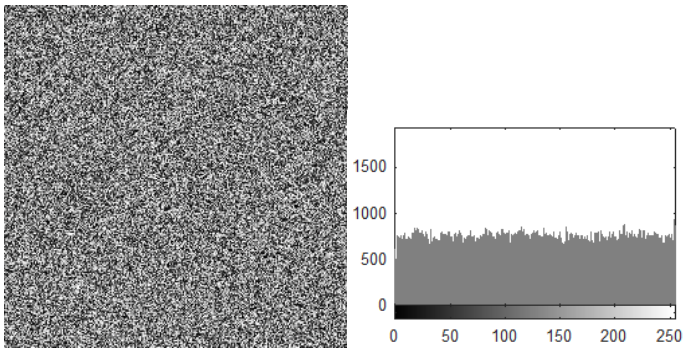
(a) Plain: Walking back and forth (b) Plain: Histogram of walking back and forth

Fig. 15: Plain and encrypted image with its histograms.

is examined using various tests, including the correlation coefficient. The test results are shown in Fig. 13 and 14. Fig. 13 is showing that the pixels are highly correlated in the case of a plain image. The pixels are scattered in case of the encrypted image. The entire scattering of pixels in Fig. 14 shows that the maximum randomized sequences are generated. The values of correlation between plain and encrypted images for three directions are shown in Table I. The proposed scheme is validated using several tests that are shown in Table I.

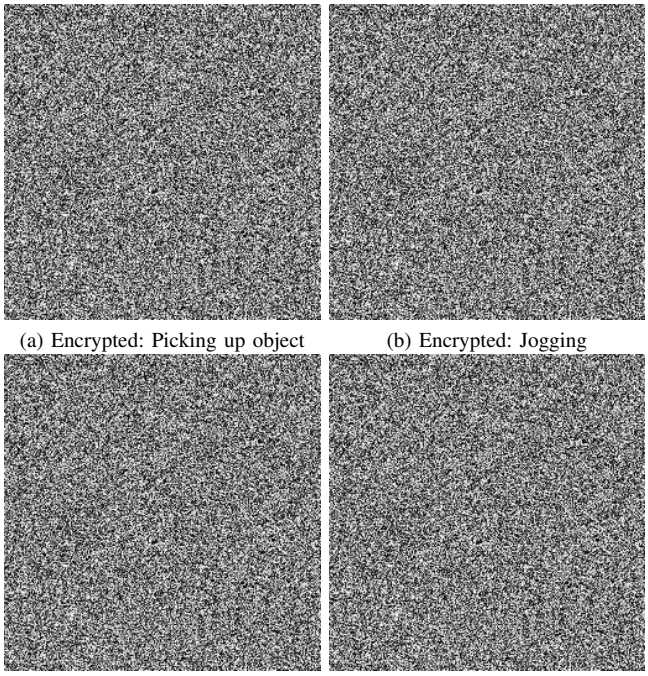
IV. Classification Results

We have implemented the autoencoder model in MATLAB tool where training, validation and testing was performed on scalograms generated from Wi-Fi signals. The neural network was trained for 200 epochs with a minibatch size of 90. The performance accuracy of the proposed system was obtained by dividing 20% of the training datasets as the validation set and the model was evaluated after the completion of each iteration. The adaptive moment estimation technique was used for optimization the given datasets during the pre-training stage for a fine-tuning learning rate of 0.002. The grid search method was used during the process where optimized values for width and depth overcoming the overfitting is shown in Table II. The three-layer unsupervised autoencoder with layers depth of of 200, 100 and 50, respectively. The optimum classification



(a) Encrypted: Walking back and forth (b) Encrypted: Histogram of walking back and forth

Fig. 16: Plain and encrypted image with its histograms.



(a) Encrypted: Picking up object (b) Encrypted: Jogging

(c) Encrypted: Sitting down on chair (d) Encrypted: Wander behaviour (Leaving room)

Fig. 17: Encrypted scalogram results for different scenarios.

performance in terms of percentage accuracy is 91.1% as highlighted in Table II.

V. Conclusion

This paper presented a novel system for monitoring of wandering behaviour in dementia patients and reported abnormal events exploiting using low-cost small wireless devices operating at 2.4 GHz. We argue that this first work that used ubiquitous wireless devices to monitoring dementia patients indoor settings. Activities of daily living were detected exploiting variances of amplitude information. The amplitude information extracted from CSI data is stable and consistent. However, the phase information consist random noise and are inapplicable for monitoring dementia patients.A continuous wavelet tranform was applied on CSI amplitude information to obtained scalograms that were treated as images to train the

unsupervised neural network namely Autoencoder.The system would work in outdoor environment as well as long as Wi-Fi transmitter and the wireless devices used operating at 2.4 GHz are used. A modified Logistic and Dynamic Newton Leipnik Maps encryption scheme was used to encrypt the data obtained from dementia patient in order to preseve the privacy.The proposed system provided high classificatoin accuracy of more than 94% each time trial was performed. Furthermore, it was noticed that the system was extremely robust in terms of security that was tested against multiple parameters including correlation coefficient (0.0001), number of pixel change rate (99.9%), unified average change intensity (33.2), energy (0.01) and contrast (10).

VI. Acknowledgement

This work is supported in parts by EPSRC EP/T021020/1 and EP/T021063/1.

References

[1] G. Tsang, X. Xie, and S. Zhou, "Harnessing the power of machine learning in dementia informatics research: Issues, opportunities, and challenges," *IEEE Reviews in Biomedical Engineering*, vol. 13, pp. 113–129, 2020.

[2] J. Alcalá, J. Ureña, Hernández, and D. Gualda, "Event-based energy disaggregation algorithm for activity monitoring from a single-point sensor," *IEEE Transactions on Instrumentation and Measurement*, vol. 66, no. 10, pp. 2615–2626, Oct 2017.

[3] M. R. Ahmed, Y. Zhang, Z. Feng, B. Lo, O. T. Inan, and H. Liao, "Neuroimaging and machine learning for dementia diagnosis: Recent advancements and future prospects," *IEEE Reviews in Biomedical Engineering*, vol. 12, pp. 19–33, 2019.

[4] A. Ferrari, D. Micucci, M. Mobilio, and P. Napoletano, "On the personalization of classification models for human activity recognition," *IEEE Access*, vol. 8, pp. 32 066–32 079, 2020.

[5] S. A. Shah and F. Fioranelli, "Rf sensing technologies for assisted daily living in healthcare: A comprehensive review," *IEEE Aerospace and Electronic Systems Magazine*, vol. 34, no. 11, pp. 26–44, Nov 2019.

[6] S. Suijkerbuijk, R. Brankaert, Y. A. W. de Kort, L. J. A. E. Snaphaan, and E. den Ouden, "Seeing the first-person perspective in dementia: A qualitative personal evaluation game to evaluate assistive technology for people affected by dementia in the home context," *Interacting with Computers*, vol. 27, no. 1, pp. 47–59, Jan 2015.

[7] C. Lin, P. Lin, P. Lu, G. Hsieh, W. Lee, and R. Lee, "A healthcare integration system for disease assessment and safety monitoring of dementia patients," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 5, pp. 579–586, Sep. 2008.

[8] S. Zhou, W. Zhang, D. Peng, Y. Liu, X. Liao, and H. Jiang, "Adversarial wifi sensing for privacy preservation of human behaviors," *IEEE Communications Letters*, vol. 24, no. 2, pp. 259–263, 2019.

[9] X. Yang, D. Fan, A. Ren, N. Zhao, and M. Alam, "5g-based user-centric sensing at c-band," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 5, pp. 3040–3047, 2019.

[10] X. Yang, D. Fan, A. Ren, N. Zhao, Z. Zhang, D. Haider, M. B. Khan, and J. Tian, "Non-contact early warning of shaking palsy," *IEEE Journal of Translational Engineering in Health and Medicine*, vol. 7, pp. 1–8, 2019.

[11] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, no. 1, pp. 1–10, 2017.

[12] Y. Gu, F. Ren, and J. Li, "Paws: Passive human activity recognition based on wifi ambient signals," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 796–805, Oct 2016.

[13] X. Yang, S. A. Shah, A. Ren, N. Zhao, J. Zhao, F. Hu, Z. Zhang, W. Zhao, M. U. Rehman, and A. Alomainy, "Monitoring of patients suffering from rem sleep behavior disorder," *IEEE Journal of Electromagnetics, RF and Microwaves in Medicine and Biology*, vol. 2, no. 2, pp. 138–143, 2018.

[14] L. Liu, S. A. Shah, G. Zhao, and X. Yang, "Respiration symptoms monitoring in body area networks," *Applied Sciences*, vol. 8, no. 4, p. 568, 2018.

[15] N. Bacaër, "Verhulst and the logistic equation (1838)," in *A Short History of Mathematical Population Dynamics*. Springer, 2011, pp. 35–39.

[16] Y. P. K. Nkandeu and A. Tiedeu, "An image encryption algorithm based on substitution technique and chaos mixing," *Multimedia Tools and Applications*, vol. 78, no. 8, pp. 10 013–10 034, 2019.

[17] I. Podlubny, *Fractional differential equations: an introduction to fractional derivatives, fractional differential equations, to methods of their solution and some of their applications*. Elsevier, 1998.

[18] R. Leipnik and T. Newton, "Double strange attractors in rigid body motion with linear feedback control," *Physics Letters A*, vol. 86, no. 2, pp. 63–67, 1981.

[19] L.-J. Sheu, H.-K. Chen, J.-H. Chen, L.-M. Tam, W.-C. Chen, K.-T. Lin, and Y. Kang, "Chaos in the newton–leipnik system with fractional order," *Chaos, Solitons & Fractals*, vol. 36, no. 1, pp. 98–103, 2008.

[20] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.