Compressed Sensing System for a Fingerprint Image Recognition Using Sensing Matrix with Chaotic Model-Based Deterministic Row Indexes

Workneh Wolde Hailemariam (worknehwolde11@gmail.com)
Sharda University https://orcid.org/0000-0001-5051-2547
Pallavi Gupta
Sharda University

Research Article

Keywords: Compressed Sensing, Fingerprint Image, Sparse Representation, Convex Optimization, Encryption, Chaotic Model

Posted Date: July 12th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-279847/v2

Compressed Sensing System for a Fingerprint Image Recognition Using Sensing Matrix with Chaotic Model-Based Deterministic Row Indexes

Workneh Wolde[*]. Pallavi Gupta

[*]worknehwolde11@gmail.com

[*]Sharda University, Greater Noida, UP, India

Abstract – This paper proposes a novel design approach for a secured compressed sensing system for fingerprint sensing and transmission. In the proposed design, the first stage is acquiring the signal followed by sparsely modeling it using Orthogonal Matching Pursuit (OMP) algorithm then compressing. In addition to compressing, we multiply the sparse modeled data by a novel, deterministic, and partially orthogonal Discrete Cosine Transform (DCT) sensing matrix to guarantee its security. Furthermore, the construction of the sensing matrix uses a modified Multiplicative Linear Congruential Generator (MLCG) to select the row index appropriately from chaotically re-arranged rows of DCT pseudo-randomly. On the other hand, the compressed image's simultaneous recovery and decryption accomplished using a convex optimization method—the proposed system tested by employing different image and security assessment techniques. The results show that we have archived a better Peak Signal to Noise Ratio (PSNR) than the recommended value for wireless transmission using samples below 25%.

Keywords - Compressed Sensing, Fingerprint Image, Sparse Representation, Convex Optimization, Encryption, Chaotic Model

1. **Introduction**

Potentially dangerous security treat forces various facilities and IoT-based communications to uses a secured authentication. And sensors array-based fingerprint scanning is one of them. Till now, several design strategies include capacitive [1][2][3][4], ultrasonic [5], and optical [6] MEMS-based systems, have been employed with a whole sampling method which includes read and record all sensors outputs. However, in terms of the optimal design, complete sampling is not an efficient approach.

Designing an extensive sensor system with a reduced sampling method can leverage those shortcomings of the previous design. The strategies employed in this design are known as compressed sensing, which works mainly based on the concept developed by Candes *et al.* [7] and Donoho [8]. This formulation allows us to take samples indirectly from few acquired data rather than the whole elements.

To implement compressive sensing, the signal must be sparse originally or in its transformed version. The sparsity of the signal in its transformed versions is two types. One of them is, over some dictionary formed analytically by DCT and wavelet transformation of itself [9][10][11], and the other is over some learned dictionary designed by prior knowledge of several correlated signals [12][13][14][15][16]. Compressed sensing based on the latter design approach is less loss, and we found it suitable for fingerprint image sampling and compression.

The scope of compressed sensing is not limited to analytical computations. It also has hardware implementation. FPGA (Field Programmable Gate Array) device has been intensively used and shows higher performance in ECG, EEG [17][18][19], and other one-dimensional signal processing [20]. It also demonstrates the transformation of a high dimensional signal to a lower one employing matrix multiplication in parallel with measurements from input [21].

Transmission of an image that has a biometric feature should be secured and reliable. Therefore, a cryptosystem is securely stored for authentication and identification. Some of the developed cryptosystems are phase-encoded schemes using joint transform[22], exclusive-OR encryption [23], and fractional Fourier transformation methods are to mention a few[24]. Not only that, how to encrypt fingerprint images using orthogonal coding also studied in[25]. Double stage chaotic biometric image-like fingerprint encryption scheme by using two maps named Arnold (permutation) and Henon (substitution) for pixel shuffling have been studied in[26].

This paper will introduce our contribution to a novel design strategy of sensing matrix for optimized, secured sensing and fingerprint images or signal transmission. This means that all sensor data will be acquired but not got directly saved or transmitted. To achieve this objective, we developed and implemented an algorithm to construct a novel sensing matrix and test its validity by employing an image and security assessment technique suitable for fingerprint image detection. The overall implementation was done with the help of MATLAB script, which runs on a personal computer.

We organized our work into six main sections, including the introduction, which was already discussed before. The

following section will discuss the theoretical background of compressed sensing, including a general introduction to data compression and recovery. Next to section two, the detailed methodology of designing the whole compressing sensing and its parts like dictionary and sensing matrix with their algorithm employed to build them has been discussed. The analysis and reliability of the proposed system tested using the encryption key method and by analyzing security threats in sections four, five, and six. Finally, we summarized our study in section seven of this paper by pointing out our main contribution.

2. **Background Studies**

The main idea of compressive sensing is to recover signals from fewer measurements that are less than the Nyquist rate [7] [8]. In addition to the sparse input signal, for the successful design of a compressed sensing system, the system must be stable against spatial transformation caused by the change of input orientations during contact between fingertip and sensor array. Hence, we select and incorporate the necessary background theories in this section.

2.1 **Concept of Compressed Sensing**

In a compressed sensing system, sparse signal $x \in \Re^{N\times 1}$ (column vector), measured signal $y \in \Re^{M\times 1}$, and a sensing matrix $\Phi \in \Re^{M\times N}$ provided that $M << N$, related by the following equation, eq.1

$$y = \Phi x \tag{1}$$

For a given integers k and n with $k < n$ the sets of k-sparse, S_k vectors in $\Re^N$ define as

$$S_k := \left\{ x \in \Re^N : \left| \sup\, p(x) \le k \right| \right\} \tag{2}$$

Any linear equation system similar to eq.1 is under-completed and will lead us to find non-unique solutions. To get a unique solution, one has to set a constraint and apply it to the following optimization problem defined by L_p

$$L_p : \qquad \min \|x\|_p \qquad s.t. \qquad \hat{y} = \Phi \hat{x} \tag{3}$$

$$\|x\|_p = \sum_{i=1}^{N} x_i^p \tag{4}$$

To get a sparse vector $\hat{x}$ from $\hat{y}$ solving $p=0$ and $p=1$ is a good optimization choice. In this project, we have applied the well-known greedy type method known as Orthogonal Matching Pursuit (OMP) [27], which is $p=0$ based optimization method.

However, under some exceptional cases, x may not be sparse in its native form. In those cases, we need to find the sparse representation $\alpha \in \Re^{N'\times 1}$ ($N' > N$ in most cases) x to satisfy the condition for compressed sensing formulation, and this makes eq. 1 to take the form of eq.5,

$$y = \Phi x = \Phi \Psi \alpha \tag{5}$$

Where $\Psi \in \Re^{N'\times N}$ are sparse basis or dictionary and $\alpha \in \Re^{N'\times 1}$ sparse representation of x. This is what we call the signal model of input which is obtained by using pursuit algorithms.

2.2 **Sensing Matrix**

The sensing matrix that we denote as Φ in this paper is a matrix used to govern the selection of sparsely modeled signals using a predetermined order of sampling process. Random or deterministic matric [28] can be used as a sensing matrix $\Phi \in \Re^{M\times N}$ to solve $p=1$ by employing the interior point method. Any hardware available for signal processing can generate this sensing matrix, for example, FPGA units configured as an LFSR (Linear Feedback Shift Register) as already done in [29] for ECG signal. A random or deterministic matrix is among the matrices that satisfy the Gaussian distribution. The deterministic matrix used in this work is generated from the DCT matrix whose indexes are arranged based on a Logistics map-based chaotic model[30]. A chaotic system is a dynamic system that fluctuates forever without even repeating itself or shows any tendency towards fixed value [31].

2.3 **Sparse Recovery Algorithms**

The spares solution of the input data can be obtained using the Orthogonal Matching Pursuit (OMP) algorithm at a low computational cost. OMP algorithm is a greedy type algorithm that helps to solve LP0 optimization problem given by

$$\min \|x\|_0 \qquad \text{s.t.} \qquad Aa = b \tag{5}$$

Where $A \in \Re^{N\times M}$, $b \in \Re^N$ and $a \in \Re^M$. Since the problem is LP0 type one, we start from b and then look for a column of A that is most correlated with b, giving the minimum dot product value as a reference for comparison. Per [32], this algorithm is non-invariant under an ill-conditioned dictionary.

2.4 **Dictionary Learning**

Dictionary is a rectangular matrix used to study and obtain the input signal's sparse representation before undergoing compression. One of the widely used methods to build it is the K-SVD. This method solves optimization problem eq. (5) iteratively. Set of signals Z known as training signal with initial dictionary given as D and the coefficients sets X can be obtained by solving the problem with and suitable matching pursuit algorithm given in eq. (4 & 5) [33]

$$\min \|Z - DX\|_1^2 \qquad \text{s.t.} \qquad \|X_i\|_0 < K \tag{6}$$

Where X_i is of the coefficients and K is sparsity level. All of the dictionary atoms are generated by updating SVD (Singular Value Decomposition) methods.

The training signals are selected based on their structural similarity index (SSIM) [34], the most fundamental image quality assessment method. This would be done by setting the threshold value and rejecting the signal whose structural similarity index value is far below the adjusted threshold.

The structural similarity index (SSIM) of an image concerning its reference image (a and b) of sizes (N, N) is

$$SSIM(a,b) = \frac{(2m_a m_b + B_1)(2\upsilon_{ab} + B_2)}{(m_a^2 + m_b^2 + B_1)(\upsilon_a^2 + \upsilon_b^2 + B_2)} \quad (7)$$

Where m_a and m_b are averages, υ_a^2 and υ_b^2 are variances, υ_{ab} the covariance of *a* and *b* respectively. And the remaining terms B_1 and B_2 are two variables to stabilize the division with a leak denominator. In this paper, we select an image patch that comprises all fingerprint features as a reference to choose the other training patches.

2.5 **Prime-Dual Interior-Point Method**

Once we find that the signal is sparse, we can randomly sample it and transmit it to the receiver to recover it back to its original form. But, this requires solving the LP-0 type optimization problem, which is a non-deterministic polynomial hard or NP-Hard problem.

To leverage this hardness, transforming the problem to the

LP-1 type is the best option. Transformation of the problem leads eq.5 to take the form of eq. 8.

In addition to the sparsity of *x*, the sensing matrix $\boldsymbol{A}$ must satisfy the Restricted Isometric Property (RIP) with a restricted isometric constant δ_s, which is given by eq.9 [36] to get a solution for eq.8, which is also valid for (1).

$$\min \|x\|_1 \qquad \text{s.t} \qquad Ax = b \quad (8)$$

$$(1-\delta_S)\|x\|_2^2 \le \|Ax\|_2^2 \le (1+\delta_S)\|x\|_2^2 \quad (9)$$

According to the prime dual method, the solution can be achieved by narrowing the dual gap between the feasible solution of the prime and dual problem. It starts from an arbitrary chosen initial point and searches for the optimal solution by applying the classical Newton method [35]. Implementation of this approach computationally possible because there is a free software package available to solve the problem iteratively.

3. **Proposed Method**

The proposed method focused on modeling the input signal and a novel design approach for a proper deterministic sensing matrix to compress and transmit it.

3.1 **The Design Work Flow**

The whole design procedure has been summarized in fig.1 and 2, which are given bellow

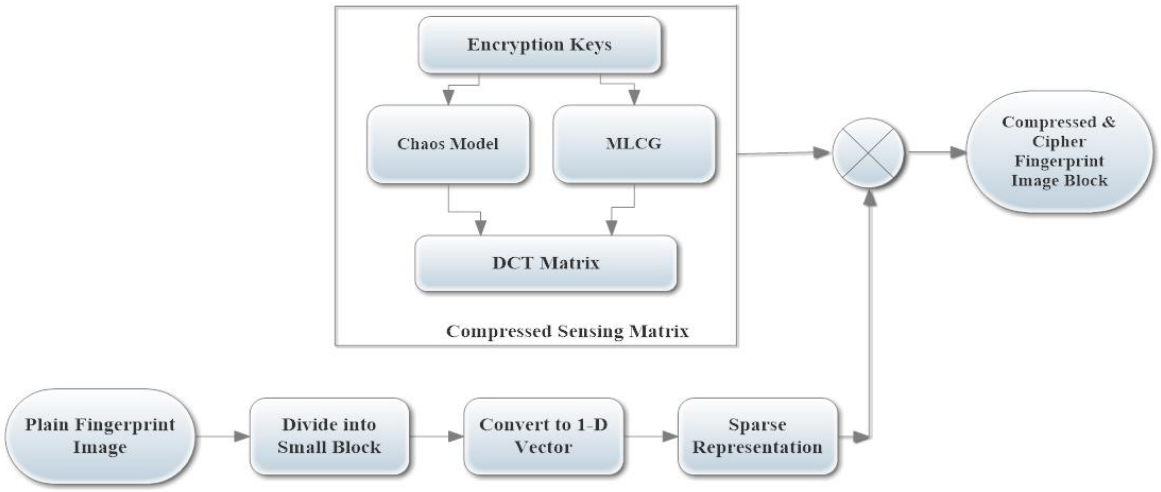


Fig.1 The proposed compressed sensing system

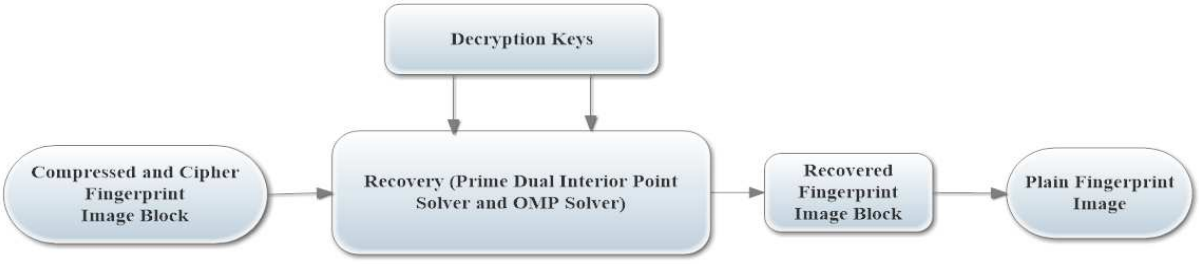


Fig.2 Recovery System

3.2 **Proposed Sensing Matrix Design for Compressed System**

To better design a compressive sensing scheme, it is vital to have an efficient sensing matrix. For sensors array which contains M by N elements, the locations at which measurements have to be taken are stored in the sensing matrix derived from a Discrete Cosine Transform Matrix (DCT) defined by eq.10 by a random selection of rows. This means

that the proposed matrix submatrix N by N size DCT matrix (eq.11).

$$\Psi_k = \sum_{n=1}^{N} \psi_n Cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right] \qquad k = 1,2,3...N \quad (10)$$

$$\Psi = \begin{pmatrix} \Psi_{1,1} & \Psi_{1,2} & . & . & . & \Psi_{1,N} \\ \Psi_{2,1} & \Psi_{2,2} & . & . & . & \Psi_{2,N} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ \Psi_{N,1} & \Psi_{N,2} & . & . & . & \Psi_{N,N} \end{pmatrix} \quad (11)$$

Equation 11 helps us generate the matrix whose row width is not less than *M*log(N)* [7] by arranging selected rows according to the recommended sequence by our algorithm. Before sub-matrix derivation, there is a step that we have incorporated to makes this design approach novel, known as masking the DCT by converting to its equivalent form of itself by swapping every row of the matrix in chaotic sequence.

The sequence generation is an entirely chaotic model based on a Logistics map. Logistics map is mathematically given by eq.12 with the population at the time, t, P_{t+1}, the ratio of the existing population to the maximum population P_t and growth rate r

$$z_{t+1} = rz_t(1 - z_t) \quad (10)$$

The value of r is any value between zero and four. At the same time, the importance of z_{t+1} and z_t is always between zero and one. As depicted in fig. 4, the logistic map is highly chaotic if the value r is 3.57 and more. The detailed step that we followed to re-arrange the matrix rows sequence is summarized in algorithm-I.

Algorithm-I Chaotic model-based row index re-arrangement of the DCT

Input: chaotic control parameters such as chaotic initial state z_0, growth rate $r \in (3.75,4]$, and the N by N DCT matrix

Output: Equivalent form of the DCT matrix or masked DCT matrix.

1) Using the recursive logistic map eq. (12) expression, generate a one-dimensional vector $[z[t]]$ of size N by 1.
2) Let $[N]$ be the index set $\{1,2,3...N\}$, and their corresponding values $[z[t]]$ are $\{z[1], z[2], z[3]...z[N]\}$
3) Performs an ascending order operation upon the $[z[t]]$ sequence, which yields another new vector $[\hat{z}[t]]$ with a new index set $[\hat{N}]$.
4) Iterate through the set $[\hat{z}[t]]$ to obtain their corresponding index subset $[N]$ and denote it by $[\mathcal{N}]$.
5) Perform a direct mapping from set $[N]$ to $[\mathcal{N}]$ ($[N] \leftrightarrow [\mathcal{N}]$) and elementary rows switching of DCT accordingly.
6) Finally, express the orthogonal equivalent matrix of DCT, by $\hat{\Psi}$.

The diagrammatical representation of the above algorithm has given in fig.3 for r = 3.7, t=121, and initial state value 0.45

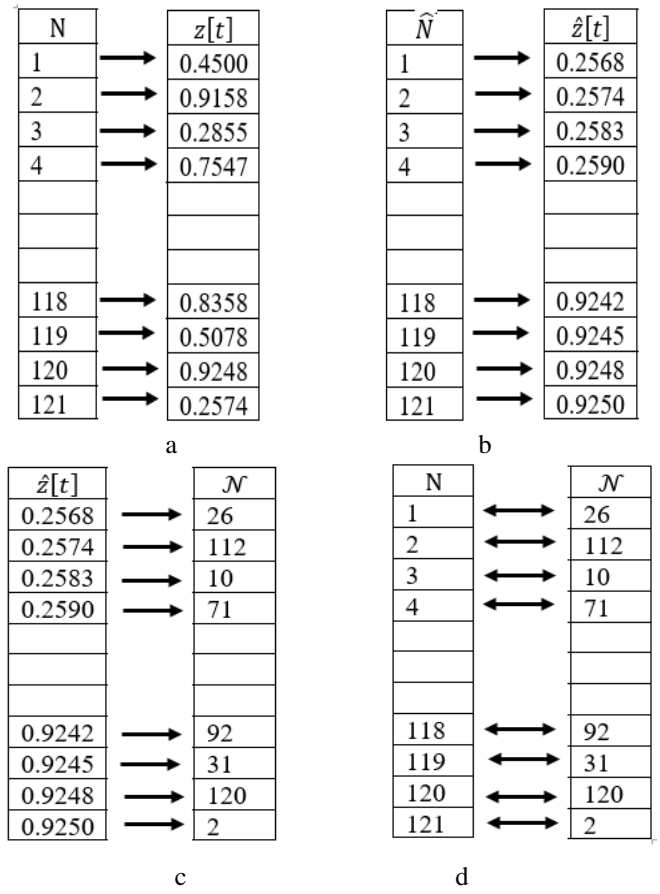


Fig. 3 DCT matrix chaotic masking process according to slgorithm-1: (a) step-1&2 (b) step-3 (c) step-4 and (d) step-5

Once this matrix is obtained, the parameters used in this design, such as *N r, t,* and the initial value, z_0 would be taken as part of the encryption keys for the sensing system. The sensing matrix obeys the RIP if the smallest set $q(M,N)$ formed by deterministic row selection with high probability equals to $O(M * \log(N))$. A Multiplicative Linear Congruential Generator (MLCG) [37] output sequence-based row selection method with slight modification can be employed to extract the sensing matrix from masked DCT.

The modified MLCG sequence generator has been designed with shifting properties and mathematically expressed as in eq. 14.

$$k_{i+1} = S + (ak_i + b) \bmod 2^t$$
$$0 \le a, b \le 2^{t-1}, (M - N - 1) \le S \le N \quad (14)$$

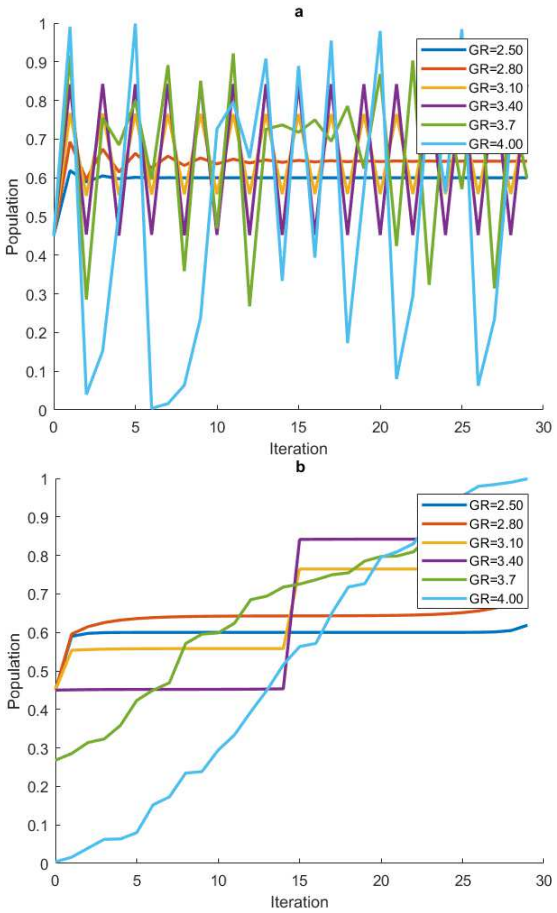


Fig. 4 Time series graph of the logistic map: (a) Standard Plot (b) Plot based on ascending order of the population

Where *a* is the multiplier, *b* is the increment, *t* is the number of bits, and *S* is an integer used to extend the row index selection. Hence by appropriately the values of *S,* we can generate several sensing matrices $\hat{\Psi}$ without repetition to make the proposed system resistive against security attacks.

Algorithm-II Deterministic sensing matrix generation

Input: control parameters such as *S* or the shifting, multiplier constant *a, b,* numbers of bit *t,* and equivalent form of the DCT matrix.

Output: a partial orthogonal deterministic sensing matrix Φ of M by 1 size.

1) Using the modified MLCG eq. (14) expression generates a sequence of integers M_{ψ} of size M by 1.
2) Select rows from $\hat{\Psi}$ whose indices belongs to M_{ψ}
3) Define them as Φ or the deterministic sensing matrix (eq. 5).
4) Repeat steps 1 through 3 to generate others sensing matrices by using different parameters for MLCG.

By applying different combinations of *S*, *a, b,* and *t* on the equivalent form of the DCT matrix we already have, we can generate many partially orthogonal sensing matrix row index sets. Now, we can consider *S*, *a, b,* and *t* as an additional encryption keys for the proposed system.

4. Analysis and Result for the Proposed Sensing Matrix

This section presents the comprehensive experimental study of the proposed system for two sensing matrices. The first one is a random matrix, and the other is the proposed sensing matrix. The practical test for the validity of the above mathematical formulation has been done using public data sources from the NIST database (https://www.nist.gov/itl/iad/image-group/nist-special-database-302).

Three assessment methods are employed to check the methodology's effectiveness that we have used to transform the input signals. These are Root Mean Square Error (RMSE), Peak Signal to Noise Ratio (PSNR), and Similarity Index of Image (SSIM). The mathematical expression for SSIM already given by eq.7 and for the PSNR of m by n image b with respect to a reference image a of a similar dimension is given by eq.15

$$PSNR(a,b) = 10 * \log \frac{PV^2}{MSE(a,b)} \qquad (15)$$

Where PV the Peake Value of the pixel in the image and $MSE(a,b)$ is Mean Square Error of an image b with respect to reference image a

$$MSE(a,b) = \frac{1}{m*n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(a(i,j) - b(i,j)\right)^2 \qquad (16)$$

4.1 Learning to Build the Dictionary Matrix

We first organized a data store to keep a set of images which used to train our dictionary. Then we have divided each image element to generate 8 by 8, 16 by 16, and 24 by 24 image patches. The similarity of each image patch is measured using their SSIM (Similarity Index) with one standard reference patch containing most of the fingerprints image features.

Then using the K-SVD algorithm, we trained three different dictionary matrices for signal transformation to sparse from its native form. The plot of these matrices is shown in the figure fig. 5.

4.2 Data Modeling for Compressed Sensing Input

Using the K-SVD algorithm, we construct the dictionary matrix to model the data, an equivalent representation of the input with length 64, 256, and 576 by another 81,400 and 1089 length vector with a few numbers of non-zero components, respectively. The best method to get the compressible model of this data is by employing the Orthogonal Matching Pursuit algorithm upon the measurement data.

As depicted in the result, our result will be better if we restrict the number of the sparse coefficient low. This result indicates that the methodology supports a high compressional ratio like 1:10, which is pretty good regarding the possibility of recovery as we already proved in the next section.

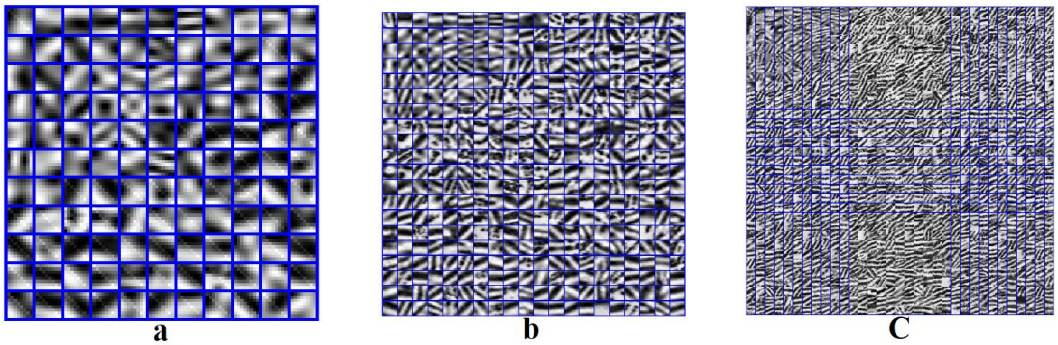
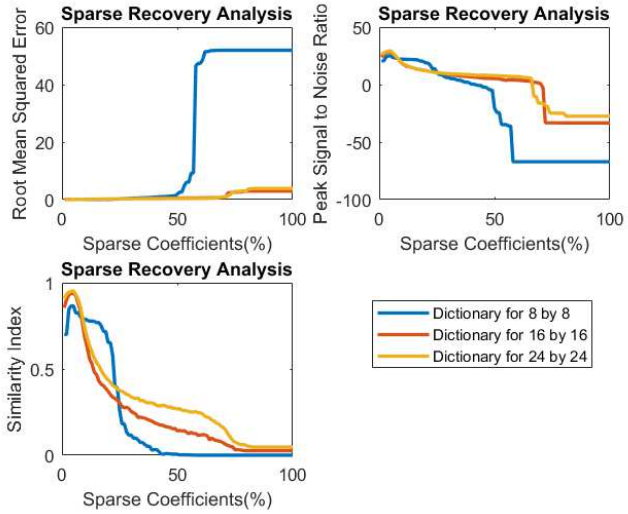


Fig. 5 The trained dictionary using (a) 8 by 8 image patches (b) 16 by 16 image patches (c) 24 by 24 image patches



(a)

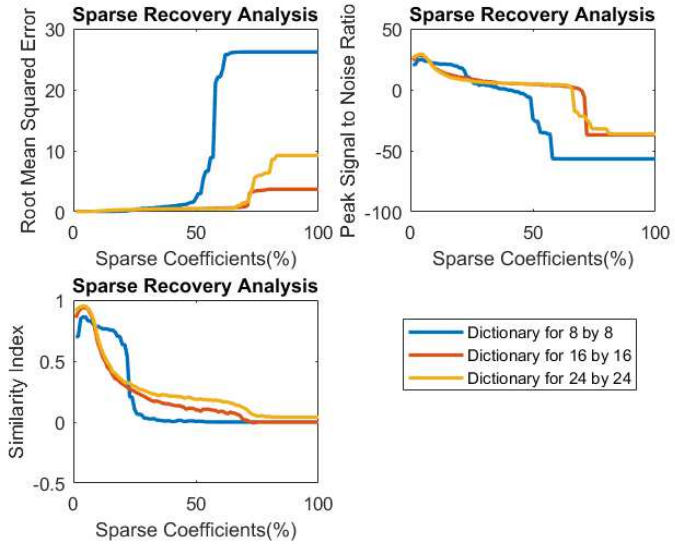


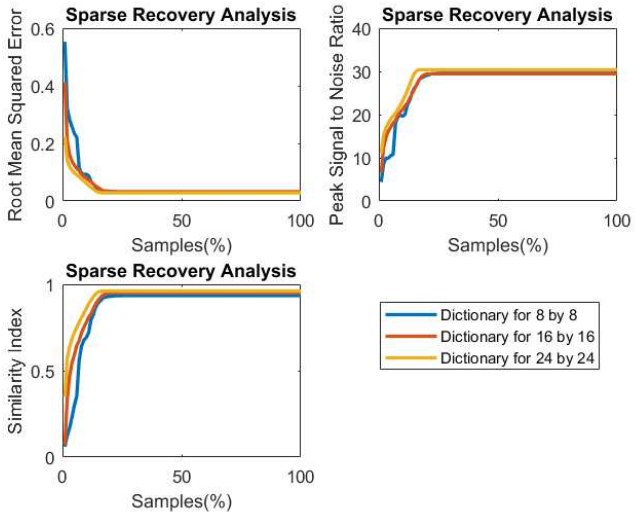
Fig. 6. Image assessment index Vs. number of sparse coefficient (a) For random sensing matrix (b) For proposed sensing matrix

4.2 **Compressing and Encryption**

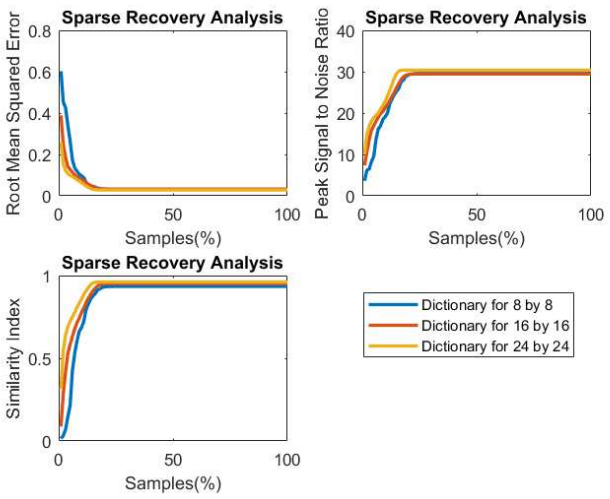
The compression of the sparse data is the easiest step in architecture. It is simply multiplying the sparse representation by sensing matrix. Both encryption and compression have been done simultaneously. As long as the sensing matrix is secreted from third-party users, the compressed data remain safe from being accessed by external agents. Furthermore, it can be constructed from the encryption key that could already be obtained in algorithm-I and II. Therefore, there is no need to send the whole sensing matrix; instead, securely transferring the encryption keys is enough.

4.3 **Decompression and Decryption**

This step or simultaneous decompression and decryption is the reverse process of the previous one and takes place at the receiver side. Once the sensing matrix keys are delivered to the receiver, the decompression is possible by solving the p-1 optimization, eq. 7, problem using the already described prim-dual interior-point method followed by sparse recovery.



(a)



(b)

Fig.7 Image assessment index Vs. number samples (a) for random sensing matrix (b) for proposed sensing matrix

Unlike the previous section, we fix the numbers of the sparse coefficient constant to study the rate of signal recovery with the number of samples taken from the sparse signal. The result shows that we still have a high recovery rate at a small number of samples. This result is better than the recommended compression rate for wireless transmission from 20 to 25dB [38][39]. This analysis concludes that the proposed sensing matrix performance is almost identical to the random matrix, which possesses the RIP feature [40].

5. **Security Threat Model**

For the safe flow of data from one state to another, in our case, from sender to receiver, the communication should be secured utilizing encrypting the data. This section will identify the expected potential threat that will impact and expose it for risk based on a literature survey.

The critical elements of the system responsible for the loss of data if potential adversaries access them are the dictionary, the sensing matrix, and the encryption key used to build the sensing matrix. The last element cannot be a problem if they securely transfer to a legitimate user. Still, the first two elements need further analysis because there are several alternative ways for the attacker to construct them. The dictionary matrix can be built using the same algorithm used in the proposed design from different training signals or fingerprint data. However, any output from it may not be sparse simultaneously, or a sparse solution is always unique for the fixed input signal, and coherent dictionary matrix once computed [41]. Hence, we will focus only on the sensing matrix.

When the attacker sends a randomly chosen plane text or image to the oracle and gets the cipher version of text or image, there will be a probability of gaining a piece of knowledge about how the system encrypts its data. This attack is known as Chosen Plain text Attack (CPA). Like other works [42][43], the proposed encryption in this paper is related but not directly to the sensing matrix. As already pointed out in [44][45], such a compressed system is not secured against CPA. We can eliminate this vulnerability by effectively extracting different sensing matrices using the modified LCG (eq. 14) from a single DCT matrix designed based on a chaotic model (eq. 11). And the rest will be discussed in the next section.

6. **Discussion on Performance Test and Reliability Study**

In this section, we will identify the sensitive part of the system that makes it vulnerable to attack and explain how the system will respond to them by analyzing how the model impacts the reliability of the design approach.

6.1 **Randomness Test Via Correlation Analysis**

Correlation analysis involves evaluating several randomly selected pairs of adjacent pixels aligned horizontally, vertically, and diagonally. For a particular figure print image with each pixel coordinates $(x.y)$ and randomly chosen numbers of pairs T, the correlation is given by eq. 17.

$$Corr(x,y)=\frac{T\sum_{i=1}^{T}\left(x_i y_i\right)-\sum_{i=1}^{T}x_i\sum_{i=1}^{T}y_i}{\sqrt{\left(T\sum_{i=1}^{T}x_i^2-\left(\sum_{i=1}^{T}x_i\right)^2\right)\left(T\sum_{i=1}^{T}y_i^2-\left(\sum_{i=1}^{T}y_i\right)^2\right)}} \quad (17)$$

We effectively utilized eq.17 for 3000-pixel pairs of plain and compressed cipher images and plot distribution as shown in

fig. 19. Comparing the figure in both plain and cipher images shows that the proposed sensing matrix possesses the expected randomness.

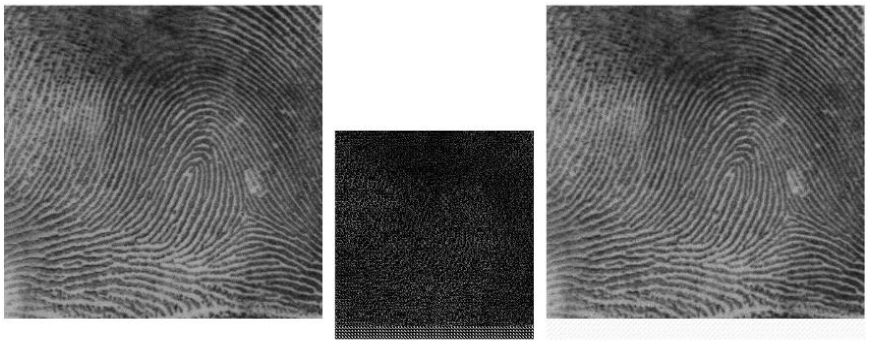
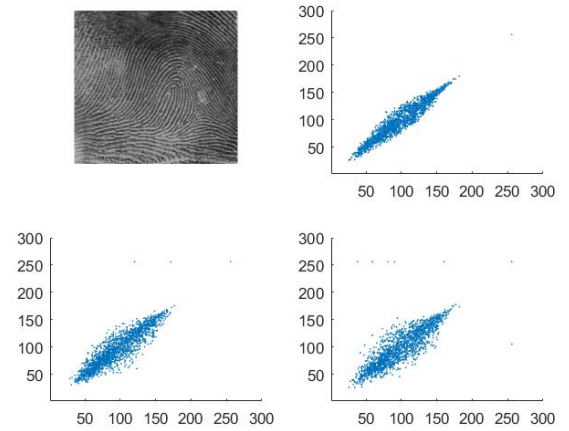
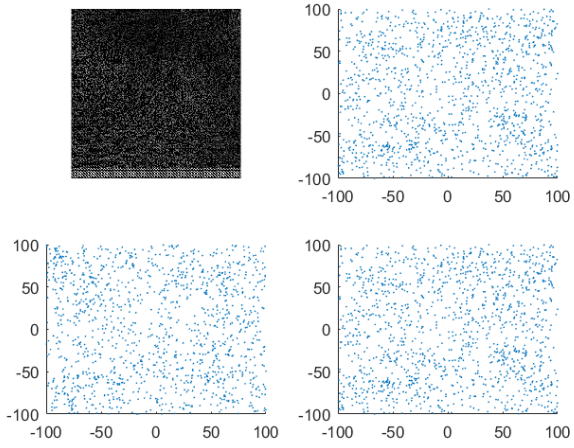


Fig. 8 From left to right, the original fingerprint image, the compressed also encrypted version, and the recovered image, respectively



(a)



(b)

Fig. 9 Correlation plots (a) for plain-image and (b) compressed image

6.2 **Histogram Analysis for Encrypted Image**

The histogram analysis is helpful to identify which data of the securely compressed image easily visible for the attacker. In the proposed scheme, there are several entries whose values are negative. As one advantage and the nearly uniform distribution of values depicted on the histogram comparison figure, fig.10 further indicates that the system is still safe from histogram-based attacks.

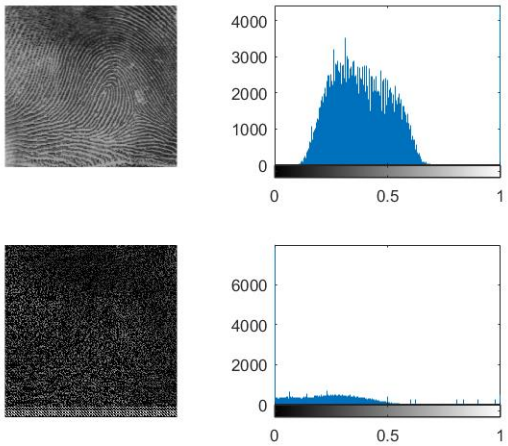


Fig. 10 Histogram plot for (a) plain-image and (b) compressed figure

6.3 **Key Sensitivity Test**

A key sensitivity test is used to examine how the proposed sensing matrix responds to a slight change in the magnitude of some of the keys used to construct the proposed sensing matrix. Keeping other keys that affect others except for the logistic map, we have observed how the sensing matrix row sequence generated if the growth rate of the Logistic map changed by $2.6333X10^{-6}$ % with the help of our proposed algorithm-I. The growth rate, which is equal to 3.7504, selects the rows of the DCT matrix according to the sequences of 8, 29, 2, 15, 19, 12….. And the other 3.7505 increase by only $2.6333X10^{-6}$ % produces the sequences of 8, 28, 3, 17, 19, 13….. Therefore, the partially orthogonal sensing matrix with those selected rows from DCT makes different cipher data. The same precision has been used in all computations of

sequence and initial values. This behavior of the sensing matrix shows that the proposed scheme is a key-sensitive scheme.

6.4 **Key Space**

When a brute force attack occurs, the adversary constructs the sensing matrix by combining rows using its technique with large trials. According to [46][44][47], the attacker must attempt a maximum of 2^{100} rows combinations of the DCT matrix, which is supposed to exceed the keyspace of the system. In this regard, the keyspace of our proposed method can be computed for row dimension 121, and 25 of them are enough to construct the sensing matrix.

$$Key.Space = (121)!*\left(\frac{121!}{25!(121-25)!}\right) \quad (18)$$
$$= 42.55^{225} \cong 2^{1225} >> 2^{100}$$

The first bracket is the number of options for an attacker to construct the masked DCT. In contrast, the second matrix is the number of choices to build the sensing matrices, and their product gives large enough value to turn the brute force attack into infeasible for the proposed system.

6.5 **Differential Attack**

We already studied types of attack before requiring analysis involve the whole signal or image at a time. Differential attack analysis is more focused on a single pixel. Therefore, we only take the image block of our interest only because different sensing matrices resist brute force and chosen-ciphertext treat. Therefore, our analysis will be based on a selected specific block using NPCR (Net Pixel Change Rate) and UACI (Unified Average Changing Intensity), given by eq. 19 and 20.

$$NCPR = \frac{\sum_{i,j} D(i,j)}{H*W} * 100\% \quad (19)$$

$$UACI = \frac{1}{H*W}\sum_{i,j}\frac{\left|c(i,j) - c'(i,j)\right|}{255} * 100\% \quad (20)$$

Where H and W are the height and width of the image block. And $c(i,j)$ is the encrypted image block, whereas $c'(i,j)$ also the encrypted image of the block with one of the pixels changed. The value $D(i,j)$ is one if there is a pixel difference between $c(i,j)$ and $c'(i,j)$ otherwise, it is zero. Our samples taken from eight by eight blocks are 100% for NCPR and 0.92% for UACI. This shows all sixty-four-pixel values were undergone changes that would make the design scheme resistive to any attack.

6.6 **Entropy Analysis**

The entropy of our compressed system's encrypted output is the measurement of the system's ability to generate random encrypted output. The entropy H of the image with different probability P of total number N is mathematically expressed and given by eq.21.

$$H = \sum_{i=1}^{N} P_i \log_2 P_i \quad (21)$$

Since our system is designed based on the DCT matrix, many entries are negative. Hence, to compute the logarithmic content of equation (21), we took the cipher image's absolute value and verified that the system has 7.20, 90% of the ideal value.

7. **Conclusion**

In this work, we aimed at a secured transmission of fingerprint images using a compressive sensing approach. To establish security, we have designed a novel deterministic sensing matrix based on a partial orthogonal matrix derived from a Discrete Cosine Transform (DST) matrix. A modified Multiplicative Linear Congruential Generator (MLCG) sub-matrix has been employed to construct the sensing matrix in a deterministic manner. The added shifting factor in MLCG expression enables us to use any rows of the DCT matrix to build our sensing matrix. The traditional MLCG has limitations in choosing any of the rows until the maximum row index of the DCT matrix. By effectively applying the shifting factor, we successfully select any rows entry following the requirement of the sub-matrix to be used as a measurement matrix. The comprehensive simulation result of our proposed compressed sensing system shows that the deterministic sensing matrix has better performance than the non-deterministic or random matrix in terms of memory resource usage and the number of sensors that are effectively used. And this may open a new way for the quest of an optimized alternative fingerprint scanning technology.

8. Conflict of interest

The authors declare that they have no conflict of interest.

References

[1] F. Liu, D. Zhang, 3D fingerprint reconstruction system using feature correspondences and prior estimated finger model, Pattern Recognit. 47 (2014) 178–193. https://doi.org/10.1016/j.patcog.2013.06.009.

[2] M.K. Thakar, T. Sharma, Digital grid method for fingerprint identification and objective report writing, Egypt. J. Forensic Sci. 6 (2016) 194–201. https://doi.org/10.1016/j.ejfs.2016.05.008.

[3] M. Lastra, J. Carabaño, P.D. Gutiérrez, J.M. Benítez, F. Herrera, Fast fingerprint identification using GPUs, Inf. Sci. (Ny). 301 (2015) 195–214. https://doi.org/10.1016/j.ins.2014.12.052.

[4] N. Sato, S. Shigematsu, H. Morimura, M. Yano, K. Kudou, T. Kamei, K. Machida, Novel surface structure and its fabrication process for MEMS fingerprint sensor, IEEE Trans. Electron Devices. 52 (2005) 1026–1032. https://doi.org/10.1109/TED.2005.846342.

[5] M.A.U. Khan, T.M. Khan, D.G. Bailey, Y. Kong, A spatial domain scar removal strategy for fingerprint image enhancement, Pattern Recognit. 60 (2016) 258–274. https://doi.org/10.1016/j.patcog.2016.05.015.

[6] S. Kim, B. Park, B.S. Song, S. Yang, Deep belief network based statistical feature learning for fingerprint liveness detection, Pattern Recognit. Lett. 77 (2016) 58–65. https://doi.org/10.1016/j.patrec.2016.03.015.

[7] E.J. Candès, J. Romberg, T. Tao, Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information, IEEE Trans. Inf. Theory. (2006). https://doi.org/10.1109/TIT.2005.862083.
[8] D.L. Donoho, Compressed sensing, IEEE Trans. Inf. Theory. (2006). https://doi.org/10.1109/TIT.2006.871582.
[9] E.J. Candès, D.L. Donoho, New tight frames of curvelets and optimal representations of objects with piecewise C 2 singularities , Commun. Pure Appl. Math. 57 (2004) 219–266. https://doi.org/10.1002/cpa.10116.
[10] J.B. Allen, L.R. Rabiner, A Unified Approach to Short-Time Fourier Analysis and Synthesis, Proc. IEEE. 65 (1977) 1558–1564. https://doi.org/10.1109/PROC.1977.10770.
[11] S.A. Nandhini, S. Radha, P. Nirmala, R. Kishore, Compressive sensing for images using a variant of Toeplitz matrix for wireless sensor networks, J. Real-Time Image Process. 16 (2019) 1525–1540. https://doi.org/10.1007/s11554-016-0658-z.
[12] G. Chen, M. Maggioni, Multiscale geometric wavelets for the analysis of point clouds, 2010 44th Annu. Conf. Inf. Sci. Syst. CISS 2010. (2010) 1–6. https://doi.org/10.1109/CISS.2010.5464843.
[13] M. Aharon, M. Elad, A. Bruckstein, K-SVD: An algorithm for designing overcomplete dictionaries for sparse representation, IEEE Trans. Signal Process. 54 (2006) 4311–4322. https://doi.org/10.1109/TSP.2006.881199.
[14] J. Mairal, F. Bach FRANCISBACH, J. Ponce JEANPONCE, G. Sapiro, Online Learning for Matrix Factorization and Sparse Coding, J. Mach. Learn. Res. 11 (2010) 19–60. http://www.jmlr.org/papers/volume11/mairal10a/mairal10a.pdf.
[15] K. Kreutz-delgado, J.F. Murray, T.J. Sejnowski, Dictionary Learning Algorithms for Sparse Representation Kenneth, Neural Comput. 15 (2003). https://doi.org/10.1162/089976603762552951.
[16] J. Mairal, F. Bach, J. Ponce, G. Sapiro, Online learning for matrix factorization and sparse coding, J. Mach. Learn. Res. (2010). https://doi.org/10.1145/1756006.1756008.
[17] I. Tawfic, S. Kayhan, Compressed sensing of ECG signal for wireless system with new fast iterative method, Comput. Methods Programs Biomed. (2015). https://doi.org/10.1016/j.cmpb.2015.09.010.
[18] L.F. Polania, R.E. Carrillo, M. Blanco-Velasco, K.E. Barner, Exploiting prior knowledge in compressed sensing wireless ECG systems, IEEE J. Biomed. Heal. Informatics. (2015). https://doi.org/10.1109/JBHI.2014.2325017.
[19] D. Liu, Q. Wang, Y. Zhang, X. Liu, J. Lu, J. Sun, FPGA-based real-time compressed sensing of multichannel EEG signals for wireless body area networks, Biomed. Signal Process. Control. 49 (2019) 221–230. https://doi.org/10.1016/j.bspc.2018.12.019.
[20] Ö. Polat, S.K. Kayhan, High-speed FPGA implementation of orthogonal matching pursuit for compressive sensing signal reconstruction, Comput. Electr. Eng. 71 (2018) 173–190. https://doi.org/10.1016/j.compeleceng.2018.07.017.
[21] D. Gangopadhyay, E.G. Allstot, A.M.R. Dixon, K. Natarajan, S. Gupta, D.J. Allstot, Compressed sensing analog front-end for bio-sensor applications, IEEE J. Solid-State Circuits. (2014). https://doi.org/10.1109/JSSC.2013.2284673.
[22] B. Javidi, Optical encryption using a joint transform correlator architecture, Opt. Eng. (2000). https://doi.org/10.1117/1.1304844.
[23] B. Javidi, Noise performance of double-phase encryption compared to XOR encryption, Opt. Eng. (1999). https://doi.org/10.1117/1.602074.
[24] Y. Zhang, C.H. Zheng, N. Tanno, Optical encryption based on iterative fractional Fourier transform, Opt. Commun. (2002). https://doi.org/10.1016/S0030-4018(02)01113-6.
[25] M.N. Islam, Encryption and multiplexing of fingerprints for enhanced security, 2011 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2011. (2011) 0–3. https://doi.org/10.1109/LISAT.2011.5784235.
[26] G. Mehta, M.K. Dutta, J. Karasek, P.S. Kim, An efficient and lossless fingerprint encryption algorithm using Henon map & Arnold transformation, 2013 Int. Conf. Control Commun. Comput. ICCC 2013. (2013) 485–489. https://doi.org/10.1109/ICCC.2013.6731703.
[27] M. Vidyasagar, A tutorial introduction to compressed sensing, 2016 IEEE 55th Conf. Decis. Control. CDC 2016. (2016) 5091–5104. https://doi.org/10.1109/CDC.2016.7799048.
[28] Y.C. Pati, R. Rezaiifar, P.S. Krishnaprasad, Orthogonal matching pursuit: recursive function approximation with applications to wavelet decomposition, in: Conf. Rec. Asilomar Conf. Signals, Syst. Comput., 1993. https://doi.org/10.1109/acssc.1993.342465.
[29] A. Ravelomanantsoa, H. Rabah, A. Rouane, Compressed Sensing: A Simple Deterministic Measurement Matrix and a Fast Recovery Algorithm, IEEE Trans. Instrum. Meas. 64 (2015) 3405–3413. https://doi.org/10.1109/TIM.2015.2459471.
[30] H. Djelouat, A. Amira, F. Bensaali, I. Boukhennoufa, Secure compressive sensing for ECG monitoring, Comput. Secur. 88 (2020) 101649. https://doi.org/10.1016/j.cose.2019.101649.
[31] R.M. May, Simple mathematical models with very complicated dynamics, Nature. (1976). https://doi.org/10.1038/261459a0.
[32] D. Ruelle, F. Takens, On the nature of turbulence, Commun. Math. Phys. (1971). https://doi.org/10.1007/BF01646553.
[33] M. Kharratzadeh, A. Sharifnassab, M. Babaie-Zadeh, Invariancy of Sparse Recovery Algorithms, IEEE Trans. Inf. Theory. 63 (2017) 3333–3347. https://doi.org/10.1109/TIT.2017.2686428.
[34] M. Aharon, M. Elad, A.M. Bruckstein, On the uniqueness of overcomplete dictionaries, and a practical way to retrieve them, Linear Algebra Appl. (2006). https://doi.org/10.1016/j.laa.2005.06.035.
[35] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, Image quality assessment: From error visibility to structural similarity, IEEE Trans. Image Process. (2004). https://doi.org/10.1109/TIP.2003.819861.
[36] E.J. Candès, The restricted isometry property and its implications for compressed sensing, Comptes Rendus Math. (2008). https://doi.org/10.1016/j.crma.2008.03.014.
[37] L. Chao, J. Han, L. Yan, L. Sun, F. Huang, Z.B. Zhu, S. Wei, H. Ji, D. Ma, Fast compressed sensing analysis for imaging reconstruction with primal dual interior point algorithm, Opt. Lasers Eng. 129 (2020). https://doi.org/10.1016/j.optlaseng.2020.106082.
[38] G.S. Fishman, L.R. Moore III, Erratum: An Exhaustive Analysis of Multiplicative Congruential Random Number Generators with Modulus $2^{31} - 1$, SIAM J. Sci. Stat. Comput. (1986). https://doi.org/10.1137/0907072.
[39] N. Thomos, N. V. Boulgouris, M.G. Strintzis, Optimized transmission of JPEG2000 streams over wireless channels, IEEE Trans. Image Process. (2006). https://doi.org/10.1109/TIP.2005.860338.
[40] X. Li, J. Cai, Robust transmission of JPEG2000 encoded images over packet loss channels, in: Proc. 2007 IEEE Int. Conf. Multimed. Expo, ICME 2007, 2007. https://doi.org/10.1109/icme.2007.4284808.
[41] M. Elad, A.M. Bruckstein, A generalized uncertainty principle and sparse representation in pairs of bases, IEEE Trans. Inf. Theory. (2002). https://doi.org/10.1109/TIT.2002.801410.
[42] S.A. Hossein, A.E. Tabatabaei, N. Zivic, Security analysis of the joint encryption and compressed sensing, in: 2012 20th Telecommun. Forum, TELFOR 2012 - Proc., 2012. https://doi.org/10.1109/TELFOR.2012.6419328.
[43] A. Orsdemir, H.O. Altun, G. Sharma, M.F. Bocko, On the security and robustness of encryption via compressed sensing, in: Proc. - IEEE Mil. Commun. Conf. MILCOM, 2008. https://doi.org/10.1109/MILCOM.2008.4753187.
[44] G. Hu, D. Xiao, Y. Wang, T. Xiang, An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications, J. Vis. Commun. Image Represent. 44 (2017) 116–127. https://doi.org/10.1016/j.jvcir.2017.01.022.
[45] Y. Zhang, L.Y. Zhang, J. Zhou, L. Liu, F. Chen, X. He, A Review of Compressive Sensing in Information Security Field, IEEE Access. (2016). https://doi.org/10.1109/ACCESS.2016.2569421.
[46] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, Int. J. Bifurc. Chaos. (2006). https://doi.org/10.1142/S0218127406015970.
[47] A.A. Shah, S.A. Parah, M. Rashid, M. Elhoseny, Efficient image encryption scheme based on generalized logistic map for real time image processing, J. Real-Time Image Process. 17 (2020) 2139–2151. https://doi.org/10.1007/s11554-020-01008-4.

Workneh Wolde has graduated from Addis Ababa University with a B.Sc. degree in Physics (2008) and M.Sc. in Applied

Electronics from Osmania University (2012). Currently, he is a research scholar at Sharda University's department of electronics and communication engineering. Before his enrolment at Sharda University, he has served as an academic staff at Wollo University and possesses over five years of educational and research experience. He is currently engaged in a project that includes designing and simulation CMOS MEMS pressure sensor array devices for measurement and surface topography scanning.

Dr. Pallavi Gupta did her B.Tech. in Electronics and Communication Engineering and M. Tech in Digital Communication & Ph.D. in Electronics Engineering from Aligarh Muslim University. Dr. Pallvi has a total experience of more than 13 years in academic & 2 year's research. Dr. Pallvi has six papers in international journals & conferences and has filed two patents. Her research interest focused on electronic sensor development. Currently, she is working in electronic and communication engineering at Sharda University as an associate professor.