Multimed Tools Appl (2018) 77:19209–19234
https://doi.org/10.1007/s11042-017-5378-2

Compressive sensing based image compression-encryption using Novel 1D-Chaotic map

R. Ponuma [1] · R. Amutha [1]

Received: 9 May 2017 / Revised: 25 October 2017 / Accepted: 1 November 2017 /
Published online: 11 November 2017

Abstract Compressive sensing based encryption achieves simultaneous compression-encryption by utilizing a low complex sampling process, which is computationally secure. In this paper, a new novel 1D–chaotic map is proposed that is used to construct an incoherence rotated chaotic measurement matrix. The chaotic property of the proposed map is experimentally analysed. The linear measurements obtained are confused and diffused using the chaotic sequence generated using the proposed map. The chaos based measurement matrix construction results in reduced data storage and bandwidth requirements. As it needs to store only the parameters required to generate the chaotic sequence. Also, the sensitivity of the chaos to the parameters makes the data transmission secure. The secret key used in the encryption process is dependent on both the input data and the parameter used to generate the chaotic map. Hence the proposed scheme can resist chosen plaintext attack. The key space of the proposed scheme is large enough to thwart statistical attacks. Experimental results and the security analysis verifies the security and effectiveness of the proposed compression-encryption scheme.

Keywords Chaotic Map · Compressed Sensing · Compression · Encryption · Security

1 Introduction

The innovation in the field of imaging sensors, multimedia systems, optics, affordable storage systems and high-speed internet communication technologies is manifold. Consequently, a colossal amount of data is generated that must be processed and distributed. The major constraints in any multimedia communication systems are limited bandwidth and security. Data compression overcomes bandwidth limitations by reducing the amount of data to be transmitted and stored, whereas encryption thwarts security risks. In [31] the authors proposed

✉ R. Ponuma
ponumar@ssn.edu.in

[1] Department of Electronics and Communication Engineering, SSN College of Engineering, Chennai, India

a wavelet based scheme, that extracts and encodes only approximations of the image using fixed-point arithmetic, which considerably improved the lifetime of the sensors. In [32] only shift and add operations together with BinDCT is used to directly extract and encode the DC coefficient and the first three AC coefficients of an 8 × 8 image blocks. An efficient multimedia communication must provide rapid transmission, information security and prompt retrieval, which can be achieved by performing compression and encryption simultaneously.

Traditional encryption schemes like DES, AES etc. are not suitable for image encryption because of the inherent properties of digital images like bulk data capacity, redundancy and strong correlation among adjacent pixels. Chaos based cryptosystem is widely used due to the properties of chaotic systems like periodicity, sensitive dependence on initial conditions and pseudo-randomness. Zhou et al. [46] proposed a new chaotic system that generates three new one-dimensional chaotic maps by combining existing one-dimensional chaotic maps like the Logistic, Sine and Tent maps. They proved that the new chaotic system has larger chaotic range, excellent diffusion and confusion properties. The proposed scheme has a 4-round encryption structure that could resist brute force attack. A cryptosystem using chaos and permutation-substitution network was proposed by Belazi et al. [3]. A new one-dimensional chaotic map which outperforms the logistic map is first used to diffuse the plain image. The substitution operation is performed by using the s-boxes. A diffusion operation is also implemented using logistic map, thereby increasing the cryptographic strength. Finally, a permutation function is used to obtain an encrypted image, that can resist statistical attacks. In [12] a double image encryption scheme using logistic map and cellular automata is proposed. The keys for the encryption are generated by the convolution of the logistic maps. The least significant bits of the two images are first combined and then diffused using cellular automata. The performance of the proposed scheme and the randomness of the key are experimentally verified. In [8] a multiple image encryption using logistic map and Fractional Fourier Transform is proposed. The fractional order is used as the key in the encryption process. The performance analysis showed that the proposed scheme is highly secure and requires less bandwidth to transmit the encrypted data.

In general, the chaotic cryptosystem based on low dimensional maps are vulnerable to security threats. The low dimensional maps are simple in structure and their chaotic values can be predicted using chaotic signal estimation technologies. Hence higher dimensional chaotic maps or coupled chaotic systems are used in many recent chaos based encryption schemes. In [42] the 3D bit matrix of an image is permuted by using a coupled chaotic system, which is obtained by coupling the Chen system and 3D chaotic map. The permuted image is again diffused to obtain the cipher image. A 2D–Sine Logistic Modulation Map [14] based encryption was proposed by Hua et al. The two one-dimensional maps are combined to form a 2D map which is then used in the encryption of the image. In [3, 14, 42, 46] the chaos based encryption is performed in the pixel domain, whereas in [36] the encryption is performed in both pixel and wavelet domain. A 6D–hyperchotic system together with 2D–DWT is used to encrypt the image. The key for the encryption scheme depends on the image and the hyperchaotic system. A non-uniform cellular automata framework together with hyper-chaos is used for encryption in [29]. Security analysis and experimental results showed that the proposed method has a very large key space and is resistive against noise and other attacks. In many applications in addition to image encryption it also requires image copyright protection and content authentication. Therefore, in areas like military, medicine etc. data hiding techniques [18, 20] can be employed along with encryption to ensure privacy and secrecy of the transmitted images.

The proposed schemes discussed above performs only encryption of the plain image. For an efficient multimedia communication, it is necessary to perform compression and encryption concurrently. [35, 40, 48] presents various models that perform both compression and encryption thereby providing a secure and fast image transmission. Yuen et al. [40] introduced a chaos based joint image compression and encryption scheme using DCT and SHA-1. The SHA-1 algorithm uses the low frequency components and the secret key to generate a message digest which is then used to diffuse the high-frequency coefficients. Huffman code is used to compress the encrypted data. The algorithm exhibited both key and plain image sensitivity. In [48] an image encryption - compression algorithm based on hyper-chaos and Chinese remainder theorem was proposed. The plain image was first shuffled using a 2D hyper-chaotic system. The Chinese remainder theorem was used to diffuse and compress the image simultaneously. The proposed method could encrypt and compress the image with a given compression ratio. A wavelet transform and a cross-chaos map based image compression and encryption is proposed by Tong et al. [35]. The high-dimensional chaotic sequence generated by the proposed cross-chaotic map is used to scramble the image pixels and then substituted by the ciphertext feedback algorithm. The low frequency components of the wavelet transform are encrypted and the security analysis showed that the algorithm has high security, good encryption speed and compression.

Compressive Sensing (CS) [9] is a new sampling, reconstruction technique which can perform sampling and compression simultaneously. Compressive sensing is extensively used in wireless sensor networks and in many applications like image encryption [44], image data hiding [19], healthcare monitoring system [39], activity recognition [17] etc. Dimensionality reduction plays a vital role in extracting salient features from a high dimensional data set. In vision based motion tracking [7, 23] and classification [22] dimensionality reduction is used. For such applications compressive sensing can be employed to achieve dimensionality reduction. CS uses optimization technique to reconstruct the original signal from the linear measurements. The linear measurements are obtained by sampling the signal at significantly lower rate than the Nyquist rate. Optimization techniques are used to maximize the benefits and minimize the production cost in various application. For example, optimization techniques are used in activity recognition [24, 26, 28], water quality prediction [27], predicting political ideology using online behavior of individuals [33], future career path prediction [25] etc.

In the resource constrained environment, it is necessary to reduce the amount of data transmitted and reduce energy consumption. Also, data security is of great importance. In the traditional method of data transmission compression and encryption are done in two steps. The sender compresses the data and then encrypts the compressed data. The receiver decompresses the received data through the channel and then decrypts the decompressed data. Compressive sensing performs the compression and encryption simultaneously. The measurement matrix that is used to compressively sample the signal acts as the shared secret key between the sender and the receiver. Generally, a Gaussian random matrix is used as the measurement matrix. However, in such a scenario the overhead required to transmit and store the secret key is high. In this paper a chaos based compressive sensing is proposed that satisfies the above stringent requirements. Compared with the traditional compressive sensing, chaos based compressive sensing can reduce the overhead required to store and transmit the secret key. Only the parameter required to generate the chaotic sequence must be stored. In addition, the sensitivity of chaos improves the security of data transmission.

In [43] the authors review the different types of encryption models that can be implemented using CS. The paper elaborates the six-different framework for an image cryptosystem, that can be implemented by combining CS with optics and chaos. In compressive sensing, based encryption models the measurement matrix acts as the secret key that is shared between the sender and receiver. In [34] the authors showed that CS based image cryptosystem does not achieve Shannon's definition of perfect secrecy but computational secrecy is accomplished. Even though the secret key i.e. the measurement matrix is not known to the eavesdropper, the recovery of the original signal is a NP-hard problem. Hence providing computational secrecy. Orsdemir et al. [30] analysed the encryption method based on compressive sensing and proved that the method is computationally secure. Cambareri et al. [4] quantified the security of CS based encryption against known-plaintext attack theoretically. They showed that there exist many encoding matrices that generate similar plaintext-ciphertext pair. Hence a brute-force attack to find the encoding matrix is inconclusive.

The security property of the low complexity multiclass encryption is analysed by Cambareri et al. in [5]. The authors first investigate theoretically the properties of the multiclass encryption scheme. The performance bounds on the recovery quality obtained by lower-class receivers with respect to high class ones are derived. They showed that asymptotic spherical secrecy i.e. weak form of secrecy, can be achieved. Cambareri et al. proved that compressive sensing with iid Gaussian encoding matrix has the property that no information can be inferred from the statistical properties of all its possible cipher text but its power. The implications of this property are the basic guarantee that a malicious eavesdropper intercepting the measurement vector will not be able to extract any information on the plain text except for its power. Fay [10] introduced Counter mode of operation in compressive sensing based encryption to achieve probabilistic encryption with security against chosen plaintext attacks. The inherent secrecy of the compressed measurements is solely responsible for the security of the proposed scheme. One secret key is used to encrypt multiple messages. Random binary matrices are generated by evaluating a pseudorandom function at different points by using the secret key, a counter and the matrix row index. Zhang et al. [41] analysed the problem of constructing a CS based symmetric cipher under the key reuse circumstance i.e. the cipher is resistant to common attacks even if a fixed measurement matrix is used multiple times.

Huang and Sakurai [15] proposed a compression combined digital image encryption method that is robust against consecutive packet loss and shear attack. A Gaussian measurement matrix was used to generate the reduced measurements and then the measurements are scrambled using an Arnold map. The scheme exhibited robustness, incoherence, low data volume, key sensitivity and resistance to brute force attack. Zhou et al. [44] introduced a key-controlled measurement matrix for performing hybrid image compression - encryption. They showed that the key-controlled measurement matrix reduces the complexity in the distribution and storage of key. The security of the scheme was verified against different attacks and also the method provided good compression performance. In [45] an image cryptosystem using chaos and compressive sensing, to achieve simultaneous compression-encryption is proposed. In [16] the authors proposed CS based encryption in a parallel computing environment. Since the measurements are linear, the cipher is vulnerable to chosen-plaintext attack. To thwart such attack, the paper proposed a block cipher structure consisting of scrambling, mixing, s-box and chaotic lattice xor. The technique increased compressibility and encryption speed because of the parallel encryption structure. Hu et al. [13] proposed an image coding scheme based on parallel compressive sensing framework. Each column of the two-dimensional image data is sampled in parallel. Since CS sampling is a linear process, security against chosen plaintext attack is achieved by employing a nonlinear chaotic sensing matrix and counter mode of operation. The energy information leakage is overcome by the implementation of a diffusion operation. In [19] a new separable data hiding in encrypted images by using CS and Discrete Fourier Transform (DFT) is proposed. After performing DFT, embedding of the secret image is done on the high frequency parts of real part and imaginary part of DFT. Iterative Reweighted Least Squares Optimization is used as the recovery algorithm of CS.

In this paper, a parallel compressive sensing framework is used to compressively sample the signal using an incoherence rotated chaotic matrix. A novel one-dimensional chaotic map is proposed and it is used in the generation of the measurement matrix. The generation of the chaotic matrix is controlled by a secret key which is dependent on the input image. Further encryption is achieved by performing confusion and diffusion operation using the chaotic sequence generated by the proposed map. The rest of the paper is organised as follows. Section 2 gives a brief introduction about compressive sensing. Section 3 elaborates the proposed chaotic map and analyses its chaotic behaviour. The incoherence rotated chaotic matrix structure and its generation is explained in Section 4. The proposed compression-encryption scheme is explained in Section 5. In Section 6, the experimental results and the performance of the proposed scheme are discussed. Finally, the conclusion is drawn in Section 6.

2 Preliminaries

2.1 Compressive sensing

Classical data acquisition states that, if a signal is sampled at Nyquist rate i.e. twice the maximum frequency it can be perfectly reconstructed. In multimedia applications the Nyquist rate can result in large amount of samples, which has to be compressed for storage and faster transmission.

Compressive Sensing [2] is a new paradigm that states that if a signal is compressible/sparse in some domain, then it can be perfectly reconstructed by sampling at a rate less than the Nyquist sampling rate. The fundamental requirements in compressive sensing are sparsity, measurement matrix and the reconstruction algorithm. Sparsity indicates that the signal has a concise representation in some basis ψ. If an image is sparse in a basis, it has few large coefficients that capture most of the information and all the other coefficients are small. Sparsity leads to efficient estimation, compression and dimensionality reduction. The image data is naturally sparse in some basis.

For a signal x with N real valued samples, its transform coefficients α is given by

$$\alpha = \psi^T x \tag{1}$$

where ψ is the orthogonal basis. Only a few large coefficients of α capture the principal information and all the other coefficients of α are close to zero. A linear measurement process is used to compute the measurements y by projecting x onto a measurement matrix φ. The measurement matrix is of size M×N and the measurements are computed as follows

$$y = \varphi x = \varphi \psi \alpha = \Theta \alpha \tag{2}$$

where $\Theta = \varphi\psi$ is the sensor matrix with size M×N.

The measurement matrix must guarantee the recovery of the signal from a small number ($M < < N$) of measurements y. Candes [6] presented the Restricted Isometry Property (RIP) as a sufficient condition on the sensing matrix to perform perfect recovery. A matrix φ satisfies the restricted isometry property if

$$(1-\delta_k)\|f\|_2^2 \leq \|\varphi f\|_2^2 \leq (1+\delta_k)\|f\|_2^2 \tag{3}$$

holds for all vectors f Є R^n with sparsity k. In [1] Banderia et al. proved that the determination of RIP for a matrix is NP-hard. An alternative approach to perfect reconstruction is to ensure that the measurement matrix φ is incoherent with the basis ψ.

The signal x can be recovered from the measurements y by finding the sparsest solution

$$\min \ \|\alpha\|_0 \quad subject \quad to, \quad y = \Theta\alpha \tag{4}$$

The commonly employed methods are Matching Pursuit (MP), Orthogonal Matching Pursuit (OMP), Smoothed l^0 ($\mathrm{S}l^0$) and so on. In this paper OMP [21] is used for reconstruction.

2.2 Security analysis of compressive sensing measurements

In this section security analysis of the compressive sensing measurements against different attacks are discussed. As CS sampling is a linear process it is prone to known/chosen-plaintext attacks. The Adversary model for the proposed scheme is that an eavesdropper has access to the encryption oracle. The eavesdropper also has access to known plaintext-ciphertext pair. From the captured data the eavesdropper tries to recover the secret key used by the encryption oracle. As proved by Rachlin and Baron [34], in CS recovering the original signal without the appropriate secret key (i.e. the measurement matrix) is equivalent to solving a NP-hard problem. In the proposed scheme a secret key shared between the sender and receiver is used as the seed to generate the measurement matrix φ. Since a data dependent key generation is used different symmetric keys are generated for different images. Therefore, a security breach will not reveal the other secret keys. Hence the adversary cannot estimate a fixed measurement matrix φ through known-plaintext attack. The eavesdropper will not be able to gather enough data to launch a known-plaintext attack as a new measurement matrix is generated for each plaintext.

The CS sampling process is vulnerable to energy leakage. In the proposed scheme a parallel CS sampling technique is used. The sparse transform coefficients of the plain image are measured column by column. Finally, a chaos based confusion-diffusion is employed to obtain the cipher image. The parallel CS sampling results in the preservation of energy information within each column. In [13] it is showed that chaos based diffusion operation results in uniform energy distribution over the entire image. Therefore, the proposed scheme mitigates the problem of energy information leakage.

In the proposed scheme a chaos based measurement matrix is used for simultaneous compression-encryption. The security of chaos based CS depends on the chaotic map's sensitivity to the initial condition and the control parameters. In the case of the widely used Gaussian measurement matrix, it is easy for the eavesdropper to decrypt the data by using an intercepted approximate key. In chaos based measurement matrix construction even a small perturbation of the order of 10^{-15} to the secret key makes the decryption unsuccessful. Security against these perturbations are quantified in Section 4.6.

3 Proposed scheme

The proposed compression-encryption scheme involves key scheduling, Chaotic map generation, IRC measurement matrix construction, compressive sampling, permutation, quantization and diffusion.

3.1 Proposed chaotic map

Chaotic maps are dynamical systems with high sensitivity to initial conditions and control parameter. An arbitrary small change in the initial conditions leads to significant deviations. This sensitivity puts an effective limit on our ability to predict the behavior of chaotic systems over long periods of time. Chaos based encryption schemes employs the initial conditions as secret key for encryption. It is impossible to know the initial conditions exactly with infinite precision. Hence, chaos based encryption schemes can resist attacks from intruders. The chaotic maps can be classified into one-dimensional chaotic maps and high-dimensional chaotic maps. The one-dimensional chaotic maps usually contain one variable and a few parameters. The 1D–maps like Logistic, Sine and Tent maps have simple structures. The chaotic structure can be determined by using chaotic signal estimation technologies. Therefore, the encryption schemes based on these 1D maps are vulnerable to various cryptographic attacks. Hence higher dimensional chaotic maps are employed for encryption. Logistic map is simple in structure and it is widely used in image encryption. The logistic map has single control parameter μ_L and is defined by the following equation

$$L_{n+1} = \mu_L L_n (1 - L_n); \ \ L \in [0, 1], 0 \le \mu_L \le 4 \tag{5}$$

The Sine Map has single control parameter μ_S and is defined as

$$S_{n+1} = \mu_S \sin(\pi * S_n); \ \ S \in [0, 1], 0 \le \mu_S \le 1 \tag{6}$$

The Tent Map is given by

$$T_{n+1} = 1 - \mu_T * |T_n - 0.5|; T \in [0, 1], 0 \le \mu_T \le 2 \tag{7}$$

In the 1D maps the next iteration value is obtained by a linear transform. Hence it can be predicted easily. Hence for chaos based cryptosystem the security can be enhanced by combining the existing 1D maps to form a one-dimensional or a higher dimensional chaotic map. Several new one-dimensional chaotic maps are proposed in literature. In this paper, a new 1D chaotic map is proposed by combining the Logistic, Sine and the Tent map. The chaotic behavior of the new map is verified by performing the bifurcation and Lyapunov exponent analysis. The proposed Sine-Tent-Logistic map (STL) is formed by performing fusion and cascading operations on the three 1D maps. The fusion operation generates new chaotic maps by mixing the dynamics of two seed maps in a nonlinear way. The cascading operation connects two 1D maps in series [47]. The new map is generated by first performing fusion operation on the two seed maps – Logistic and Tent map. Secondly, cascading operation is performed using the Sine map and the map generated in the first step. The structure for generating the proposed one-dimensional map is as shown in Fig. 1.

The Tent map exhibits highly chaotic behavior when the control parameter $\mu_T = 2$, therefore in the first seed map the control parameter is taken as the constant value 2. The fusion operation combines the two seed maps – Tent, Logistic map in a non-linear way. The input

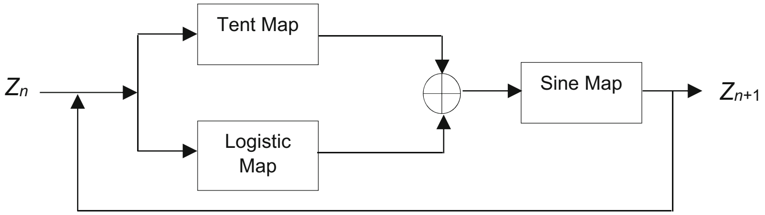

Fig. 1 Structure of proposed chaotic map

Z_n is simultaneously fed into the two seed maps and then the output of the two seed maps are added together. The cascading operation connects the Sine map and the fusion of the Tent, Logistic map in series to obtain Z_{n+1}. The proposed map is mathematically represented as

$$Z_{n+1} = \begin{cases} \sin(\pi((1-2*|Z_n-0.5|)+(\mu*Z_n*(1-Z_n))))-1, Z_n > 1 \\ \sin(\pi((1-2*|Z_n-0.5|)+(\mu*Z_n*(1-Z_n))))+1, Z_n < 0 \end{cases} ; Z_n \in (0,1), \mu > 0 \quad (8)$$

where $n = 0, 1, 2, \ldots$.

The chaotic behavior of the proposed map is evaluated using the Lyapunov exponent, Shannon entropy and bifurcation analysis. The performance of the proposed map is compared with that of the one-dimensional seed maps. The bifurcation diagrams of the seed maps and the proposed map are shown in Fig. 2. The bifurcation diagram is obtained by plotting the chaotic sequence generated for an initial value 0.2301. From Fig. 2, we can infer that the chaotic sequence generated by the proposed STL map is highly chaotic and uniformly distributed for $\mu \in (0, 4)$. The seed maps are not uniformly distributed, they are chaotic in certain intervals of μ. when the parameter $\mu_L \in [3.86, 4]$, the logistic map exhibits good chaotic characters. The logistic map exhibits chaotic behavior when $\mu_L > 3$ with intermittent intervals of stability called the periodic window. For $3.284 \le \mu_L \le 3.8415$ the logistic map exhibits a stable 3-cycle [11]. As μ_L moves further away from this periodic window, interspersed periods of chaos start appearing and fully chaotic behavior is once again achieved. For an initial value of $x_0 = 0.2301$, the bifurcation diagram of the logistic map in the interval [3.5, 4] is shown in Fig.2(a). From the figure, we can observe that for $\mu_L = 3.86$ the logistic map exhibits a fully chaotic behavior.

Chaotic behavior of a map can be evaluated using the Lyapunov exponent. The Lyapunov Exponent (LE) is a measure of the sensitivity of the map to the initial condition i.e. an estimate of the amount of chaos in a system. If the Lyapunov exponent is negative then the system is stable. A positive LE quantify the exponential divergence from the initial condition. The greater the value of the maximum LE, greater the chaos in a system. The LE of the seed maps and the proposed maps are shown in Fig. 3. The LE of the proposed map is positive for all $\mu \in (0, 4)$. From Fig. 3(a), we can see that the logistic map is not chaotic for some values of μ. The comparison of the LE of the proposed map and the 1D map employed by Belazi et al. [3] is shown in Fig.3(b). The values of the initial parameter Z_0 and the control parameter μ of the chaotic map is used as the secret key in the encryption operation. For $\mu \in (0, 8)$ the map in [3] is chaotic in certain bands, whereas the proposed map is highly chaotic in the entire range. Hence, a larger key space can be obtained when using the proposed map thereby increasing the cryptographic strength of the algorithm. The Lyapunov exponent determines the overall predictability of the system. The Lyapunov exponents sharply discriminate between the different dynamics. A fixed point or stable periodic orbit will have all negative exponents, a LE of zero indicates that the system is in some sort of steady state mode and a positive LE

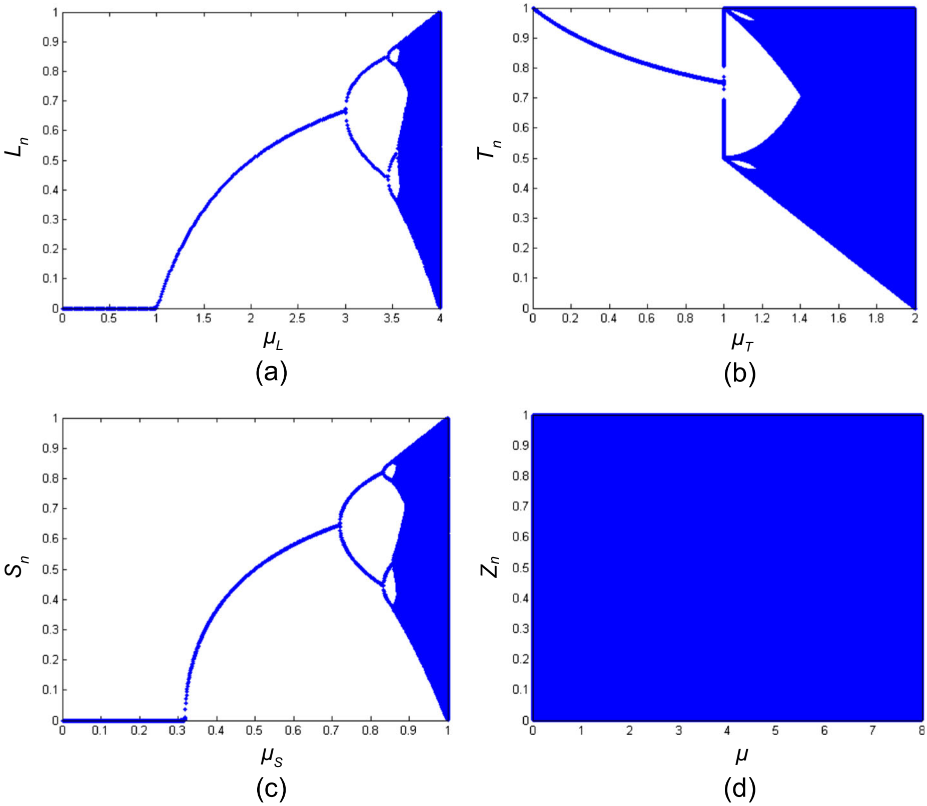

Fig. 2 Bifurcation diagram of (a) Logistic map, (b) Tent map, (c) Sine map, (d) Proposed Chaotic map

indicates that the system is chaotic. Also, larger the Lyapunov exponent greater the chaos of the system. Table 1 shows the comparison between the LE values of the Logistic map, Proposed map and the map used in [3]. For a given initial value and control parameter the LE of different maps are computed and tabulated in Table 1. The sequence generated by the maps for the given parameters are chaotic, as indicated by the positive LE values in Table 1. Also, it is inferred that the LE obtained for the chaotic sequence generated using the proposed map is greater than the LE of the compared maps i.e. the sequence generated using the proposed map is more chaotic. Therefore, the proposed map is more suitable for measurement matrix construction.

For the exact recovery of signal from the reduced measurements, the measurement matrix must satisfy the Restricted Isometry Property. The measurement matrix constructed using elements drawn from distributions like Gaussian and Bernoulli satisfies the RIP condition with high probability. The drawback of these random distribution based measurement matrix construction is hardware implementation, the overhead to store and transmit the same. Yu et al. [38] employed chaotic sequence in the construction of the measurement matrix. They showed that the pseudorandom measurement matrix constructed using the chaotic sequence satisfied the RIP with overwhelming probability. The hardware implementation of the chaotic matrix can be realized easily and only the initial condition, the control parameter should be stored and transmitted. The experimental results verified that the performance of the chaotic

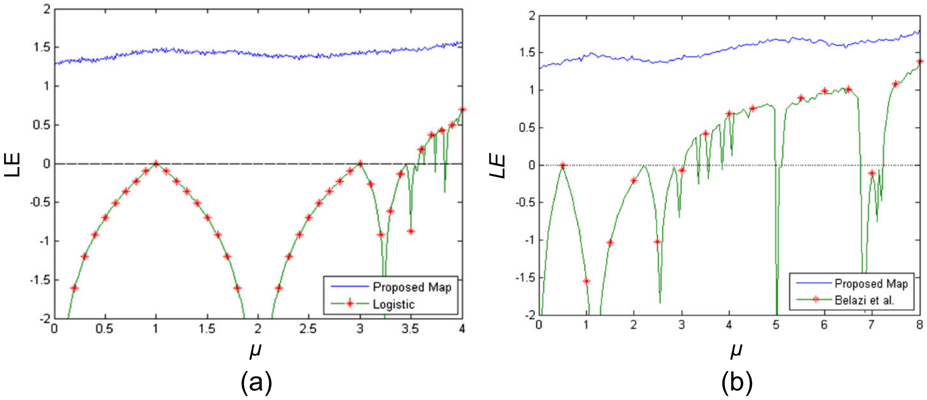

Fig. 3 Comparison of Lyapunov Exponent (LE)

measurement matrix is comparable to that of the commonly used Gaussian random matrix. Yu et al. showed that chaotic measurement matrix can be used in compressive sensing applications. The embedding of security in compressive sensing application can be achieved by using the initial conditions and the control parameter as the shared key between the sender and the receiver.

3.2 Generation of parameters of Chaotic map

The generation of the chaotic map is controlled by the initial parameter Z_0 and the control parameter μ. These two parameters are used as the shared secret key between the sender and receiver. The secret key is distributed through a secure channel. The plain image is used in the key generation process. A 256-bit secret key K is obtained using the SHA-256 hash function on the plain image. The 256-bit key is divided into eight subkeys of length 32-bits, such that

$$K = k_1, k_2, \cdots, k_8; \quad k_i = \left\{k_{i,0}, k_{i,1}, \cdots, k_{i,31}\right\} \tag{9}$$

where $k_{i,\,j}$ denotes the j^{th} bit in the i^{th} subkey.

The subkeys together with the secret keys Z'_0, μ' is used to generate the initial conditions and the control parameters of the chaotic maps used in the encryption process.

$$\begin{aligned} Z_{0k} &= \left(kZ_0^{'} + t_{2k-1}\right) \bmod 1 \\ \mu_k &= \left(k\mu_0^{'} + t_{2k}\right) \bmod 8; k = 1, 2, 3, 4 \end{aligned} \tag{10}$$

Table 1 Comparison of Lyapunov Exponent value for different Initial Parameter (IP) and Control Parameters (CP)

(IP, CP)	Lyapunov Exponent		
	Proposed Map	Logistic Map	Map in [3]
(0.5301, 3.99)	1.5350	0.6475	0.6636
(0.2874, 3.9541)	1.5526	0.5875	0.5936
(0.1011, 3.7862)	1.5033	0.4090	0.5536
(0.7432, 3.6254)	1.4629	0.1975	0.4163

where t_i is the intermediate value. The intermediate values are computed using the subkeys k_i as follows,

$$t_i = \sum_{j=1}^{32} k_{i,j} * \left(\frac{2^{32-j}}{2^{32}}\right); \; i = 1, 2, \cdots 8 \tag{11}$$

By varying the keys Z_0' and μ' different secret keys can be generated for the same image. Hence it is difficult for an attacker to find the secret key. To thwart chosen plaintext attack, the reuse of measurement matrix should be avoided. By using the key controlled chaotic measurement matrix construction and input dependent key generation the chosen plaintext attack can be resisted by the proposed compression-encryption scheme.

3.3 Chaotic measurement matrix generation

The measurement matrix used for compressive sampling and reconstruction is constructed using the chaotic sequence generated by the proposed map. The measurement matrix construction is based on the Incoherence Rotated Chaotic (IRC) as proposed by Yao et al. [37]. They proved that the IRC measurement matrix satisfied RIP and has better performance than Gaussian matrix, Bernoulli matrix etc. The proposed map is used to generate a chaotic sequence Z. The chaotic sequence is then down sampled at sampling distance $d = 10$ and transformed to obtain a sequence r. The construction of the IRC matrix $\varphi_{M \times N}$ is as follows,

1. A chaotic sequence of length $N_0 + dN$ is generated using the proposed map, whose initial parameter is Z_0 and the control parameter is μ. The Initial $N_0 = 1000$ values of the chaotic sequence are neglected to remove the transient effect.
2. The chaotic sequence is sampled at a distance d and a transformed sequence is obtained using

$$r_i = 1\text{–}2Z_{N_0+id}, i = 1, 2, \cdots \tag{12}$$

3. The transformed sequence is then employed to construct a IRC matrix whose structure is given below.

$$\varphi = \sqrt{\frac{1}{2M}} \begin{bmatrix} r_1 & r_2 & \cdots & r_{N-1} & r_N \\ \eta r_N & r_1 & r_2 & \cdots & r_{N-1} \\ \eta r_{N-1} & \eta^2 r_n & r_1 & \cdots & r_{N-2} \\ \eta r_{N-2} & \eta^2 r_{N-1} & \eta^3 r_N & \cdots & r_{N-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \eta r_{N-M+2} & \eta^2 r_{N-M+3} & \eta^3 r_{N-M+4} & \cdots & r_{N-M+1} \end{bmatrix} \tag{13}$$

where η is the incoherent coefficient and M is the number of measurements.

3.4 Proposed compression-encryption scheme

The overall schematic of the proposed scheme is shown in Fig. 4(a). The block diagram of the proposed compression-encryption scheme is given in Fig. 4(b).

The proposed scheme is as follows,

1. The SHA-256 hash function of the plain image is generated and a 256-bit secret key K is obtained. The secret key K and the parameters Z_0', μ' are used to generate the initial

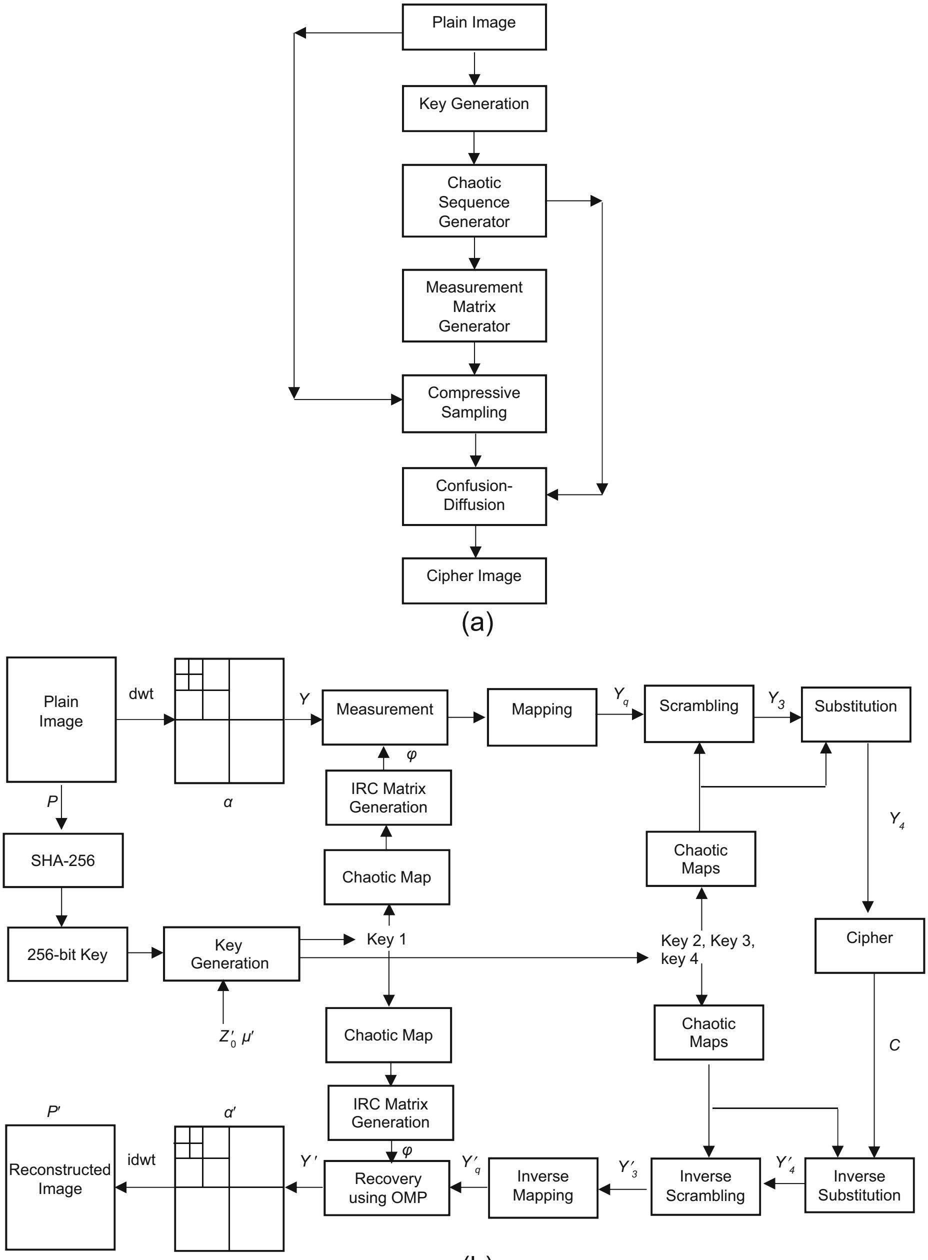

Fig. 4 (a) Flowchart of the proposed scheme (b) Block diagram of the proposed compression-encryption scheme

condition and the control parameters for the four chaotic maps used in the compression-encryption scheme as given in Section 3.2.

2. The plain image P of size $N \times N$ is transformed using the DWT to obtain the sparse coefficients matrix α whose size is same as that of the plain image.
3. The measurement matrix φ of size $M \times N$ is constructed using the chaotic sequence generated using the proposed STL map as given in Section 3.3. The number of measurements $M =$ round (Sampling Ratio × N).
4. Each column (x_i) of the coefficient matrix α, of length N, is measured using parallel compressive sensing using the measurement matrix φ as given below,

$$y_i = \varphi\ x_i \tag{14}$$

where the size of x_i is $N \times 1$ and the measurement y_i is of size $M \times 1$. The measurement Y of the coefficient matrix α is represented as

$$Y = [y_1, y_2, \cdots, y_N] \tag{15}$$

5. The measurement Y of size $M \times N$ is then mapped to the interval [0, 255] using

$$Y_q = round\left(\frac{255*(Y - Y_{\min})}{Y_{\max} - Y_{\min}}\right) \tag{16}$$

where $Y_{\min}$ and $Y_{\max}$ are the maximum and minimum values of the measurement Y. *round*(x) rounds the value of x to the nearest integer.

6. Block Scrambling: The mapped measurements Y_q are then divided into blocks of size $b_1 \times b_2$, where $b_1 = M / \gcd(M, N)$ and $b_2 = N / \gcd(M, N)$. The number of blocks b depends on the number of measurements M. The blocks are then scrambled using Arnold transform to obtain scrambled measurements Y_1. If the block index is (p, q), then the scrambled index of the block after Arnold transform is given by (p', q')

$$\begin{bmatrix} p' \\ q' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} p \\ q \end{bmatrix} \mathrm{mod} \sqrt{b} \tag{17}$$

By performing l iterations of Arnold transform the security of the encryption can be greatly enhanced.

7. Row Scrambling: The scrambled measurements (Y_1) are then subjected to row scrambling using the STL map. A chaotic sequence of length $2M$ is generated. The first M elements of the sequence is neglected to remove the transient effect. Then the sequence of length M is sorted in ascending order to obtain the index sequence. The index sequence is then used to scramble the rows of Y_1 to obtain Y_2.

8. Column Scrambling: Column scrambling is applied on Y_2 using the proposed STL map. A chaotic sequence of length $2N$ is generated using the STL map. The first N elements of the sequence is neglected to remove the transient effect. Then the sequence of length N is sorted in ascending order to obtain the index sequence. The index sequence is then used to scramble the columns of Y_2 to obtain Y_3.
9. Diffusion: Y_3 is then rasterized to form a sequence (Y_4) of length $MN \times 1$. The cipher image (C) is obtained by performing sequential xor operation between Y_4 and the integer sequence (*int_seq*) obtained from the chaotic sequence generated by the proposed map.

$$C_i = \begin{cases} Y_4(i) \oplus \mathrm{int\_}seq(i), & i = 1 \\ Y_4(i) \oplus \mathrm{int\_}seq(i) \oplus C_{i-1}, & i = 2, 3, \cdots, MN \end{cases} \tag{18}$$

where int_$seq = \lfloor \mathrm{mod}\,(Z \times 10^{14}, 256) \rfloor$ and the length of the sequence is $MN \times 1$. $\lfloor x \rfloor$ calculates the largest integer that is less than or equal to x.

The sequence C_i is reshaped to obtain the cipher image of dimension $M \times N$. The proposed compression-encryption algorithm is summarized in Table 2. At the receiver, the cipher image obtained is subjected to inverse operations which are performed in the reverse order. The shared secret key between the sender and receiver is used to generate the four-chaotic sequences, which are then used to descramble and reconstruct the original image. The OMP algorithm is used for the reconstruction of the transform coefficients and inverse DWT is applied to reconstruct the plain image.

4 Experimental results and analysis

The test images are taken from USC-SIPI Miscellaneous image data set. The test images are resized to a size 256 × 256. The plain image is transformed using DWT to obtain the sparse transform coefficients. The DWT decomposition is achieved using the 'Symlet4' wavelet function. A four-level wavelet decomposition is used. The parameters of the chaotic maps used as the shared secret key are $Z_0^{'} = 0.5489$, $\mu' = 4.0856$. The IRC measurement matrix is constructed using the chaotic sequence and used to compressively sample the sparse transform coefficients. The chaotic sequence is down sampled using a sampling interval $d = 10$. The parameters used in the construction of IRC matrix are $\eta = 0.85$ and M, the number of measurements. The measurements are confused and diffused to obtain the cipher image. The

Table 2 Summarized proposed compression-encryption Algorithm

Algorithm Compression-Encryption Algorithm
1. Compute the 256-bit secret key using SHA-256 hash function and the plain image.
2. Generate the parameters of the proposed chaotic map 256-bit secret key and parameters Z'_0, μ'.
3. Generate the chaotic sequence using proposed map and construct the measurement matrix φ.
4. Transform the plain image using DWT to obtain the sparse coefficients.
5. Measure the sparse coefficients using parallel compressive sensing.
6. Map the measurements to the interval [0, 255].
7. Scramble the mapped measurements using the sequence generated using the proposed chaotic map.
8. Xor the scrambled measurements with the chaotic sequence generated using the proposed map to obtain the cipher image.

proposed scheme was tested using five different test images. The OMP algorithm is used for the reconstruction operation. The plain image, cipher image, the reconstructed image and their corresponding histogram are as shown in Fig. 5.

4.1 PSNR and SSIM analysis

The proposed scheme compresses and encrypt the plain image simultaneously. The quality of the reconstructed image can be evaluated by computing the Peak Signal to Noise Ratio (PSNR) and the Structural Similarity Index (SSIM). Mathematically PSNR is defined by,

$$PSNR = 10\log\frac{255^2}{\left(1/N^2\right)\sum_{i=1}^{N}\sum_{j=1}^{N}\left[P(i,j)-P'(i,j)\right]^2} \tag{19}$$

where $P(i, j)$ is the plain image and $P'(i, j)$ is the reconstructed image. The test image is of size $N \times N$. Structural Similarity Index (SSIM) is used for measuring the similarity between plain image and reconstructed image. The SSIM is given by

$$SSIM = \frac{\left(2\,\mu_P\,\mu_{P'}+C_1\right)\left(2\,\sigma_{PP'}+C_2\right)}{\left(\mu_P^2+\mu_{P'}^2+C_1\right)\left(\sigma_P^2+\sigma_{P'}^2+C_2\right)} \tag{20}$$

where $C_1 = 0.01 \times (2^8–1)$, $C_2 = 0.01 \times (2^8–1)$, μ_P, $\mu_{P'}$, σ_P,$\sigma_{P'}$, $\sigma_{PP'}$ are the mean, standard deviation and cross-covariance of the plain and reconstructed image respectively. The effectiveness of the IRC measurement matrix constructed using the proposed map is verified by comparing it to other measurement matrices. The measurement matrices used for comparison are the Gaussian matrix, Bernoulli matrix, Hadamard matrix and the IRC matrix constructed

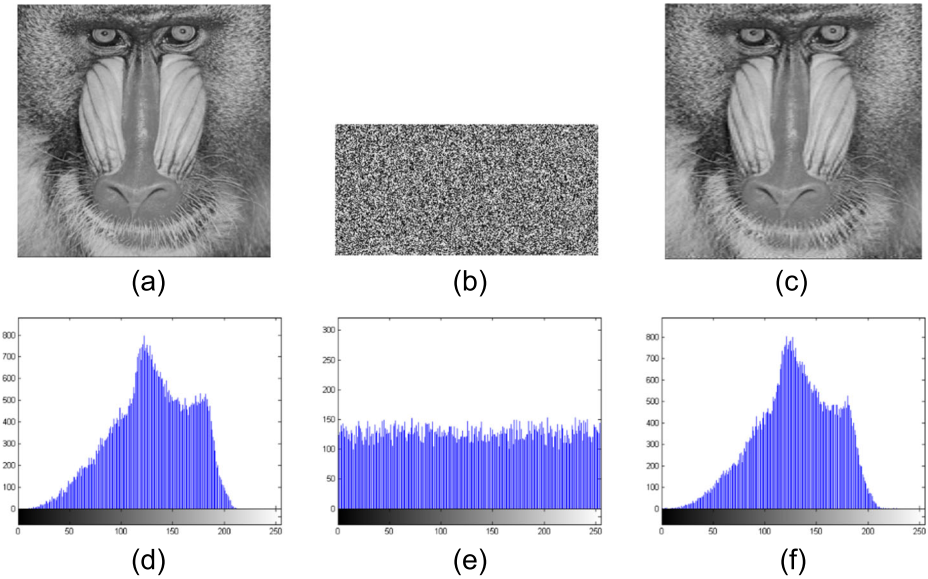

Fig. 5 (a) Plain Image, (b) Cipher image, (c) Reconstructed Image; Histogram of (d) Plain Image, (e) Cipher image, (f) Reconstructed Image

using the chaotic sequence generated by the logistic map. For the test image Peppers of size 256 × 256, the sampling ratio is varied and the PSNR is computed and tabulated in Table 3 for different measurement matrices. From Table 3, we can infer that the PSNR value is high for the proposed measurement matrix i.e. the quality of the reconstructed image is better for the measurement matrix constructed using the proposed map. The PSNR and SSIM of the test images Baboon, Boat, Lake, Man and Peppers are computed for different sampling ratio and tabulated in Table 4. The PSNR and SSIM values are compared with the schemes proposed in [13] and [45]. From Table 4, it is evident that the proposed scheme achieves high PSNR compared to other schemes. The average PSNR is approximately 8 dB higher than that obtained in [13] and approximately 6 dB higher than the scheme in [45]. From Table 3, we also infer that the reconstruction quality of the proposed scheme is better as the average SSIM value achieved using the proposed scheme is high. The SSIM of the proposed scheme is higher than [13], [45] by 43.22%, 77.29% respectively. In Fig. 6 the PSNR of different test images obtained using the proposed and the compared schemes are plotted. Fig.6 clearly shows that the PSNR values for the proposed scheme are higher for all five test images compared with that of [13] and [45].

4.2 Histogram analysis

Histogram graphically represent the distribution of the pixel intensities of a digital image. The histogram of the plain image is unique, which makes it vulnerable to statistical attacks. To thwart such attacks the histogram of the encrypted images must have uniform distribution and significantly different from the plain image. Fig. 7 shows the histogram of the test images and their corresponding cipher. The histogram of the ciphers is relatively uniform and different from the plain image. Hence the proposed technique is robust against statistical attacks.

4.3 Correlation analysis

The digital images pixels are highly correlated. An encryption algorithm resistant to statistical attack must be able to break the correlation between the pixels given by

Table 3 Comparison of PSNR of reconstructed peppers image for different measurement Matrix for varying sampling ratio

Sampling Ratio	PSNR (dB)				
	IRC matrix		Gaussian	Bernoulli	Hadamard
	Proposed Map	Logistic Map			
0.3	27.6985	27.4684	12.6751	13.1001	17.1415
0.4	30.2356	28.7934	21.7792	20.9644	21.3683
0.5	32.2387	30.1762	23.5817	22.5974	24.1497
0.6	32.1281	30.5455	23.7606	23.9693	25.8599
0.7	33.2777	30.8514	25.8706	28.2969	24.1126
0.8	33.4866	31.0300	25.6785	29.3910	24.0670
Average	30.2809	29.1806	20.1495	20.8645	20.7145

Table 4 PSNR and SSIM analysis for different test images for sampling ratio = 0.5

Test Images	PSNR (dB)			SSIM		
	Proposed	[13]	[45]	Proposed	[13]	[45]
Baboon	28.9701	20.5268	22.1599	0.8774	0.5420	0.4616
Boat	28.5048	22.2174	22.6369	0.8224	0.5753	0.4767
Lake	29.2761	19.9962	21.5376	0.8201	0.5783	0.4496
Man	29.0090	20.8783	23.0375	0.8574	0.6049	0.4654
Peppers	32.2387	23.0676	24.6136	0.8376	0.6427	0.5242
Average	29.5997	21.3373	22.7971	0.8430	0.5886	0.4755

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}} \tag{21}$$

where $\operatorname{cov}(x,y)=\frac{1}{P}\sum_{i=1}^{P}[x_i-E(x)][y_i-E(y)]$, $D(x)=\frac{1}{P}\sum_i^P[x_i-E(x)]^2$, $E(x)=\frac{1}{P}\sum_{i=1}^{P}x_i$.

2000 pixels and their corresponding adjacent pixels along the horizontal, vertical and diagonal directions were randomly chosen for the correlation analysis. A correlation coefficient value of one represents a highly-correlated image which is susceptible to statistical attacks. So, for a cipher image the correlation coefficient must be close to zero. From the Table 5, we infer that in the proposed scheme, the correlation between adjacent pixels in the cipher image is negligible. Table 5 also shows that the correlation coefficient of the cipher is very negligible when compared with the plain image. In comparison to the correlation coefficient achieved by the algorithms [13] and [45], the proposed method is better in the horizontal direction and comparable with the other schemes in the vertical and diagonal direction. Fig. 8 shows the pictorial representation of the distribution of the pixels

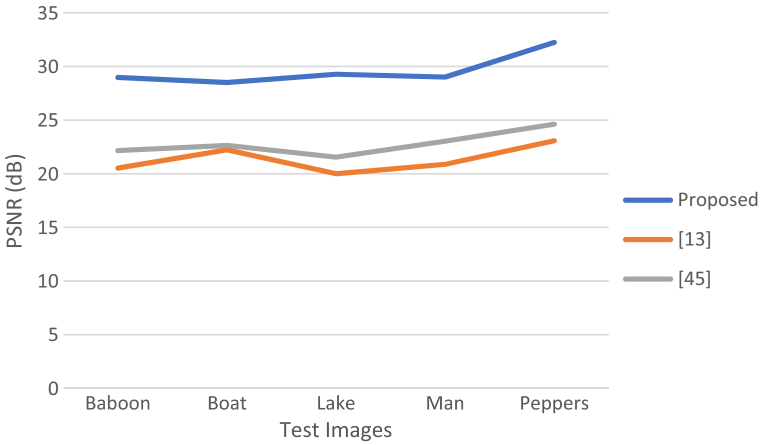

Fig. 6 Comparison of PSNR

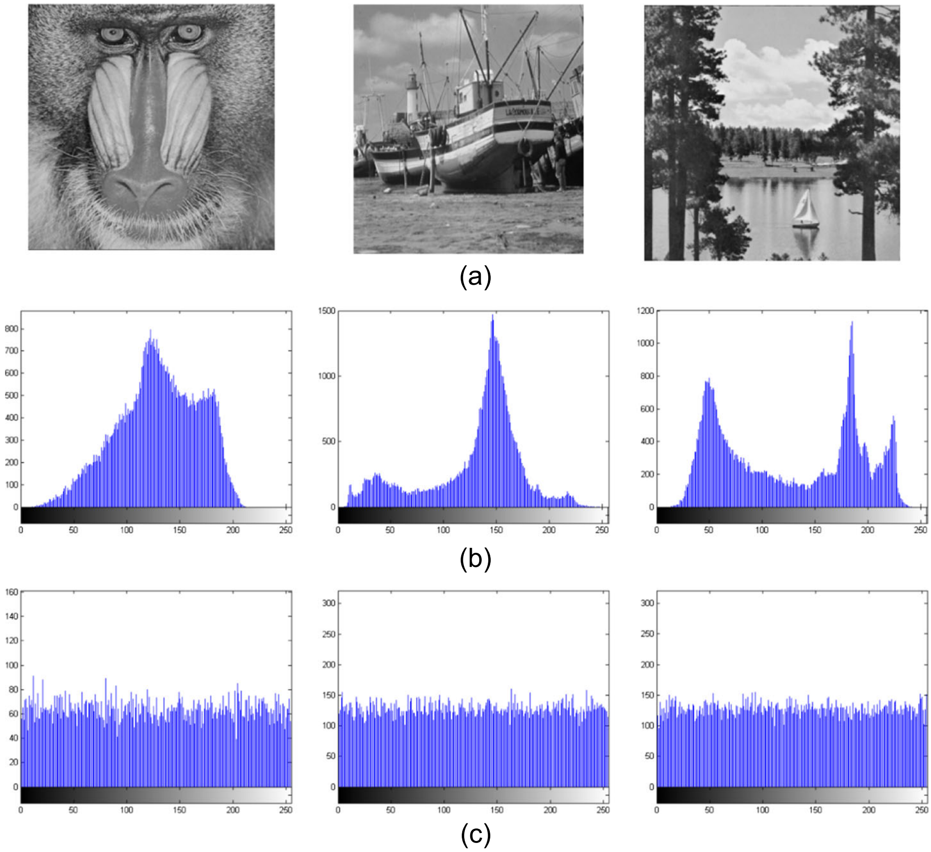

Fig. 7 (a) Test Images, (b) Histogram of Test images, (c) Histogram of Cipher images

in plain and cipher images in the horizontal, vertical and diagonal direction for the test image Peppers.

4.4 Entropy analysis

Entropy is used to measure the randomness of the image. The entropy of the image is given by,

$$H(X) = -\sum_{i=1}^{N\times N} \Pr(I_i)\log_2\Pr(I_i) \tag{22}$$

where $\Pr(I_\mathrm{i})$ is the probability of I_i. For an image with 256 Grey levels the absolute maximum of entropy is 8 bits per pixel. The maximum entropy is obtained when the gray levels have equal probability of occurrence. Therefore, the maximum entropy is achieved when the histogram is flat. Hence for a cipher image, the entropy value should be close to 8. From Table 6, we can infer that the encrypted image has high randomness as the entropy of cipher is close to theoretical value of 8. The average entropy of the proposed scheme is 7.9941 which is better than the entropy of the scheme in [45] and equal to the average entropy in [13].

Table 5 Comparison of correlation coefficient

Test Image	Direction	Correlation Coefficient of Plain Image	Correlation Coefficient of Cipher Image		
			Proposed	[13]	[45]
Baboon	Horizontal	0.8857	0.0003	0.0074	−0.0235
	Vertical	0.8309	−0.0162	0.0164	0.0234
	Diagonal	0.7956	0.0134	0.0108	−0.0193
Boat	Horizontal	0.9223	−0.0037	0.02003	0.0264
	Vertical	0.9440	−0.0177	0.0030	0.0154
	Diagonal	0.8742	−0.0131	−0.0443	0.0308
Lake	Horizontal	0.9587	−0.0005	0.0146	−0.0118
	Vertical	0.9570	−0.0179	0.0086	−0.0199
	Diagonal	0.9321	0.0291	−0.0101	0.0005
Man	Horizontal	0.9455	0.0072	−0.0038	0.0324
	Vertical	0.9574	0.0062	−0.0006	0.0137
	Diagonal	0.9071	0.0127	−0.0045	−0.0152
Peppers	Horizontal	0.9636	0.0001	0.0233	0.0325
	Vertical	0.9757	0.0315	−0.0077	−0.0192
	Diagonal	0.9414	−0.0035	0.0078	0.0133
Average	Horizontal	0.9352	−0.0005	0.0124	0.0112
	Vertical	0.9330	−0.0028	0.0039	0.0027
	Diagonal	0.8901	0.0077	−0.0081	0.0020

4.5 UACI and NPCR analysis

The one-bit pixel change can lead to considerably distinct cipher image. The sensitivity to this change is measured by the Number of Pixels Change Rate (NPCR) and by Unified Average Changing Intensity (UACI) computed using the expression given below

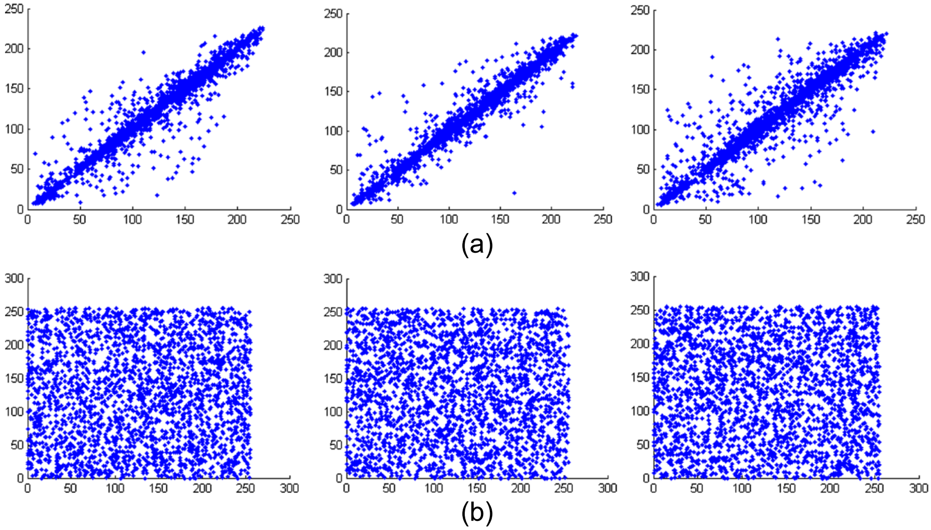

Fig. 8 Scatter plot of the correlation coefficient for the test image Peppers (a) Plain image (b) Cipher image

Table 6 Entropy analysis

Test Image	Entropy of Plain Image	Entropy of Cipher image		
		Proposed	[13]	[45]
Baboon	7.5770	7.9949	7.9938	7.9890
Boat	7.5360	7.9944	7.9939	7.9885
Lake	7.2283	7.9939	7.9949	7.9890
Man	7.1583	7.9942	7.9942	7.9883
Peppers	7.4582	7.9931	7.9938	7.9889
Average	7.3916	7.9941	7.9941	7.9887

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{23}$$

$$UACI = \frac{1}{M \times N} \frac{\sum_{i,j} \left| C_1(i,j) - C_2(i,j) \right|}{L} \times 100\% \tag{24}$$

C_1 (i, j) and C_2 (i, j) are the values of the pixels in the position (i, j) of the two ciphered-image C_1 and C_2 respectively; L is the number of gray levels. D (i, j) is determined based on the rule

$$D(i,j) = \begin{cases} 0, C_1(i,j) = C_2(i,j) \\ 1, \ otherwise \end{cases} \tag{25}$$

For NPCR and UACI analysis, a pixel was chosen at random and the least significant bit of its binary representation was toggled to form the modified image. Using the ciphered version of the plain image (C_1) and the ciphered version of the modified image (C_2), values for NPCR and UACI were computed and tabulated in Table 7. The results shown in Table 7 indicates that the algorithm can resist differential attacks as the NPCR and UACI values are close to the theoretical values of 99.61% and 33.46% respectively. The average NPCR of the proposed scheme is better than the compared algorithms [13, 45]. From Table 7, we can infer that the average UACI value of proposed scheme is better than the other two schemes. Table 7 shows that the encryption scheme proposed in [45] has poor NPCR and UACI values as it does not employ diffusion operation.

Table 7 NPCR and UACI analysis

Test Image	NPCR %			UACI %		
	Proposed	[13]	[45]	Proposed	[13]	[45]
Baboon	99.8322	99.6735	0.3876	34.1922	33.6889	0.1201
Boat	99.3500	99.6674	0.3906	36.5397	33.4745	0.118
Lake	99.8718	99.6735	0.3906	38.9861	33.8226	0.1205
Man	99.6704	99.5972	0.3876	30.1514	33.3759	0.1307
Peppers	99.8840	99.5911	0.3906	35.3155	33.3975	0.1469
Average	99.7217	99.6405	0.3894	35.0370	33.5519	0.1272

4.6 Keyspace and key sensitivity analysis

To resist brute-force attack an encryption scheme must have a large key space. In the proposed scheme the key generation is dependent on the input image. The 256-bit hash code generated by implementing the SHA-256 algorithm on the input image. This hash code together with the keys Z'_0, μ' are shared between the sender and receiver using a secure channel. According to the IEEE floating point standard the data precision for the double values is 10^{-15}. Therefore, the keyspace of the proposed scheme is given by $2^{256} \times 10^{15} \times 10^{15}$ which is approximately equal to 2^{356}.The comparison between the key space of the proposed scheme and the schemes in [13] and [45] is shown in Table 8. The key space provided by the proposed scheme is very large when compared with the other algorithms, which indicates a very high security.

For an efficient encryption scheme the security key should be highly sensitive. A small change in the security key should result in a totally different decrypted image. The cipher is decrypted using the same key as used in encryption and the reconstructed image is shown in Fig. 9(b). A small value $\Delta=10^{-15}$ is added to the correct keys (Z'_0, μ') and the cipher image is decrypted. The reconstructed images with incorrect keys are shown in Fig. 9, which shows that the proposed scheme is highly sensitive to even a small change in the key.

4.7 Chosen-plaintext attack analysis

In chosen-plaintext attack the adversary has access to the encryption oracle and tries to gain information by encrypting arbitrary plaintext of his choice. In a CS based cryptosystem, the cipher text is vulnerable to chosen plaintext attack, as the measurement matrix (i.e. the secret key) can be retrieved by cryptanalysis. By choosing an identity matrix as plaintext the measurement matrix can be deduced as the compressive sensing measurements are linear. The chosen-plaintext attack can be thwarted by diffusing the linearity of the CS measurements. In the proposed scheme a permutation process is used to break the linearity. If a single permutation vector is used for multiple images, the encryption algorithm can be easily broken. By employing a plaintext dependent diffusion process chosen-plaintext attack can be prevented. In the proposed scheme a chaos based permutation process is utilized. A SHA-256 hash code of the plain image is generated which is used to generate the parameters of the chaotic system. The proposed chaotic system is then used to generate a chaotic sequence which is used to scramble the measurements. Block scrambling using Arnold transform followed by proposed chaotic map based row and column scrambling greatly increase the resistance to chosen-plaintext attack. Also, the proposed cryptosystem adopts xor based substitution function that chosen-plaintext attack the adversary has access to the encryption oracle and tries to gain information by encrypting arbitrary plaintext of his choice.

Table 8 Key space analysis

Proposed	[13]	[45]
2^{356}	2^{199}	2^{112}

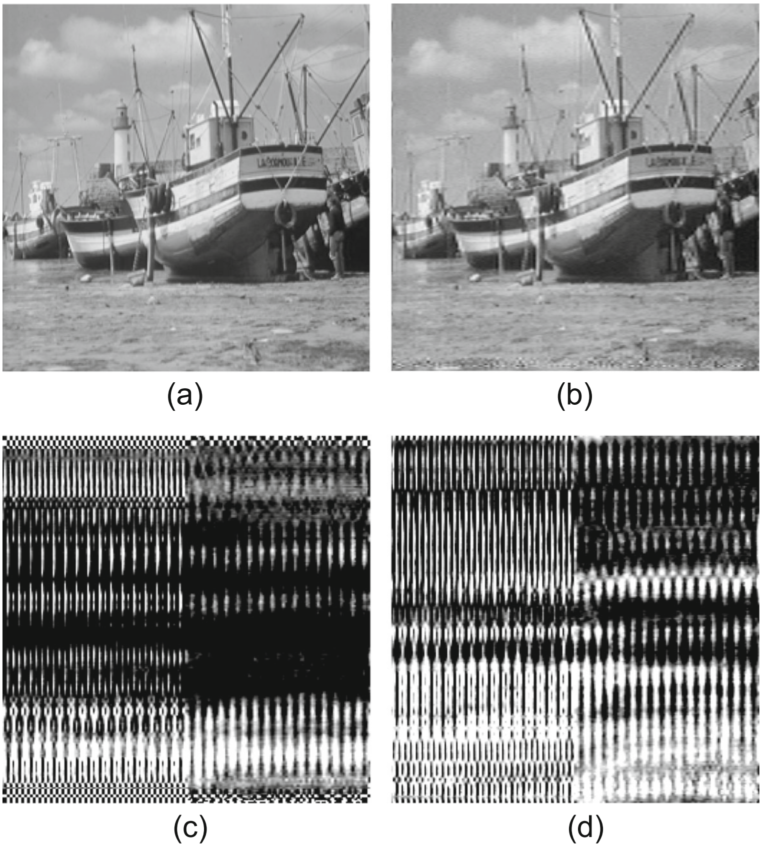

Fig. 9 (a) Original Image (b) Reconstructed Image with correct keys (c) Reconstructed Image with incorrect key Z_0' (d) Reconstructed Image with incorrect key μ'

4.8 Maximum deviation analysis

The deviations in the pixel values between the plain image and cipher image is a measure of the quality of the encryption algorithm. Higher the deviation greater the strength of the encryption algorithm. The maximum deviation MD is computed as follows:

$$MD = \frac{A0 + AN{-}1}{2} + \sum_{i=1}^{L-2} Ai \tag{26}$$

where L is the number of gray levels and A_i is the amplitude difference between the histogram of the plain image and the cipher image at index i. The cipher image is highly deviated from the plain image if the value of M_D is higher. The Table 9 shows the maximum deviation of the proposed scheme in comparison to that of [13] and [45]. The average maximum deviation value is slightly less when compared with [13] and greater when compared with [45]. The average maximum deviation value of the proposed scheme is high enough to conceal statistical information from an intruder.

Table 9 Maximum deviation analysis

Test Image	Maximum Deviation		
	Propose	[13]	[45]
Baboon	32,890	32,901	32,821
Boat	32,888	32,881	32,840
Lake	32,893	32,915	32,827
Man	32,363	32,375	32,300
Peppers	32,901	32,889	32,836
Average	32,787	32,792	32,725

4.9 Contrast analysis

Contrast of an image is defined as the difference between the maximum and the minimum pixel intensity in an image. The encrypted image has high contrast levels because of the randomness of the pixel intensity. Hence higher the contrast greater the encryption strength. The contrast is mathematically computed as:

$$Contrast = \sum_{i,j} |i{-}j|^2 G(i,j) \tag{27}$$

where $G(i, j)$ is the number of gray-level co-occurrence matrices. The contrast of the encrypted image obtained using the proposed scheme is high, when compared to other techniques. It indicates that the high randomness of the pixels in the cipher image. From Table 10, we can observe that the average contrast value of the proposed scheme is comparable to other schemes.

5 Conclusion

In this paper, a compression-encryption algorithm based on parallel compressive sensing and chaotic measurement matrix is proposed. The proposed chaotic map is used to construct an incoherence rotated measurement matrix. The experimental results demonstrated the effectiveness of the measurement matrix in reconstructing the image when compared with other measurement matrices. The increase in average PSNR is about 6–8 dB, when compared with other schemes. For enhancing security against chosen plain text attack, an input dependent key scheduling is employed. The keyspace of the proposed scheme is large enough to resist brute-force attacks. The histogram, entropy and correlation analysis shows that the proposed scheme

Table 10 Contrast analysis

Test Image	Contrast		
	Proposed	[13]	[45]
Baboon	10.4816	10.4104	10.4146
Boat	10.5927	10.5353	10.4816
Lake	10.5179	10.5372	10.5793
Man	10.4214	10.4211	10.4291
Peppers	10.3762	10.2599	10.5199
Average	10.4780	10.4328	10.4849

can thwart statistical attacks. Simulation results verify that the proposed scheme is efficient as well as secure.

References

1. Banderia AS, Dobriban E, Mixon DG, Sawin WF (2012) Certifying the Restricted Isometry Property is Hard. IEEE Trans Inf Theory 59:3448–3450
2. Baraniuk R (2007) Compressive Sensing (lecture notes). IEEE Signal Process Mag 24(4):118–121
3. Belazi AAA, El-Latif BS (2016) A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process 128:155–170
4. Cambareri V, Mangia M, Pareschi F, Rovatti R, Setti G (2015) On known-plaintext attacks to a compressed sensing-based encryption: a quantitative analysis. IEEE Trans Inf Forensics Security 10(10):2182–2195
5. Cambareri V, Mangia M, Pareschi F, Rovatti R, Setti G (2015) Low-complexity multiclass encryption by compressed sensing. IEEE Trans Signal Process 63(9):2183–2195
6. Candes EJ (2008) The restricted isometry property and its implications for compressed sensing. C R Math 346(9–10):589–592
7. Cui J, Liu Y, Xu Y, Zhao H, Zha H (2013) Tracking generic human motion via fusion of low-and high-dimensional approaches. IEEE Trans Syst Man Cybern 43(4):996–1002
8. Deepak M, Ashwin V, Amutha R (2014) A new Multistage multiple image encryption using a combination of Chaotic Block Cipher and Iterative Fractional Fourier Transform. In First International Conference on Networks & Soft Computing (ICNSC2014):360–364
9. Donoho DL (2006) Compressed Sensing. IEEE Trans Inf Theory 52:1289–1306
10. Fay R (2016) Introducing the counter mode of operation to Compressed Sensing based encryption. Inform Process Lett 16(4):279–283
11. Gordon WB (1996) Period three trajectories of the logistic map. Math Mag 69(2):118–120
12. Hanis S, Amutha R (2017) Double image compression and encryption scheme using logistic mapped convolution and cellular automata. Multimed Tools Appl :1-16
13. Hu G, Xiao D, Wang Y, Xiang T (2017) An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications. J Vis Commun Image R 44:116–127
14. Hua Z, Zhou Y, Pun CM, Chen CP (2015) 2D Sine Logistic modulation map for image encryption. Inform Sciences 297:80–94
15. Huang R, Sakurai K (2011) A robust and compression-combined digital image encryption method based on compressive sensing. In Proc Intelligent Information Hiding and Multimedia Signal Processing IIH-MSP, 105–108
16. Huang R, Rhee KH, Uchida S (2014) A parallel image encryption method based on compressive sensing. Multimed Tools Appl 72(1):71–93
17. Jiang J, He X, Gao M, Wang X, Wu X (2015) Human action recognition via compressive-sensing-based dimensionality reduction. Optik-Int J Light Electron Optics 126(9):882–887
18. Liao X, Shu C (2015) Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. J Vis Commun Image R 28:21–27
19. Liao X, Li K, Yin J (2017) Separable data hiding in encrypted image based on compressive sensing and discrete Fourier transform. Multimed Tools Appl 76(20):20739–20753
20. Liao X, Qin Z, Ding L (2017) Data embedding in digital images using critical functions. Signal Proces-Image 58:146–156
21. Liu E, Temlyakov VN (2012) The orthogonal super greedy algorithm and application in compressed sensing. IEEE Trans Inf Theory 58:2040–2047
22. Liu Y, Zhang X, Cui J, Wu C, Aghajan H, Zha H (2010) Visual analysis of child-adult interactive behaviors in video sequences. In Proc of IEEE Int Conf Virtual Systems and Multimedia (VSMM) :26–33
23. Liu Y, Cui J, Zhao H, Zha H (2012) Fusion of low-and high-dimensional approaches by trackers sampling for generic human motion tracking. In Proc of IEEE Int Conf Patt Recog (ICPR) :898–901
24. Liu Y, Nie L, Han L, Zhang L, Rosenblum DS (2015) Action2Activity: Recognizing Complex Activities from Sensor Data. In Proc of Int Joint Conf Artif (IJCAI) :1617–1623
25. Liu Y, Zhang L, Nie L, Yan Y, Rosenblum DS (2016) Fortune Teller: Predicting Your Career Path. In Proc of AAAI :201-207
26. Liu L, Cheng L, Liu Y, Jia Y, Rosenblum DS (2016) Recognizing Complex Activities by a Probabilistic Interval-Based Model. In Proc of AAAI 30:1266–1272
27. Liu Y, Zheng Y, Liang Y, Liu S, Rosenblum DS (2016) Urban water quality prediction based on multi-task multi-view learning. In Proc of Int Joint Conf Artif (IJCAI) :2576–2582

28. Liu Y, Nie L, Liu L, Rosenblum DS (2016) From action to activity: Sensor-based activity recognition. Neurocomputing 12(181):108–115
29. Niyat AY, Moattar MH, Torshiz MN (2017) Color image encryption based on hybrid hyper-chaotic system and cellular automata. Opt Laser Eng 90:225–237
30. Orsdemir A, Altun HO, Sharma G, Bocko MF (2008) On the security and robustness of encryption via compressed sensing. In IEEE Milit Commun C (MILCOM 2008) San Diego, CA :1-7
31. Phamila AVY, Amutha R (2013) Low complexity energy efficient very low bit-rate image compression scheme for wireless sensor network. Inform Process Lett 113(18):672–676
32. Phamila AVY, Amutha R (2015) Energy-efficient low bit rate image compression in wavelet domain for wireless image sensor networks. Electron Lett 51(11):824–826
33. Preoţiuc-Pietro D, Liu Y, Hopkins D, Ungar L (2017) Beyond binary labels: political ideology prediction of Twitter users. In Proc of the 55th Annual Meeting of the Association for. Computational Linguistics 1:729–740
34. Rachlin Y, Baron D (2008) The secrecy of compressed sensing measurements. In Proc 46th Annual Allerton Conf. Comm. Control Comput :813-817
35. Tong XJ, Wang Z, Zhang M, Liu Y (2013) A new algorithm of the combination of image compression and encryption technology based on cross chaotic map. Nonlinear Dynam 72(1–2):229–241
36. Wu X, Wang D, Kurths J, Kan H (2016) A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. Inform Sciences 349:137–153
37. Yao S, Wang T, Shen W, Shaoming P, Chong Y (2017) Research of incoherence rotated chaotic measurement matrix in compressed sensing. Multimed Tools Appl 76(17):17699–17717
38. Yu L, Barbot JP, Zheng G, Sun H (2010) Compressive sensing with chaotic sequence. IEEE Signal Process Lett 17(8):731–734
39. Yuan X, Wang X, Wang C, Weng J, Ren K (2016) Enabling secure and fast indexing for privacy-assured healthcare monitoring via compressive sensing. IEEE Trans Multimedia 18(10):2002–2014
40. Yuen CH, Wong KW (2011) A chaos-based joint image compression and encryption scheme using DCT and SHA-1. Appl Soft Comput 11(8):5092–5098
41. Zhang LY, Wong KW, Zhang Y, Zhou J (2016) Bi-level protected compressive sampling. IEEE Trans Multimedia 18(9):1720–1732
42. Zhang W, Yu H, Zhao YL, Zhu ZL (2016) Image encryption based on three-dimensional bit matrix permutation. Signal Process 118:36–50
43. Zhang Y, Zhang LY, Zhou J, Liu L, Chen F, He X (2016) A review of compressive sensing in information security field. IEEE Access 4:2507–2519
44. Zhou NR, Zhang AD, Zheng F, Gong LH (2014) Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. Opt Laser Technol 62:152–160
45. Zhou N, Zhang A, Wu J, Pei D, Yang Y (2014) Novel hybrid image compression–encryption algorithm based on compressive sensing. Optik-International Journal for Light and Electron Optics 125(18):5075–5080
46. Zhou Y, Bao L, Chen CP (2014) A new 1D chaotic system for image encryption. Signal Process 97:172–182
47. Zhou Y, Hua Z, Pun CM, Chen CP (2015) Cascade chaotic system with applications. IEEE Trans Cybern 45(9):2001–2012
48. Zhu H, Zhao C, Zhang X (2013) A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem. Signal Process-Image 28(6):670–680

Ponuma R received her B.E. degree in Electronics and Communication Engineering from Manonmaniam Sundaranar University, India, in 2002 and M.E degree in Communication Systems from Anna University, Chennai, India, in 2004. Her current research interests include Image processing and Cryptography. She is a Life member of Indian Society for Technical Education (ISTE).

Amutha R graduated from Thiagarajar college of Engineering, India, in the year 1987. She received her M.E. degree from PSG college of Technology, Coimbatore, India and her Ph.D. degree from Anna University in 2006. She has got 29 years of teaching and 15 years of research experience. She is a Life member of Indian Society for Technical Education (ISTE) and Institution of electronics and Telecommunication Engineers (IETE). Her research area includes Wireless communication network and Image processing.