




Article

Privacy-Preserving Non-Wearable Occupancy Monitoring System Exploiting Wi-Fi Imaging for Next-Generation Body Centric Communication

Syed Aziz Shah ¹, Jawad Ahmad ^{2,*}, Ahsen Tahir ³, Fawad Ahmed ⁴, Gordon Russell ² , Syed Yaseen Shah ⁵, William J. Buchanan ² and Qammer H. Abbasi ⁶

¹ School of Computing and Mathematics, Manchester Metropolitan University, Manchester M13 9PL, UK; s.shah@mmu.ac.uk

² School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK; g.russell@napier.ac.uk (G.R.); B.Buchanan@napier.ac.uk (W.J.B.)

³ Department of Electrical Engineering, University of Engineering and Technology, Lahore, Punjab 39161, Pakistan; ahsenkn001@gmail.com

⁴ Department of Electrical Engineering, HITEC University Taxila, Punjab 47080, Pakistan; fawad@hitecuni.edu.pk

⁵ School of Computing, Engineering and Built Environment, Glasgow Caledonian University, Glasgow G4 0BA, UK; yasinshah@gmail.com

⁶ School of Engineering, University of Glasgow, Glasgow G12 8QQ, UK; Qammer.Abbasi@glasgow.ac.uk

* Correspondence: J.Ahmad@napier.ac.uk

Received: 11 March 2020; Accepted: 26 March 2020; Published: 3 April 2020

Abstract: Nano-scaled structures, wireless sensing, wearable devices, and wireless communications systems are anticipated to support the development of new next-generation technologies in the near future. Exponential rise in future Radio-Frequency (RF) sensing systems have demonstrated its applications in areas such as wearable consumer electronics, remote healthcare monitoring, wireless implants, and smart buildings. In this paper, we propose a novel, non-wearable, device-free, privacy-preserving Wi-Fi imaging-based occupancy detection system for future smart buildings. The proposed system is developed using off-the-shelf non-wearable devices such as Wi-Fi router, network interface card, and an omnidirectional antenna for future body centric communication. The core idea is to detect presence of person along its activities of daily living without deploying a device on person's body. The Wi-Fi signals received using non-wearable devices are converted into time–frequency scalograms. The occupancy is detected by classifying the scalogram images using an auto-encoder neural network. In addition to occupancy detection, the deep neural network also identifies the activity performed by the occupant. Moreover, a novel encryption algorithm using Chirikov and Intertwining map-based is also proposed to encrypt the scalogram images. This feature enables secure storage of scalogram images in a database for future analysis. The classification accuracy of the proposed scheme is 91.1%.

Keywords: Wi-Fi; privacy; occupancy; deep learning; encryption

1. Introduction

Nano-scaled structures, wireless sensing, wearable devices, and wireless communications systems are anticipated to support the development of new next-generation technologies in near future. The exponential rise in future Radio-Frequency (RF) sensing systems has demonstrated its applications in areas such as wearable consumer electronics, remote healthcare monitoring, wireless implants, and smart buildings. The advances of low-cost small electronic devices, wireless sensing systems, real-time monitoring, and the Internet of Things (IoT) has played the role of a catalyst that has

primarily expanded the horizon of these technologies. In this context, we introduce a privacy-preserving, device-free occupancy real-time occupancy monitoring system for energy optimizing in smart buildings.

The smart built environment essentially refers to the man-made environment providing the setting for different human activities including smart cities, large scale buildings, and beyond. It consumes a significant amount of electricity around the world and keeps on increasing day by day [1]. In this context, effective strategies are required to be developed in order to decrease the overall energy consumption while maintaining and improving the thermal comfort of occupants residing in buildings. Several studies indicate that smart lighting systems and Heating Ventilating and Air Condition (HVAC) save energy up to 30%, provided they work based on the suggestions given in [2]. The HVAC system can automatically turn off in unoccupied settings and the ventilation rate can be adjusted as well depending on the total number of occupants present to optimize the energy consumption. In addition to energy-saving, the adaptive crowd density control scheme can be applied by estimating occupant number in various places.

For example, optimized services provided at shopping malls, hotels, restaurants, and transportation stations can be allotted to improve customer care service. Crowd density control and counting can enhance the indoor evacuation process in emergency cases. Hence, the design of a low-cost, robust, accurate, safe, and secure occupancy monitoring system is of utmost importance that can count the number of occupants while keeping the privacy preserved. Presently, the majority of the occupancy monitoring and detection systems use infrared sensors. However, these systems present a huge number of false alarms when occupants are moving slowly. Furthermore, state-of-the-art occupancy detectors estimate the total number of people in the indoor environment as well. Camera-based systems [3] are one of the most used detectors. However, the person has to be in line-of-sight with sufficient light; dedicated cameras have to be deployed; and it raises privacy concerns as well. Several researchers have used Radio Frequency (RF) such as Bluetooth [4], Radio Frequency Identification (RF) [5], and sensor fusion [6] to detect occupants. The limitation of the aforementioned RF technologies is that a person has to carry RF or Bluetooth tags all the time within the area of interest. In addition to the limitation of RF sensing devices, some of the main advantages are that it is inexpensive, robust, and accurate with no issue of privacy. The ubiquitous Wi-Fi routers have been widely used for various application, ranging from remote health monitoring to fall detection, and so on [6–9]. The Wi-Fi technology is the best possible solution for occupancy monitoring in an indoor setting as it transmits the signal in omnidirections, covering almost the entire indoor area.

The Received Signal Strength Indicator (RSSI) obtained from Wi-Fi signals has been used to estimate occupants. The disadvantage of RSSI is that it suffers from coarse grain resolution, is highly susceptible to noise, and presents fluctuations, making it an infeasible solution for occupancy detection. On the other hand, channel state information extracted from Wi-Fi signals provide multiple frequency sub-channels, where one or more frequency carriers can be used to detect a person in an indoor environment. In this paper, we propose a novel low-cost, easily deployable, device-free, privacy-preserving Wi-Fi technology-based occupancy detection system using commercially available, off-the-shelf wireless devices such as Wi-Fi router, network interface card. and an omnidirectional antenna. In this research, two independent modules were implemented: (i) deep learning for occupancy detection; and (ii) chaos-based scalogram image encryption.

2. Related Work

Numerous researchers have introduced different RF sensing-based occupancy monitoring systems over the past few years [10–15]. In this regards, this section introduces some of the most commonly used RF sensing techniques to estimate the occupant within the area of interest, along with their advantages and limitations. For instance, the authors of [16] used Passive Infrared Sensor (PIR) to detect a person within the specific zone. The system identifies the presence of a person by estimating the variances in radiation emitted from the source (sensor in this case). Furthermore, Duarte et al. [17]

exploited the PIR device to measure occupancy in real-time at various zones, comprising of different rooms. Occupancy detection system using two PIR sensors were used in [18,19] to localize the occupant. The main advantage of this technology is its low cost and low power consumption level. However, the PIR sensor fails to detect intricate or stationary occupants due to its limited range resolution. Camera-based technology for occupancy monitoring is another method for crowd estimation and person monitoring. This system uses frames extracted from video recordings, where accurate and precise information about the occupant can be obtained. The image processing classification technique has three main essential steps: background score subtraction from the main body, movement detection, and occupant identification. The limitation of the vision-based technique is that it is dependent on the light intensity and the occupant has to be in line-of-sight of the camera, which raises privacy concerns as well. On the other hand, some researchers have used the Bluetooth Low Energy (BLE) module for crowd counting and occupancy estimation [4]. Deploying multiple iBeacons in the area of interest (indoor setting), the occupant can be estimated using RSSI in combination with machine learning algorithms such as support vector machine, K-nearest neighbor, etc.. The minimum requirement in the deployment of the BLE module is its biggest limitation to being implemented. To the best of the authors' knowledge, none of the existing monitoring systems consider the cost, easy deployment, security, and privacy preservation aspects. This paper addresses all the open areas that have not been addressed so far.

3. Security and Privacy in Body Centric Communication

Body centric communication systems need specific privacy and security protocol to ensure the privacy, confidentiality, and data integrity of a person's information. A supporting body centric communication infrastructure should deploy particular security measures that ensure all aforementioned features [20]. A comprehensive survey of main challenges (security and privacy) in wireless body area networks is presented in detail in [21]. Preserving and securing privacy of important data from adversaries without modifications, digital model learning, and sharing private information in body centric communication are extremely challenging. In an ideal world, the privacy preservation require available datasets always be secured from outside the data by the users. The private privacy should be enabled throughout the communication process of a given task. However, fool-proof ideal privacy preservation is impossible. For example, deploying fully-secured image encryption techniques including an AES-256 encryption scheme that is used to secure the available information from potential threats can harm typical delivering services in body area network. On the contrary, agreeing with simple and straightforward encryption schemes, such as information anonymization, is ineffective against breaches. The selection of encryption schemes also plays an important role in the designing of preserving data for next-generation body centric communications. Data and information protection schemes make space operations that are limited on the obscure data, while complex data protection techniques must be separate from simple schemes. For instance, a homomorphic encryption system is introduced in [22] to secure information using data mining techniques in the context of plain homomorphic multiplications. In addition, privacy-preserving schemes have a rapid rise in computational costs, thus often making it infeasible to be deployed in real-world applications. For instance, the overall cost of an effective multiplication-based homomorphic encryption algorithm transforming a plaintext number into a 256-byte ciphertext with a 1024-bit security key within 5 s sums to 1500 s for such encrypted ciphertexts. Hence, it is very important to divide the collective workload of encryption schemes to corresponding distributors in relation to the available resources.

4. Wi-Fi Sensing for Occupancy Monitoring

The received signal strength indicator and the Channel State Information (CSI) extracted are two of the most widely used types of information, applicable in various areas of wireless communication. RSSI measurements only present simple signal strength in the context of signal propagation, which is why this information is inadequate for occupancy monitoring due to its unstable nature. Zou et al. [23]

presented an occupancy monitoring system based on RSSI measurements that could obtain an overall accuracy of nearly 70%. On the contrary, the CSI measurements obtained using low-cost wireless devices provide fine-grained information by exploiting multiple frequency subcarriers [24]. The overall proposed architecture based on Wi-Fi signals is given Figure 1.

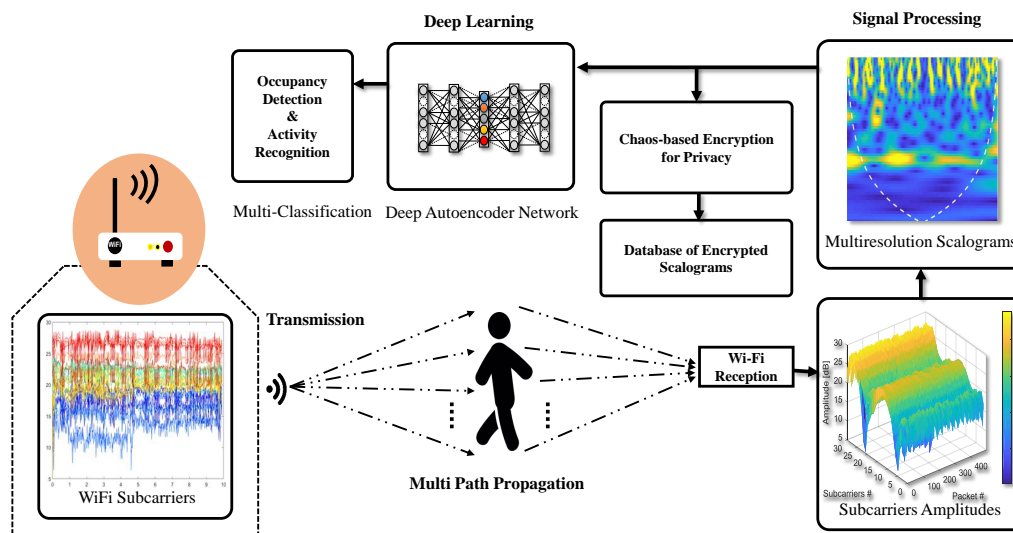


Figure 1. Architecture for an occupancy monitoring system based on Wi-Fi signals, driven by deep network.

The Wi-Fi technology powered by IEEE 802.11 a/a/ac utilizes Orthogonal Frequency Division Multiplexing (OFDM), effectively encountering the multipath propagation effect caused in indoor settings due to physical obstructions such as walls, ceiling, floor, etc. In OFDM, the frequency carrier is divided into multiple (orthogonal) subcarriers where the data stream [25,26]. The Wi-Fi signal received, i.e., the pass-band signal, is converted into message or baseband signal. The orthogonal frequency subcarriers are transformed into the frequency domain from the time domain by applying serial-to-parallel converter on RF signal, and Fast Fourier Transform (FFT) is then applied on all received subcarrier, as shown in Figure 2.

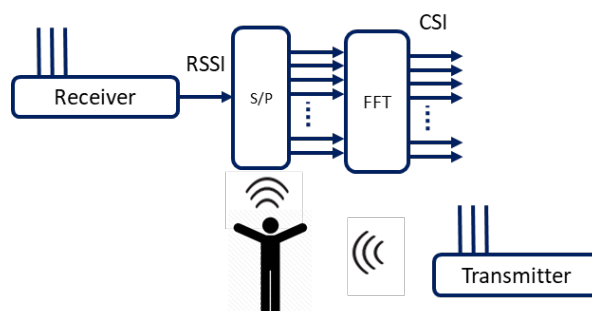


Figure 2. Frequency carrier conversion: time domain to frequency domain using RSSI/CSI.

A low-cost, off-the-shelf small wireless device, such as Atheros ar5b225, can be used to extract the CSI information from OFDM subcarriers. Open-source network interface card wireless device drivers reveal the measured CSI for all subcarriers, providing fine-resolution wireless channel information, comprising wireless medium characteristics including multipath fading, reflection, refraction, and shadowing effect.

Let H_i represent the CSI data for i th subcarrier that carries complex information and is denoted as follows:

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

where $|H_i|$ and $\angle H_i$ provide the variances of amplitude and phase information for i th frequency channel, respectively. The phase information extracted from CSI data for single frequency channel i , $\angle H_i$ is expressed as:

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

where β is the phase offset for i th frequency subcarrier and m_i is the frequency channel number. The internal noise of the network interface card and external noise is denoted 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. In this context, we only use variances of amplitude information extracted from CSI data. The raw CSI measurements for five different activities, including occupant leaving the room, are shown in Figure 3. The proposed system deals with interference produced by other devices working in the 2.4 GHz band (microwave ovens, alarms, remote controls, Wi-Fi networks used for communications, etc.). The technical reasons are discussed as follows:

- (1) Wi-Fi router is deployed closer to the receiving antenna.
- (2) We avoid using other wireless systems nearby common sources of interference, such as power cables, microwave ovens, fluorescent lights, and cordless phones.
- (3) We minimize the total number of live devices using the same RF band.
- (4) Deploying the Wi-Fi router close to the receiving antenna enables the receiver to get the maximum power, thus other nearby devices operating on same frequency do not affect the proposed system.

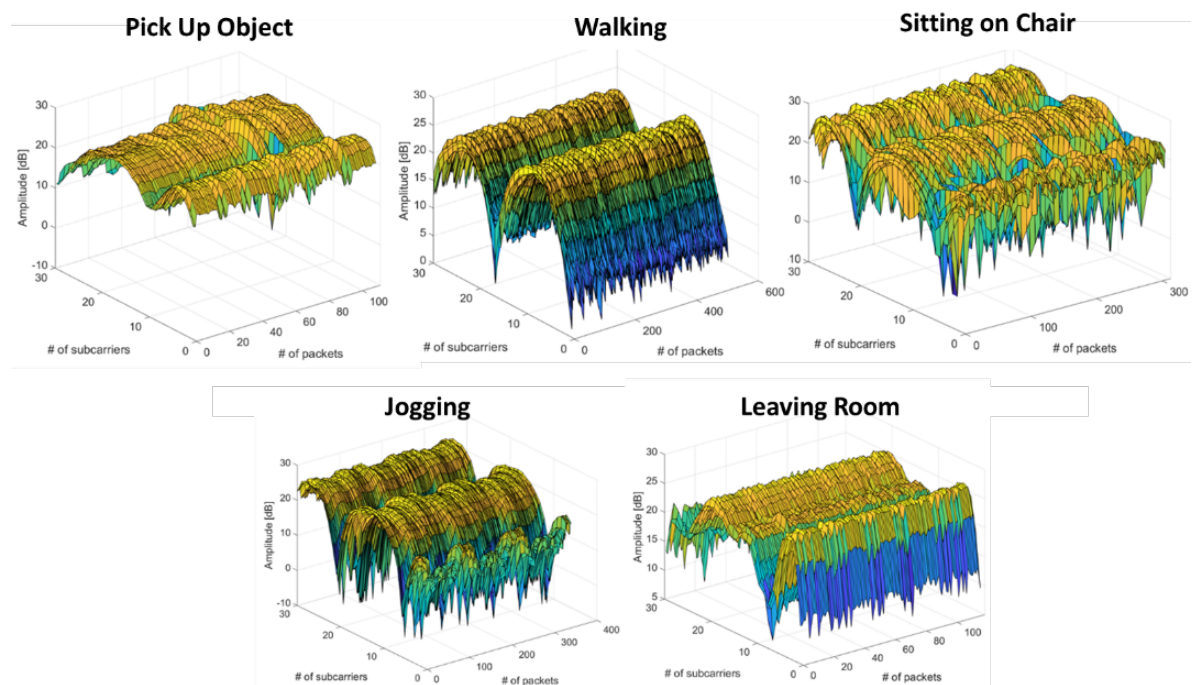


Figure 3. Variances of amplitude information against time and frequency domain.

4.1. Data Processing and Signal Acquisition

The channel station information recorded using the network interface card connected with the Wi-Fi router is discussed in this section. The CSI data are recorded from the data stream obtained from

the Internet Control Messages Protocol (ICMP) data. In principle, the overall recorded CSI data are the same when compared to the ICMP data stream. Nonetheless, it was noticed that marginally fewer CSI data packets were transmitted than ICMP packets. To synchronize the frequency of the recorded data packets, we applied linear transformation function on CSI data recorded in raw form. In theory, the OFDM subcarriers that Wi-Fi signal exploit should carry independent data. However, in practice, the neighboring frequency subchannels carry similar information most of the time. To detect occupancy and obtain separate information from each subcarrier, we applied principal component analysis (PCA) to get independent datasets for each observation. The CSI data stream can be easily incorporated into several independent principle components.

4.2. Experimental Setup and Trials

We conducted extensive experiments and trials in a hall, as described in Figure 4. The experiment was conducted on 15 subjects who were asked to do five ADLs. The age range of all subjects was 20–60 years. The transmitter (Wi-Fi router) and receiving antenna were placed 5 m away from each other at height of 1 m. The firmware introduced in [7] was used to record raw CSI and was installed in a desktop PC that continuously received OFDM packets. To identify occupants in indoor settings, we performed five sets of activities, as described above. Each human body movement brings a unique change in wireless channel that was inferred to identify activities performed by occupant in indoor environment.

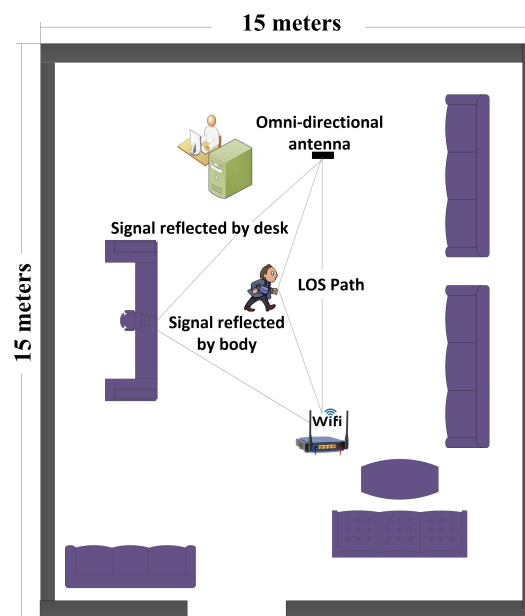


Figure 4. Experimental setup and trials for occupancy monitoring.

4.3. Scalogram for Activity Detection and Occupancy Estimation

The multiresolution scalograms, represented in terms of time–frequency, obtained from channel state information packets were used to estimate the occupancy within indoor settings. The scalograms are energy density function retrieved by applying Continuous Wavelet Transform (CWT) on 1000 CSI data packets. The energy density function $E(t, f)$ can be obtained from variances of the amplitude information of the CWT function $C_d(t, f)$ by applying a squaring function on a discrete sequence. The time–frequency measurement can be calculated from the CWT $C_c(t, s)$ of a Wi-Fi signal $x(t)$, denoted as time t and scale s , as described in Equation (3).

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

where $\psi(\frac{v-t}{s})$ is the dilation of the wavelet $\psi(t)$. The expression $v - t = \tau$ is scaled down to the value of s as denoted as a function of frequency f , given $s = g_1(w) = g_2(f)$. The continuous wavelet transform of Wi-Fi signal for CSI data packets are expressed in Equation (4):

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

where $x(KT)$ is a discrete sequence of samples with a time period $T = 1/F$, and the value of F represents the sampling frequency of an RF signal. The continuous wavelet transform of a discrete Wi-Fi signal can be acquired when the expression $x(kT)$ is substituted with $CSI^{SC}(kT)$, written as:

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

The value of f in Equation (6) was set to 60 Hz, i.e., the sampling frequency of variance of amplitude information of Wi-Fi signals, and the value of T was set to 03 ms. In this study, we chose mother wavelet, which is also known as the ‘‘morse’’ wavelet. The scalogram $E(t, f)$ of the Wi-Fi signals can be elaborated further as:

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

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

The CWT-based time–frequency scalograms provided fine-grained resolution analysis, independent of time window size. Consequently, they result in different dilations of morse wavelet. The time–frequency scalograms give significant variations in terms of CSI amplitude information due to the presence of an occupant within the indoor environment and give granular resolution due to small window time size at higher frequencies. Furthermore, the scalograms extracted have the potential to identify intricate features in RF signals due to large time window durations at lower RF frequencies. The scalograms shown in Figure 5 are produced against the frequency domain (logarithmic scale). The white dotted line represents the cone of influence that splits the region where edge effects are significant to identify occupant presence within the indoor environment.

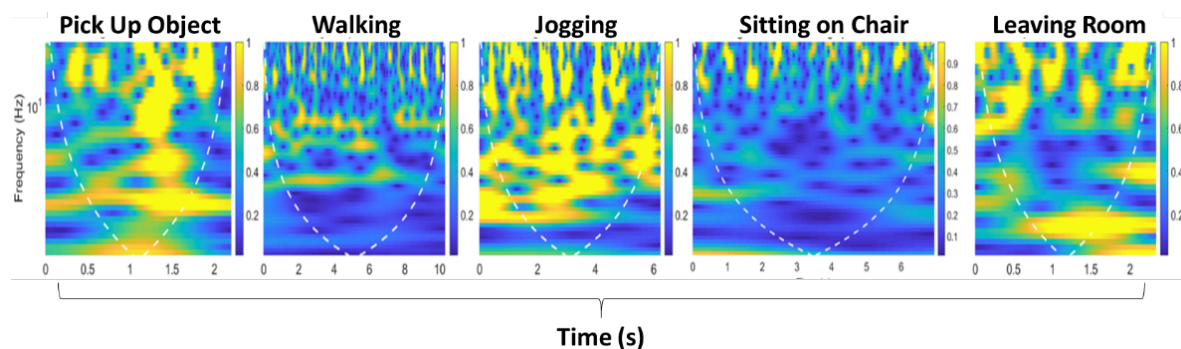


Figure 5. Scalograms obtained from variances of amplitude information when occupant for present in area of interest.

4.4. Autoencoder for Scalogram Classification

The biggest challenge that researchers face is the classification of RF signals due to the limited amount of data as a huge amount of time is required for data collection. To cope with the small number of observations, we used the autoencoder neural network, which delivers the best classification performance when exposed in such scenarios [27–29]. The autoencoder classifier provided the input data at the output, as shown in Figure 6. For example, for input value x , the neural network tries to find a function, namely, $hw(x) \approx x$. The unsupervised algorithm was introduced to initialize the

weights and biases of an autoencoder, which was extremely effective when limited training data were available. This algorithm implements unsupervised data processing (pre-training) by encoding and decoding the available datasets, respectively. It also estimates a nonlinear mapping on given datasets as an input x that is expressed as follows.

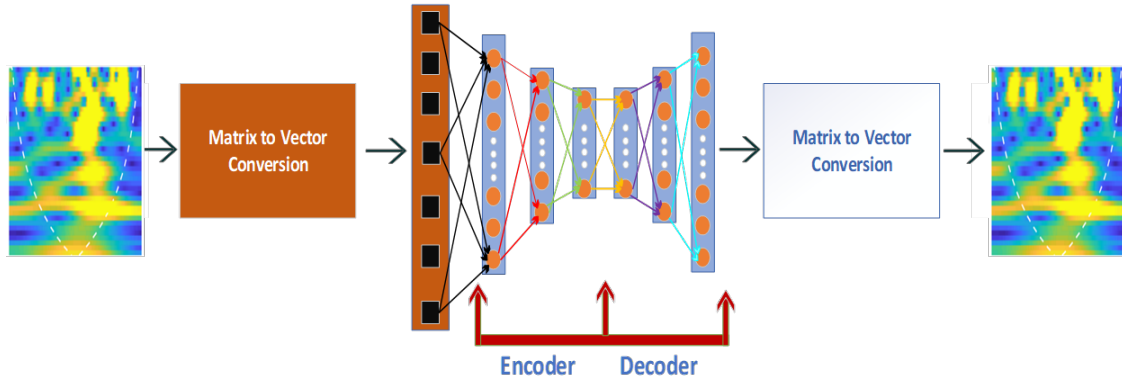


Figure 6. Deep autoencoder-based classification.

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

where \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 optimize the autoencoder neural network, cost function in conjunction with a sparsity parameter is implemented to drive the neural network for learning the correlation when different inputs are given [30]. In addition to the these parameters, the cost function can be expressed as follows:

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

where h denotes the number of hidden neurons, β is the sparsity proportion, and KL describes Kullback–Leibler divergence and can be expressed as follows:

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

4.5. The Proposed Encryption Scheme

The scalogram images are encrypted with lightweight Chirikov and Intertwining maps. The flowchart of the encryption process is highlighted in Figure 7. One can see in Figure 7 that both confusion and diffusion steps are deployed for protecting the privacy from eavesdroppers. Due to lightweight nature, pseudo-randomness, ergodicity, and dynamic behavior, the chaos-based algorithm is used in this work. Two chaotic maps, Chirikov standard map and Intertwining map, are used during the encryption. Mathematically, Chirikov standard map is written as:

$$\begin{cases} \alpha_{n+1} &= \alpha_n + K \sin \theta_n \pmod{2\pi} \\ \theta_{n+1} &= \theta_n + \alpha_{n+1} \pmod{2\pi} \end{cases} \tag{12}$$

where K is control parameter, and α_n and θ_n are real values between $(0, 2\pi)$. The constant coefficient K influences the degree of chaos exhibited by the map, as highlighted in Figure 8.

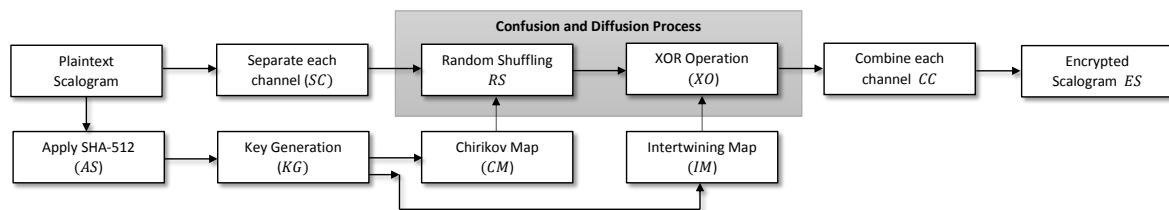


Figure 7. Flowchart of the encryption process.

Each plot is on the $\theta\alpha$ -plane, and it can be seen that increasing the value of K leads to a rich set of dynamics. It is obvious in Figure 8a that the map has regular values for $K = 0$. The chaotic region grows for higher values of K . In a chaotic cryptographic primitive, θ and p represent hidden inputs [31], with the other parameters akin to the group setting in Diffie–Hellman, the RSA prime, or the curve used in elliptic curve cryptography. The secret parameters are protected by the difficulty of determining (θ_0, α_0, K) given (θ_i, α_i, K) , after the chaotic map has been iterated i times. For a secure crypto-system, the keyspace should be more than 2^{100} . If the computational precision is 10^{-14} , the keyspace is $\approx 2^{140}$, which indicates that the output of the Chirikov standard map is secure against brute-force attack. Moreover, slightly different values of α cause different output, which highlights the key sensitivity of the chaotic map, as shown in Figure 9. The key sensitivity test illustrates the strength of the Chirikov standard map.

During the diffusion step, the intertwining map is used, which is written as:

$$\begin{aligned}
 x_{n+1} &= (\lambda \times \alpha \times y_n \times (1 - x_n) + z_n) \bmod(1), \\
 y_{n+1} &= (\lambda \times \beta \times y_n + z_n \times \frac{1}{1 + (x_{n+1})^2}) \bmod(1), \\
 z_{n+1} &= (\lambda \times (x_{n+1} + y_{n+1} + \gamma) \times \sin(z_n)) \bmod(1). \quad (13)
 \end{aligned}$$

where x_n, y_n , and $z_n \in (0,1)$, $0 \leq \lambda \leq 3.999$, $|\alpha| > 33.5$, $|\beta| > 37.9$, $|\gamma| > 35.7$.

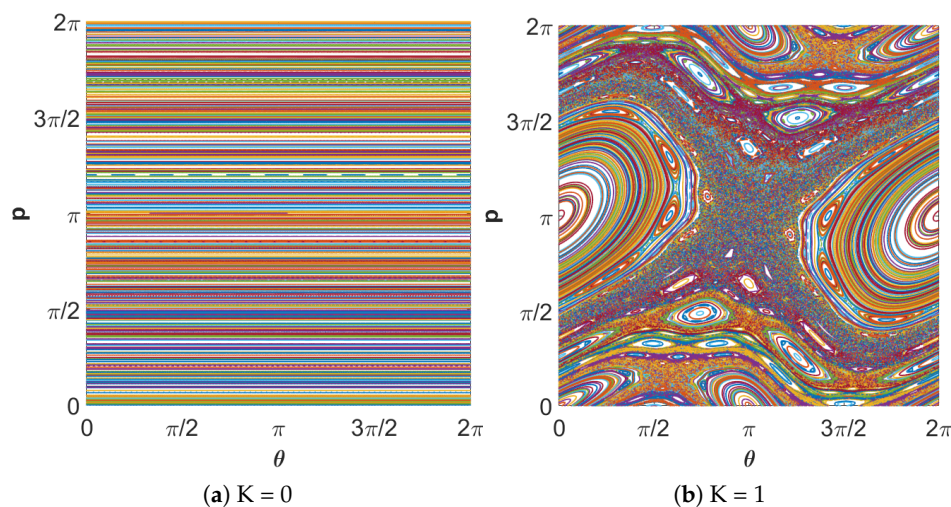


Figure 8. Cont.

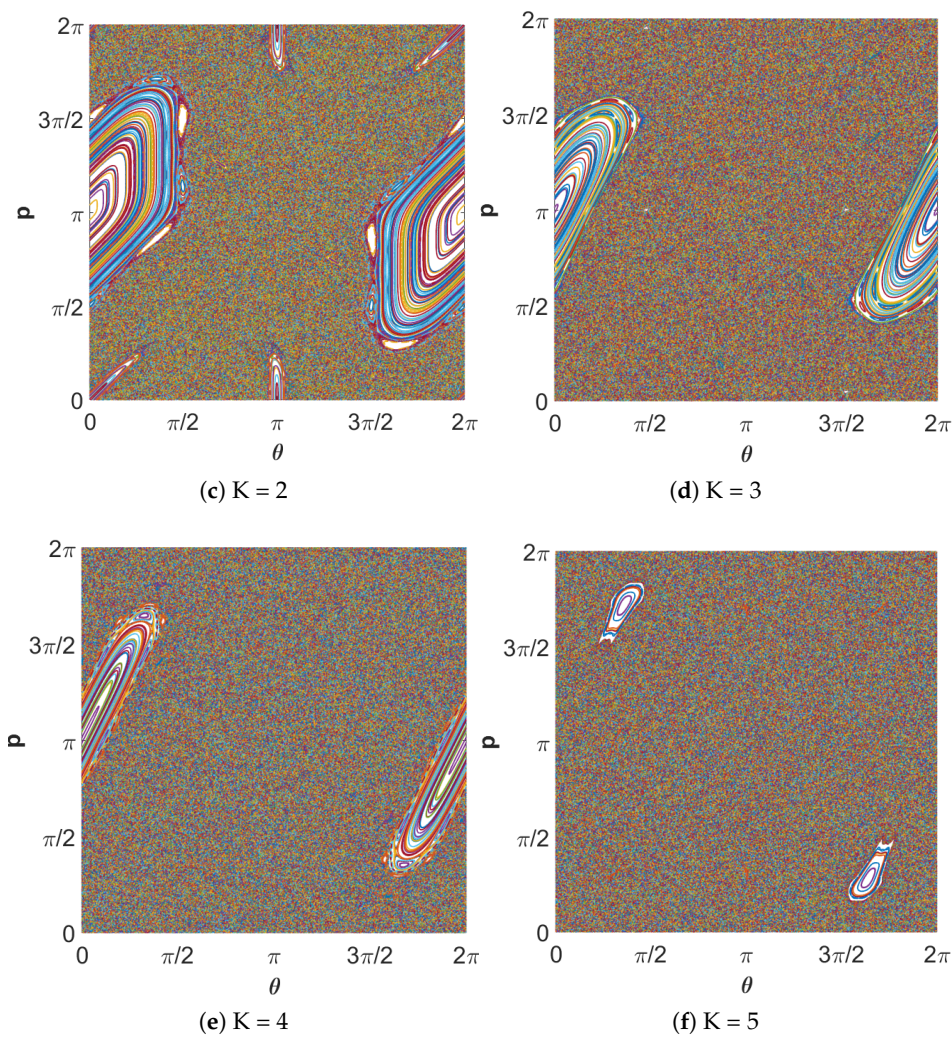


Figure 8. Chaotic orbits of the standard map for different values of K .

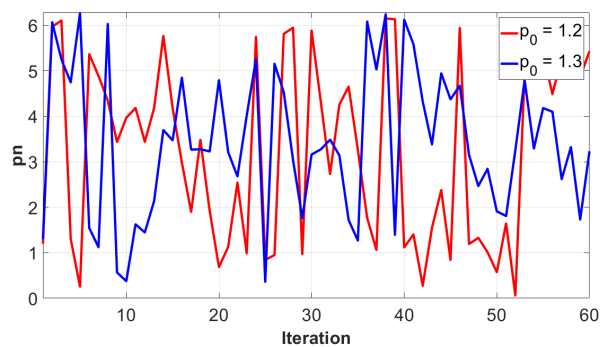


Figure 9. Output of Chirikov standard map for slightly different values of initial p .

Encryption Steps:

1. Let I be the original image scalogram having size $m \times n$. Apply SHA-512 to get a hash value for initial conditions that can be utilized in chaos maps.
2. Save SHA-512 results in ω . The hexadecimal value is $\omega = \omega_1\omega_2 \dots \omega_{128} = H1H2 \dots H128$, where $H1 = 2^0 \times 2^1 \times 2^2, \dots 2^{15}$.
3. Generate keys from the hash value. Convert hash value to decimal and apply modulus operation and set initial conditions for Chirikov standard map:

$$\alpha_i = \text{convert2decimal}(\omega_1\omega_2 \dots \omega_{32}).$$

$$\alpha_0 = \frac{\alpha_i}{\zeta} \bmod(2\pi), \text{ where } \zeta \text{ is } 3.40 \times 10^{38}.$$

$$\theta_i = \text{convert2decimal}(\omega_{33}\omega_{34} \dots \omega_{64}).$$

$$\theta_0 = \frac{\theta_i}{\zeta} \bmod(2\pi).$$

4. Set initial condition value for Intertwining map:

$$x_i = \text{convert2decimal}(\omega_{65}\omega_{66} \dots \omega_{96}).$$

$$x_0 = \frac{x_i}{\zeta} \bmod(1).$$

$$y_i = \text{convert2decimal}(\omega_{97}\omega_{98} \dots \omega_{128}).$$

$$y_0 = \frac{y_i}{\zeta} \bmod(1).$$

$$z_0 = (x_0 + y_0) \bmod(1).$$

5. Separate each red, green, and blue channel and save the results in ψ , δ , and η , respectively.
6. Iterate Chirikov map $3 \times m \times n$ times, randomly shuffle each pixel of ψ , δ , and η , and the save results in ψ_p , δ_p , and η_p , respectively, through the random sequences obtained from Chirikov map.
7. Iterate Intertwining map $3 \times m \times n$ times, multiply the obtained value with 10^{14} , and save the results in a row matrix A . Apply the modulus operator and save the results in B :
- $$B = A \bmod(256).$$
8. Reshape B into three separate matrices, i.e, B_1 , B_2 , and B_3 , and apply XOR operation:
- $$C_1 = \psi_p \oplus B_1.$$
- $$C_2 = \delta_p \oplus B_2.$$
- $$C_3 = \eta_p \oplus B_3.$$
9. Slightly change the initial conditions by adding a value $\sigma = 0.001$:
- $$\alpha_0 = (\alpha_0 + \sigma) \bmod(2\pi).$$
- $$\theta_0 = (\theta_0 + \sigma) \bmod(2\pi).$$
- $$x_0 = (x_0 + \sigma) \bmod(1).$$
- $$y_0 = (y_0 + \sigma) \bmod(1).$$
- $$z_0 = (x_0 + y_0 + \sigma) \bmod(1).$$
10. Repeat Steps 6–9 ϵ times, and select $\epsilon = 4$ for a good confusion and diffusion.
11. Combine each channel, C_1 , C_2 , and C_3 , and save the encrypted scalogram results in C .

4.6. Encryption and Security Analysis

The proposed scheme was tested on pick up object scalogram. The original and encrypted scalogram of pick up object are shown in Figure 10a,b, respectively. Additionally, encrypted walking scalogram is shown in Figure 11b. In Figures 10b and 11b, it is clear that contents of scalogram are encrypted and an eavesdropper cannot predict the original activity. Visually, it is clear that contents are hidden; however, the security of an encryption scheme should be highlighted thorough a number of parameters, as outlined in our previous work [32,33]. Several parameters in Table 1 indicate the robustness and higher security of the proposed scheme. How such security parameters reflect robustness the proposed scheme can be found in [32,34–36].

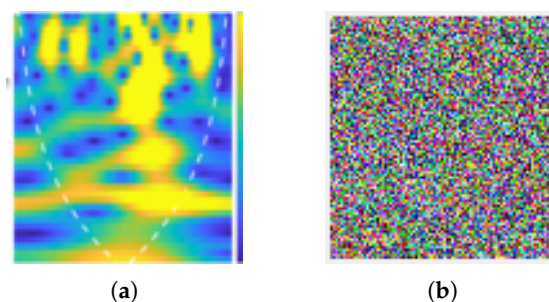


Figure 10. (a) Pick up original scalogram; and (b) encrypted scalogram.

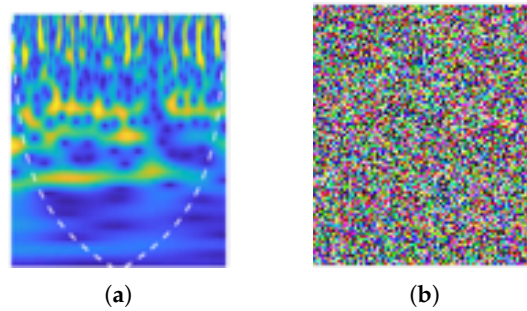


Figure 11. (a) Walking original scalogram; and (b) encrypted Scalogram.

Table 1. Evaluation of the scheme through a number of security parameters.

| Security Parameter | Original Pick up Scalogram | Encrypted Scalogram | Original Walking Scalogram | Encrypted Scalogram |
|------------------------|----------------------------|---------------------|----------------------------|---------------------|
| <i>Corr Coff (H)</i> | 0.9060 | 0.1599 | 0.8753 | 0.0644 |
| <i>Corr Coff (V)</i> | 0.9425 | 0.1245 | 0.9448 | 0.0341 |
| <i>Corr Coff (D)</i> | 0.8721 | 0.0900 | 0.8140 | 0.0068 |
| <i>Entropy</i> | 7.1273 | 7.7068 | 6.7482 | 7.9422 |
| <i>Key Sensitivity</i> | NA | 99.4311% | NA | 99.6735% |
| <i>NPCR</i> | NA | 99.4362 % | NA | 99.6575% |
| <i>UACI</i> | NA | 33.2151 | NA | 33.4512 |
| <i>Contrast</i> | 1.6186 | 10.0731 | 1.6889 | 10.5830 |
| <i>Homogeneity</i> | 0.8059 | 0.4228 | 0.7866 | 0.3944 |
| <i>Energy</i> | 0.1067 | 0.0197 | 0.1405 | 0.0162 |

5. Classification Results

We implemented the autoencoder model in a MATLAB tool, where training, validation, and testing were 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 optimizing 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 problem are shown in Table 2. The three-layer unsupervised autoencoder had layer depths of 200, 100, and 50, respectively. The optimum classification performance in terms of percentage accuracy is 91.1%, as highlighted in Table 2.

Table 2. Optimized parameters for autoencoder (scalograms/Wi-Fi Sensing).

| # | Width | Depth | Accuracy |
|----------|---------------------|----------|-------------|
| 1 | 20 | 1 | 77.3 |
| 2 | 50 | 1 | 78.1 |
| 3 | 100 | 2 | 76.7 |
| 4 | 50–100 | 2 | 80.0 |
| 5 | 150–200 | 3 | 88.0 |
| 6 | 50-100-200 | 3 | 91.1 |
| 7 | 10–25–50–100 | 4 | 81.3 |
| 8 | 15–30–60–200 | 4 | 80.7 |
| 9 | 30–60–120–240 | 5 | 81.5 |
| 10 | 40–80–240–300 | 5 | 79.9 |
| 11 | 15–30–45–90–200–400 | 6 | 80.9 |
| 12 | 50–100–200–400–800 | 6 | 85.5 |

6. Conclusion

This paper presents the application of next-generation body centric communication towards occupancy monitoring that can provide an effective and privacy preserved solution for reducing the energy consumption and carbon footprint. In the proposed model, non-wearable wireless devices such as Wi-Fi router, network interface card, and omnidirectional antennas operating at 2.4 GHz, are used to acquire data. Continuous wavelet transform is applied to the acquired RF signals to obtain Wi-Fi images that are processed using a deep learning algorithm to detect occupancy and to further perform occupancy classification. An unsupervised auto-encoder algorithm is used to classify images corresponding to different human activities of the occupants present in the area of interest. The performance of the proposed system was evaluated in terms of percentage accuracy, providing an overall accuracy of more than 91%. Lightweight image encryption techniques using multi-chaotic maps are proposed to encrypt the scalogram images. This feature enables secure storage of scalogram images for future usage such as improving training and testing accuracy of deep neural model.

Author Contributions: Data curation, J.A.; Formal analysis, S.A.S. and S.Y.S.; Investigation, A.T., F.A., G.R. and W.J.B.; Methodology, Q.H.A. All authors have read and agreed to the published version of the manuscript.

Funding: This is a joint work of, and is funded by School of Computing and Mathematics, Manchester 297 Metropolitan University with Edinburgh Napier University, University of Engineering and Technology, 298 Lahore and JamesWatt School of Engineering, University of Glasgow UK.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Allouhi, A.; El Fouih, Y.; Kousksou, T.; Jamil, A.; Zeraoui, Y.; Mourad, Y. Energy consumption and efficiency in buildings: Current status and future trends. *J. Clean. Prod.* **2015**, *109*, 118–130. [[CrossRef](#)]
2. Yang, J.; Santamouris, M.; Lee, S.E. Review of occupancy sensing systems and occupancy modeling methodologies for the application in institutional buildings. *Energy Build.* **2016**, *121*, 344–349. [[CrossRef](#)]
3. Cao, N.; Ting, J.; Sen, S.; Raychowdhury, A. Smart sensing for HVAC control: Collaborative intelligence in optical and IR cameras. *IEEE Trans. Ind. Electron.* **2018**, *65*, 9785–9794. [[CrossRef](#)]
4. Zou, H.; Jiang, H.; Luo, Y.; Zhu, J.; Lu, X.; Xie, L. Bluedetect: An ibeacon-enabled scheme for accurate and energy-efficient indoor-outdoor detection and seamless location-based service. *Sensors* **2016**, *16*, 268. [[CrossRef](#)]
5. Weekly, K.; Zou, H.; Xie, L.; Jia, Q.S.; Bayen, A.M. Indoor occupant positioning system using active RFID deployment and particle filters. In Proceedings of the 2014 IEEE International Conference on Distributed Computing in Sensor Systems, Marina Del Rey, CA, USA, 26–28 May 2014; pp. 35–42.
6. Huang, B.; Qi, G.; Yang, X.; Zhao, L.; Zou, H. Exploiting cyclic features of walking for pedestrian dead reckoning with unconstrained smartphones. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Heidelberg, Germany, 12–16 September 2016; pp. 374–385.
7. Yang, X.; Fan, D.; Ren, A.; Zhao, N.; Shah, S.A.; Alomainy, A.; Ur-Rehman, M.; Abbasi, Q.H. Diagnosis of the Hypopnea syndrome in the early stage. *Neural Comput. Appl.* **2019**, *32*, 1–12. [[CrossRef](#)]
8. Dong, B.; Ren, A.; Shah, S.A.; Hu, F.; Zhao, N.; Yang, X.; Haider, D.; Zhang, Z.; Zhao, W.; Abbasi, Q.H. Monitoring of atopic dermatitis using leaky coaxial cable. *Healthc. Technol. Lett.* **2017**, *4*, 244–248. [[CrossRef](#)]
9. Yang, X.; Shah, S.A.; Ren, A.; Zhao, N.; Zhao, J.; Hu, F.; Zhang, Z.; Zhao, W.; Rehman, M.U.; Alomainy, A. Monitoring of patients suffering from REM sleep behavior disorder. *IEEE J. Electromagn. RF Microw. Med. Biol.* **2018**, *2*, 138–143. [[CrossRef](#)]
10. Qiu, Z.; Zou, H.; Jiang, H.; Xie, L.; Hong, Y. Consensus-based parallel extreme learning machine for indoor localization. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–6.
11. Zou, H.; Chen, Z.; Jiang, H.; Xie, L.; Spanos, C. Accurate indoor localization and tracking using mobile phone inertial sensors, Wi-Fi and iBeacon. In Proceedings of the 2017 IEEE International Symposium on Inertial Sensors and Systems (INERTIAL), Kauai, HI, USA, 27–30 March 2017; pp. 1–4.

12. Shah, S.A.; Fioranelli, F. RF Sensing Technologies for Assisted Daily Living in Healthcare: A Comprehensive Review. *IEEE Aerosp. Electron. Sys. Mag.* **2019**, *34*, 26–44. [[CrossRef](#)]
13. Haider, D.; Ren, A.; Fan, D.; Zhao, N.; Yang, X.; Shah, S.A.; Hu, F.; Abbasi, Q.H. An efficient monitoring of eclamptic seizures in wireless sensors networks. *Comput. Electr. Eng.* **2019**, *75*, 16–30. [[CrossRef](#)]
14. Tanoli, S.A.K.; Rehman, M.; Khan, M.B.; Jadoon, I.; Ali Khan, F.; Nawaz, F.; Shah, S.A.; Yang, X.; Nasir, A.A. An experimental channel capacity analysis of cooperative networks using Universal Software Radio Peripheral (USRP). *Sustainability* **2018**, *10*, 1983. [[CrossRef](#)]
15. Fioranelli, F.; Le Kernec, J.; Shah, S.A. Radar for Health Care: Recognizing Human Activities and Monitoring Vital Signs. *IEEE Potential* **2019**, *38*, 16–23. [[CrossRef](#)]
16. Weekly, K.; Jin, M.; Zou, H.; Hsu, C.; Soyza, C.; Bayen, A.; Spanos, C. Building-in-Briefcase: A rapidly-deployable environmental sensor suite for the smart building. *Sensors* **2018**, *18*, 1381. [[CrossRef](#)]
17. Duarte, C.; Van Den Wymelenberg, K.; Rieger, C. Revealing occupancy patterns in an office building through the use of occupancy sensor data. *Energy Build.* **2013**, *67*, 587–595. [[CrossRef](#)]
18. Erickson, V.L.; Carreira-Perpiñán, M.Á.; Cerpa, A.E. OBSERVE: Occupancy-based system for efficient reduction of HVAC energy. In Proceedings of the 10th ACM/IEEE International Conference on Information Processing in Sensor Networks, Chicago, IL, USA, 12–14 April 2011; pp. 258–269.
19. Yang, X.; Shah, S.A.; Ren, A.; Zhao, N.; Fan, D.; Hu, F.; Ur Rehman, M.; von Deneen, K.M.; Tian, J. Wandering Pattern Sensing at S-Band. *IEEE J. Biomed. Health Inf.* **2018**, *22*, 1863–1870. [[CrossRef](#)]
20. Kumar, R.; Mukesh, R. State of the art: Security in wireless body area networks. *Inter. J. Comput. Sci. Eng. Technol. (IJCSET)* **2013**, *4*, 622–630.
21. Al-Janabi, S.; Al-Shourbaji, I.; Shojafar, M.; Shamshirband, S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egypt. Inform. J.* **2017**, *18*, 113–122. [[CrossRef](#)]
22. Mert, A.C.; Öztürk, E.; Savaş, E. Design and Implementation of Encryption/Decryption Architectures for BFV Homomorphic Encryption Scheme. *IEEE Transact. VLSI Syst.* **2020**, *28*, 353–362. [[CrossRef](#)]
23. Zou, H.; Jiang, H.; Yang, J.; Xie, L.; Spanos, C. Non-intrusive occupancy sensing in commercial buildings. *Energy Build.* **2017**, *154*, 633–643. [[CrossRef](#)]
24. Shah, S.A.; Yang, X.; Abbasi, Q.H. Cognitive health care system and its application in pill-rolling assessment. *Int. J. Numer. Model. Electron. Net. Device. Field.* **2019**, *32*, e2632. [[CrossRef](#)]
25. Haider, D.; Shah, S.A.; Shah, S.I.; Iftikhar, U. Mimo network and the alamouti, stbc (space time block coding). *Am. J. Electric. Electron. Eng.* **2017**, *5*, 23–27.
26. Shah, S.I.; Shah, S.Y.; Shah, S.A. Intrusion Detection through Leaky Wave Cable in Conjunction with Channel State Information. In Proceedings of the IEEE 2019 UK/China Emerging Technologies (UCET), Glasgow, UK, 21–22 August 2019; pp. 1–4.
27. Ayyaz, S.; Qamar, U.; Nawaz, R. HCF-CRS: A Hybrid Content based Fuzzy Conformal Recommender System for providing recommendations with confidence. *PLoS ONE* **2018**, *13*, 0204849. [[CrossRef](#)]
28. Anwaar, F.; Iltaf, N.; Afzal, H.; Nawaz, R. HRS-CE: A hybrid framework to integrate content embeddings in recommender systems for cold start items. *J. Comput. Sci.* **2018**, *29*, 9–18. [[CrossRef](#)]
29. Yunus, R.; Arif, O.; Afzal, H.; Amjad, M.F.; Abbas, H.; Bokhari, H.N.; Haider, S.T.; Zafar, N.; Nawaz, R. A framework to estimate the nutritional value of food in real time using deep learning techniques. *IEEE Access* **2018**, *7*, 2643–2652. [[CrossRef](#)]
30. Qadir, H.; Khalid, O.; Khan, M.U.; Khan, A.U.R.; Nawaz, R. An optimal ride sharing recommendation framework for carpooling services. *IEEE Access* **2018**, *6*, 62296–62313. [[CrossRef](#)]
31. Bahi, J.M.; Couchot, J.F.; Guyeux, C. Quality analysis of a chaotic proven keyed hash function. *Int. J. Adv. Internet Technol.* **2016**, *5*, 26–33.
32. Ahmad, J.; Hwang, S.O. A secure image encryption scheme based on chaotic maps and affine transformation. *Multimed. Tool. Appl.* **2016**, *75*, 13951–13976. [[CrossRef](#)]
33. Masood, J.A.F.; Shah, S.A.; Jamal, S.S.; Hussain, I. A Novel Secure Occupancy Monitoring Scheme Based on Multi-Chaos Mapping. *Symmetry* **2020**, *12*, 350.
34. Ahmad, J.; Hwang, S.O. Chaos-based diffusion for highly autocorrelated data in encryption algorithms. *Nonlinear Dyn.* **2015**, *82*, 1839–1850. [[CrossRef](#)]
35. Ahmad, J.; Khan, M.A.; Hwang, S.O.; Khan, J.S. A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices. *Neural Comput. Appl.* **2017**, *28*, 953–967. [[CrossRef](#)]

36. Masood, F.; Ahmad, J.; Shah, S.A.; Jamal, S.S.; Hussain, I. A Novel Hybrid Secure Image Encryption Based on Julia Set of Fractals and 3D Lorenz Chaotic Map. *Entropy* **2020**, *22*, 274. [[CrossRef](#)]



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).