J Opt (January–March 2014) 43(1):1–17
DOI 10.1007/s12596-013-0147-8

RESEARCH ARTICLE

A novel approach for secure compressive sensing of images using multiple chaotic maps

Sudhish N. George · Deepthi P. Pattathil

Received: 27 May 2013 / Accepted: 23 August 2013 / Published online: 15 September 2013

Abstract In this paper, a novel approach for secure compressive sensing of images based on multiple one dimensional chaotic maps is proposed. The basic idea is to perform the random selection of a combination of two one dimensional chaotic maps to generate a random stream. One or more values from the random stream are used to generate each normal value in the random measurement matrix for compressive sensing. In the proposed approach, eight different one dimensional chaotic maps are used. For one measurement matrix generation, two of them are randomly selected based on a secret key. The number of iterations and the initial states of the chaotic maps are also decided by external secret keys. The chaotic output of iterations of the two selected chaotic maps are XORed to generate a new chaotic value so that the measurement matrix so generated can withstand known plaintext attack. The block-based compressive sensing (BCS) of images is adopted to validate the proposed system. Further enhancement in the security of the proposed system for BCS of images can be obtained by using different measurement matrices for different blocks of images. An algorithm for generating multiple measurement matrices is also presented in this work. It is experimentally proved that the proposed encryption system can maintain the robustness to noise of the compressive sensing system. The proposed robust encryption system is subjected to several forms of attacks and is proved to be resistant against all.

Keywords Compressive sensing · Chaotic maps · Encryption · Data compression

S. N. George (✉) · D. P. Pattathil
Department of Electronics & Communication Engineering, National Institute of Technology, Calicut 673601, India
e-mail: sudhish@nitc.ac.in

D. P. Pattathil
e-mail: deepthi@nitc.ac.in

Introduction

The increasing demand in the multimedia data necessitates the use of efficient compression techniques for maintaining the huge traffic in the limited bandwidth environment. The newly developed compressive sensing system is a method in this direction, where the sampling rate is less than the Nyquist rate so that the achievable compression performance is better than the standard coding techniques. Compressive sensing (CS) is a mathematical framework meant for permitting signals to be sampled at sub-Nyquist rates (sub-rates) under certain conditions, by linear projection into a lower dimension than the original signal [11].

The basic theory of CS is investigated in [2, 6, 11, 12, 34]. Compressive sensing relies in the sparseness of the signal and gathers linear measurement $y = \phi x$ of a sparse signal x, where size of y is a small fraction of samples needed for Nyquist sampling. The random measurement ensemble ϕ follows uniform uncertainty principle (UUP) [5] and gives equal importance to each measurement. This helps to provide unified decoder for compressive sensed coding schemes [8]. The receiver obtains the linear measurements y and reconstructs the signal by solving it as an optimization problem.

Over the last years, a number of image/video coding schemes based on compressive sensing were proposed. In [21], Han et al. proposed an image representation problem for visual sensor networks. Multi-scale wavelet based CS scheme was proposed by Deng et al. [7, 8]. In [40], different compressive sensing based surveillance video coding systems were proposed and compared by Venkatraman et al. Information theoretic approach for CS based image coding is presented in [20]. A compressive sensing based robust image transmission scheme for wireless channels was proposed by Gao et al. in [18]. The block-based CS (BCS) for 2D images was initially proposed by Gan [17] to reduce the large computational complexity and storage requirement of measurement matrices for large sized images. Smoothed projected Landweber (SPL) iterations were incorporated in the block-based compressive sensing reconstruction to enhance the reconstruction quality. The further enhancement in quality of the reconstructed images was obtained by using directional transforms (dual-tree DWT and contourlet transforms) [28] or multiscale variant of BCS-SPL [16].

To protect the private data from the unauthorized usage, perfect security is a mandatory requirement in the compressive sensing framework. A robust encryption system based on cryptographic key based selection of random measurement matrix was proposed by Orsdemir et al. [31]. Rachlin et al. showed that compressed sensing based encryption does not achieve Shannon's definition of perfect secrecy, but can provide a computational guarantee of secrecy [33]. In another approach, Kumar et al. proposed an encryption system by performing the compressive measurements over an encrypted image [25]. A compression-combined digital image encryption method which is robust against consecutive packet loss and malicious shear attack was proposed by Huang et al., where one dimensional logistic mapping is used to generate chaotic sequences, which is regarded as the parameters of block Arnold transformation and the pseudorandom sequence for XOR operation [23]. In [27], Lu et al. proposed an image information encryption method based on compressive sensing and double random-phase encoding. Soman et al., proposed an encryption system by scrambling the compressed measurements using Arnold transform [37]. These approaches are either vulnerable to some forms of attack or offer high level of complexity. Moreover, most of the above mentioned approaches do not maintain the robustness to noise of the compressive sensing system.

The main motivation behind the proposed work is to design a less complicated encryption system with high level of security such that it maintains the robustness of the CS system. Multiple one dimensional chaotic maps based CS encryption technique can provide a highly secure system with low complexity. In the proposed approach, pairs of chaotic maps are considered and the pairs are randomly selected to generate random values. The chaotic output values of the selected pair are XORed to get new random value so that the newly generated random stream can withstand known plaintext attack. One or more uniform values from this random stream are used to generate each normal value in the random measurement matrix for performing the secure compressive sensing operation. It is proposed to use separate measurement matrices for different blocks of images in BCS to increase security of the proposed encryption system.

The remaining sections of this paper are organized as follows. Section "Basic principle of compressive sensing" deals with the basic principles of compressive sensing. Section "Proposed system: secure compressive sensing based on multiple chaotic maps" proposes a multiple chaotic map based encryption system for compressive sensing of images. The experimental analysis of the proposed system is given in section "Analysis

of the proposed encryption system". The paper concludes in section "Conclusion".

Basic principle of compressive sensing

This section briefly explains the theory behind the compressive sensing, the different imaging techniques via compressive sensing and the different reconstruction techniques in BCS of images.

Compressive sensing

The compressed sensing framework is used to reduce the data acquisition and computational load at sensors, at the cost of increased computation at the intended receiver [11, 12]. Thus, the basic idea is to recover signal $\mathbf{x}$ with length N from M samples such that $M \ll N$ with subsampling rate or subrate, being $S = M/N$. Even if, the number of unknowns $\mathbf{x} \in R^N$ is larger than number of observations $\mathbf{y} \in R^M$, it is possible to reconstruct $\mathbf{x}$ from $\mathbf{y}$, if $\mathbf{x}$ is sufficiently sparse in some domain [11].

A real-valued, finite length, one dimensional signal $\mathbf{x}$, represented as $N \times 1$ column vector in R^N, can be represented in terms of an orthonormal basis $\{\psi_i\}_{i=1}^N$ as follows.

$$\mathbf{x} = \sum_{i=1}^{N} s_i \psi_i = \psi \mathbf{s} \tag{1}$$

where, $\mathbf{x}$ and $\mathbf{s}$ are the same signal representations in time/space domain and ψ domain respectively. $\mathbf{s}$ is an $N \times 1$ column vector of weighting coefficients, $s_i = \langle \mathbf{x}, \psi_i \rangle$. But $\mathbf{x}$ has sparsity such that $\mathbf{x}$ can be represented as a linear combination of only K basis vectors [2]. In compressive sensing, instead of direct sampling $\mathbf{x}$, a lower number of CS measurements are taken. Let the measurement matrix be $\phi = \{\phi_i\}_{i=1}^N$ of order $M \times N$ with $M \ll N$. Then, the M linear samples $\mathbf{y}$ can be represented as,

$$\mathbf{y} = \{y_i\}_{i=1}^M = \phi \mathbf{x} = \{\langle \mathbf{x}, \phi_i \rangle\}_{i=1}^M \tag{2}$$

Even if, $\mathbf{y}$ is quantized as finite precision samples and added with some amount of noise in real-world, the signal can be reconstructed, maintaining the robustness to noise by solving it as a convex optimization problem under the condition that the measurement matrix ϕ satisfies uniform uncertainty principle (UUP) [5, 8].

$$\min \|\psi^T \tilde{x}\|_{l_1} \qquad s.t. \qquad \|\phi \psi^T \tilde{x} - y\|_{l_2} \leq \epsilon \tag{3}$$

for some tolerance $\epsilon > 0$. For $\Theta = \phi \psi^T$ to be stable solution for this optimization problem, Θ should satisfy the restricted isometry property (RIP) [3]. The related condition for RIP is incoherence, which requires that the rows of ϕ cannot sparsely represent the columns of ψ [2]. Both the properties, RIP and incoherence can be achieved by selecting ϕ as a random matrix. A random matrix whose elements ϕ_{ij} are iid random variables from a Gaussian probability density function with mean zero and variance $\frac{1}{N}$ is able to satisfy these requirements [11]. Multiplying the sparse signal with random iid Gaussian matrix gives equal importance to each CS measurements. This feature makes the CS technique to have inherent error controlling capability [8]. The basic constrained optimization given in (3) is closely related to the unconstrained Lagrangian formulation, known as basic-pursuit denoising (BPDN) given by,

$$\min \|\psi^T \tilde{x}\|_{l_1} + \lambda \|\phi \psi^T \tilde{x} - y\|_{l_2} \tag{4}$$

where, the l_1 driven sparsity against the l_2 based measure of distortion is balanced by the Lagrangian multiplier λ [15]. The following subsection discusses the different imaging techniques via compressive sensing.

Imaging via compressive sensing

A number of architectures for the CS acquisition of images were proposed in the literature. Rice university proposed a single-pixel camera for CS based acquisition of images [12]. Neifeld et al. proposed some optical architectures for compressive imaging [30]. In another approach, Xiao et al. proposed a CMOS low data rate imaging approach by implementing compressed sensing [42]. An overview of different CS acquisition architectures are described in [13]. The single-pixel camera from Rice university for CS acquisition is given in Fig. 1.

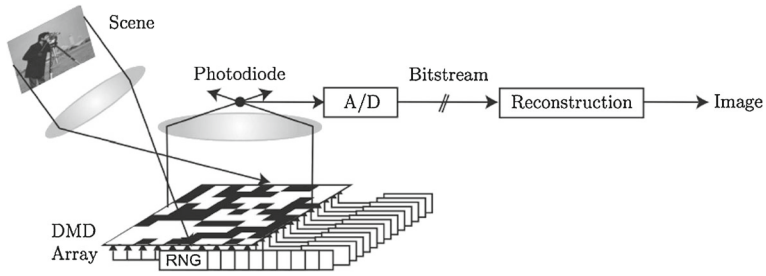

Fig. 1 Block diagram of single-pixel pixel camera system for CS acquisition [38]

The CS based implementation of images is classified into straightforward approach and block-based approach. In straightforward approach, the 2D image is converted into a 1D vector and the compressive sensing procedure is performed on this 1D vector. Since there is a linear increase in the size of the measurement matrix with the increase in size of the image, the memory requirement to store the ϕ matrix and the computational complexity are very high for large images in the straightforward approach. In block-based compressive sensing (BCS) method, the image is divided into non-overlapping blocks and the compressive sensing operation is performed on the corresponding 1D vector of each block, where primary importance is given to the memory efficient measurement operator so that the drawbacks of straightforward approach for large sized images can be reduced.

Block-based compressive sensing for images

To alleviate the large memory requirement Gan proposed a method to divide the image into smaller blocks and to perform CS on smaller blocks independently. This method is known as block-based compressive sensing (BCS) [17]. In BCS scheme, the image is divided into blocks of size $B \times B$ with respect to the size requirement of measurement matrix. Let $\mathbf{x}_j$ be the 1D vector corresponding the j^{th} block of image $\mathbf{X}$. Then, the BCS output is given as,

$$\mathbf{y}_j = \phi_B \mathbf{x}_j \tag{5}$$

Let the order of ϕ_B be $M_B \times B^2$, where $M_B = \lfloor \frac{M}{N} B^2 \rfloor$. Then, the subrate of the image is given as, $S = M_B/B^2$. The whole image measurement matrix can be represented as a block diagonal matrix given as follows,

$$\phi = \begin{bmatrix} \phi_B & 0 & \dots & 0 \\ 0 & \phi_B & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \phi_B \end{bmatrix}$$

If block-by-block reconstruction is directly performed, it will create blocking artifacts on the reconstructed image. To improve the quality of the reconstructed image, several methods were proposed time to time. The following subsections deal with the BCS reconstruction methods to improve the reconstructed image quality.

BCS-TV based reconstruction

The total variation (TV) based CS reconstruction replaces the sparsity in the transform domain with the sparsity in the discretized gradient domain. It can provide smoothness in the reconstructed image [26]. This is due to the fact that it has the ability to suppress the high frequency artifacts produced by the direct block-by-block reconstruction of image. The optimization problem is reformulated as follows,

$$\min \|\mathbf{X}\|_{TV} + \lambda \|\mathbf{y} - \phi \mathbf{x}\|_{l_2} \tag{6}$$

The total variation of the image is given as,

$$\|\mathbf{X}\|_{TV} = \sum_{i,j} \sqrt{(x_{i+1,j} - x_{i,j})^2 + (x_{i,j+1} - x_{i,j})^2} \tag{7}$$

where, $x_{i,j}$ represents the pixel value in the location (i, j).

The above minimization problem can be solved by using the second order cone programming, which is solvable by interior-point algorithms [4, 26]. In this method, the first step is to find

an initial feasible solution from the received measurement vector **y** and the generated ϕ matrix. The initial feasible solution represents a noisy version of the original image. Total variation of feasible solution is calculated from (6) and it is minimized through log-barrier iteration. At each log-barrier iteration, Newton's method proceeds with the approximate solution at the last iteration as the initial guess. Applying Newton's method at each iteration is still time consuming in a large-scale problem.

BCS with smoothed projected Landweber (BCS-SPL) reconstruction

The BCS-SPL is a iterative projection and thresholding based reconstruction method [22]. It starts from an initial approximation $\breve{x}$. The approximation in $(i+1)^{th}$ iteration is a specific instance of specific projected Landweber (PL) algorithm and is given as [28],

$$\breve{\breve{x}}^{(i)} = \breve{x}^{(i)} + \frac{1}{\gamma}\psi\phi^T(y - \phi\psi^{-1}\breve{x}^{(i)}), \tag{8}$$

$$\breve{x}^{(i+1)} = \begin{cases} \breve{\breve{x}}^{(i)}, & |\breve{\breve{x}}^{(i)}| \geq \tau^{(i)} \\ 0, & \text{else} \end{cases} \tag{9}$$

where, γ is the scaling factor and its value is chosen by finding the largest eigenvalue of $\phi^T\phi$ and $\tau^{(i)}$ is the threshold value chosen appropriately at each iteration.

To improve the quality of reconstructed image Wiener filtering is incorporated into the basic PL framework [17] to provide smoothness in the reconstruction. The approximation of the image in the $(i+1)^{th}$ iteration is given as follows [15],

$$x^{(i+1)} = \text{SPL}(x^{(i)}, y, \phi_B, \psi, \lambda)$$

$$\hat{x}^{(i)} = \text{Wiener}(x^{(i)})$$

for each block j

$$\hat{\hat{x}}_j^{(i)} = \hat{x}_j^{(i)} + \phi_B^T\left(y - \phi_B\hat{x}_j^{(i)}\right)$$

$$\breve{\breve{x}}^{(i)} = \psi\hat{\hat{x}}^{(i)}$$

$$\breve{x}^{(i)} = \text{Threshold}(\breve{\breve{x}}^{(i)}, \lambda)$$

$$\bar{x}^{(i)} = \psi^{-1}\breve{x}^{(i)}$$

for each block j

$$x_j^{(i+1)} = \bar{x}_j^{(i)} + \phi_B^T\left(y - \phi_B\bar{x}_j^{(i)}\right)$$

$$D^{(i+1)} = \frac{1}{\sqrt{N}}\|x^{(i+1)} - \hat{\hat{x}}_j^{(i)}\|_2$$

until $|D^{(i+1)} - D^{(i)}| < 10^{-4}$

$$x = x^{(i+1)}$$

where, Wiener(.) is pixelwise adaptive Wiener filtering operation and Threshold(.) is a thresholding operation. The initial value $x^{(0)}$ is given as,

$$x^{(0)} = \phi^T y$$

For BCS-SPL-DCT, ψ is selected as discrete cosine transform (DCT) and hard thresholding is used to select the value of τ. The universal threshold is the suitable candidate for such an application [10].

$$\tau^{(i)} = \lambda\sigma^{(i)}\sqrt{2logK} \tag{10}$$

where, K is the number of transform coefficients and λ is a constant to manage the convergence. $\sigma^{(i)}$ can be estimated using the median estimator, which is given as,

$$\sigma^{(i)} = \frac{\text{median}|\breve{\breve{x}}^{(i)}|}{0.6745} \tag{11}$$

Since the hard thresholding is based on the fact that the transform coefficients are independent, the hard thresholding is not a suitable choice in DWT based BCS-SPL reconstruction techniques. Bivariate shrinkage function [36] gives superior performance than hard thresholding in DWT based BCS-SPL reconstruction methods. Thus, the threshold function in BCS-SPL-DWT is the MAP estimator and is given as,

$$\text{Threshold}(\xi, \lambda) = \frac{\left(\sqrt{\xi^2 + \xi_p^2} - \lambda\frac{\sqrt{3\sigma^{(i)}}}{\sigma_\xi}\right)_+}{\sqrt{\xi^2 + \xi_p^2}}.\xi \tag{12}$$

where the function,

$$(g)_+ = \begin{cases} 0, & g < 0 \\ g, & \text{else} \end{cases}$$

ξ and ξ_p are the specific transform coefficient and its parent coefficient respectively. $\sigma^{(i)}$ is

the median estimator applied to only first scale transform coefficients and λ is the convergence control factor. σ_ξ^2 is the marginal variance of coefficient ξ estimated in a local 3×3 neighbourhood surrounding of ξ [28]. Since the directional transforms, contourlet transform (CT) [9] and dual-tree discrete wavelet transform (DDWT) [24] show good directional sensitivity and shift invariance properties than DWT, Fowler et al. proposed that the BCS-SPL based on directional transforms (BCS-SPL-DDWT and BCS-SPL-CT) give better reconstruction quality than BCS-SPL-DCT and BCS-SPL-DWT [28].

Multiscale block-based compressive sampling

In [16], Fowler et al. proposed a multiscale variant of block based compressive sensing smoothed projected Landweber reconstruction (MS-BCS-SPL). In this approach, block-based compressive sampling is performed in each subband of wavelet transform of an image. The compressive sensed image in the MS-BCS-SPL based approach is given as,

$$\mathbf{y} = \phi' \Omega \mathbf{x} \tag{13}$$

where, Ω represents the multiscale transform and ϕ' is the multiscale block based measurement process. For L level of decomposition, ϕ' consists of L different block based sampling operators. Let the DWT of the image be,

$$\tilde{\mathbf{x}} = \Omega \mathbf{x} \tag{14}$$

Then, each subband s at a level l is divided into $B_l \times B_l$ blocks and sampled with corresponding ϕ_l. Then, for $1 \leq l \leq L$

$$\mathbf{y}_{l,s,j} = \phi_l \tilde{\mathbf{x}}_{l,s,j} \tag{15}$$

where, $\tilde{\mathbf{x}}_{l,s,j}$ represents the vector corresponding to the jth block of subband s at level l, with $s \in \{H, V, D\}$.

Since different levels of wavelet decomposition have different significance in the reconstruction, Fowler et al. proposed to use different subrate S_l at each level l, where the subrate for DWT baseband is taken as $S_0 = 1$. The subrate for lth level is given as,

$$S_l = W_l S' \tag{16}$$

under the condition that the overall subrate becomes,

$$S = \frac{1}{4^L} S_0 + \sum_{l=1}^{L} \frac{3}{4^{L-l+1}} W_l S' \tag{17}$$

For a given subrate S and level weights W_l, it is possible to find out the value of S' to obtain the level subrate values S_l. This procedure may produce $S_l > 1$. If $S_1 > 1$, set $S_1 = 1$ and modify the (19) as,

$$S = \frac{1}{4^L} S_0 + \frac{3}{4^L} S_1 + \sum_{l=2}^{L} \frac{3}{4^{L-l+1}} W_l S' \tag{18}$$

and repeat this procedure to keep all $S_l \leq 1$. The level weights can be calculated as follows,

$$W_l = 16^{L-l+1} \tag{19}$$

In MS-BCS-SPL reconstruction, Landweber step on each block of each subband in each decomposition level use different ϕ_l for current level l [15, 16]. Among all BCS approaches, the BCS-TV has the highest computational time than BCS-SPL and MS-BCS approaches.

The following section proposes a robust encryption system through compressive sensing, based on multiple one dimensional chaotic maps for generating the measurement matrix used in the compressive sensing paradigm.

Proposed system: secure compressive sensing based on multiple chaotic maps

The chaotic maps have great importance in cryptography due to its sensitive dependence to the initial condition and system parameter, nonperiodicity, ergodicity and pseudorandom property [43]. Over the last years, a large number of discrete chaotic maps were proposed for cryptographic applications. In this paper, eight well known one dimensional discrete chaotic maps are chosen to develop an encryption system for compressive sensing applications. The selected one dimensional chaotic maps are logistic map, sine map, cubic map, tent map, Gao's new chaotic map (GNCA), Singer map, piecewise linear chaotic map (PLCM) and Mehrab map. The selected

chaotic maps, their mathematical representations and the system parameter values are listed in Table 1. A number is assigned to each chaotic map starting from '0' to '7', mentioned as chaotic index number (CIN) in the first column of Table 1. In all chaotic maps, the initial value and/or system parameter value are kept as secret to attain the secrecy.

The one dimensional logistic map shows the exact chaotic behaviour only in the region $\mu \in [3.6, 4)$ [19]. Even though, the logistic map provides high efficiency with simple design, it has smaller key space and lower security. Hence, Gao et al. proposed a new chaotic algorithm named as NCA [19]. It consists of two system parameters α and β. The typical parameter value of sine map is 0.99 [1]. The expressions for cubic map and tent map and the typical paremeter values are mentioned in [32]. In [39], it is mentioned that the the typical parameter values of Singer is in the interval (0.90, 1.08). The PLCM shows the chaotic behaviour on interval [0, 1) [41]. Mehrab map is a modified version of PLCM, which consists of two system parameters [14].

The main drawback with the chaotic maps is their vulnerability to known plaintext attack. To overcome this issue, in this paper, it is proposed to select any two chaotic maps from the chosen group of eight chaotic maps using a secret key. Combining the corresponding random values of these two chaotic maps will ensure that the security of the newly generated chaotic values is increased. The initial values of these two chaotic maps and the number of iterations are also determined by secret keys. The random array generated by the proposed approach is used as the random stream for generating the measurement matrix in the compressive sensing operation of images.

Secure measurement matrix generation

Four stages of encryption are proposed in this approach; one for chaotic maps selection, second for initial value of first chaotic map, third for initial value of second chaotic map and fourth for the number of iterations of the selected chaotic maps to get the required number of random values to form the random array. Four secret keys (32-bit each) are considered for this purpose. Thus, the total key size of the proposed measurement matrix generation is 128-bit. If we use hexadecimal representation for the key, total 32 characters are included in the key. Let *Key* be the external secret key to the user. Then, it can be represented as follows,

$$Key = Key_1 Key_2 Key_3 Key_4 \tag{20}$$

Table 1 Selected one dimensional chaotic maps, the chaotic index number(CIN), mathematical expressions and parameter values

Number (CIN)	Chaotic map	Equation	Parameter value
0	Logistic map	$x_{n+1} = \mu x_n(1 - x_n)$	$\mu = 3.99$
1	Sine map	$x_{n+1} = \mu sin(\pi x_n)$	$\mu = 0.99$
2	Cubic map	$x_{n+1} = \mu x_n(1 - x_n^2)$	$\mu = 2.59$
3	GNCA	$x_{n+1} = (1 - \beta^{-4}).\text{ctg}\left(\frac{\alpha}{1+\beta}\right).\left(1 + \frac{1}{\beta}\right)^{\beta}.\text{tg}(\alpha x_n).(1 - x_n)^{\beta}$	$\alpha = 1.1, \beta = 5$
4	Singer map	$x_{n+1} = \mu(7.86x_n - 23.31x_n^2 + 28.75x_n^3 - 13.30x_n^4)$	$\mu = 0.98$
5	Tent map	$x_{n+1} = \begin{cases} \mu x_n, & x > 0.5 \\ \mu(1 - x_n), & x \le 0.5 \end{cases}$	$\mu = 1.97$
6	PLCM	$x_{n+1} = F(x_n) = \begin{cases} x_n/\mu, & 0 \le x_n < \mu \\ (x_n - \mu)/(0.5 - \mu), & \mu \le x_n < 0.5 \\ F(1 - x_n), & 0.5 \le x_n < 1 \end{cases}$	$\mu = 0.35$
7	Mehrab map	$x_{n+1} = \begin{cases} \mu\sqrt{\frac{x_n}{a}}, & x_n < a \\ \mu\sqrt{\frac{(1-x_n)}{(1-a)}}, & x_n \ge a \end{cases}$	$\mu = 0.2, a = 0.5$

where, Key_1, Key_2, Key_3 and Key_4 represent the secret keys used for chaotic map pair selection, initial value of first chaotic map, initial value of second chaotic map and the number of iteration of the chaotic maps respectively. The key selection is based on the condition that Key_1, Key_2, Key_3 and Key_4 do not divide each other.

$$Key_i \nmid Key_j; \quad i \neq j \tag{21}$$

As mentioned earlier, a pairwise selection of chaotic maps are proposed in this paper. The eight chaotic maps are identified by chaotic index number (CIN) as mentioned in Table 1. By using CIN, the chaotic pair index number (CPIN) can be represented as follows,

$$\text{CPIN} = \{mn\}_{m,n=0,1,\ldots,7} \tag{22}$$

For example, if the random selection of CPIN using Key_1 is 12, the selected chaotic maps will be sine map and cubic map respectively. Similarly, if CPIN is 55, both the selected chaotic maps will be tent map itself. For eight chaotic maps, 64 pairwise combinations are possible. CPIN for each pair is coming as the octal number repesentation starting from '00' to '77'.

The random selection of pairwise chaotic maps based on Key_1 can be implemented by using the following relation after converting the hexadecimal number Key_1 into corresponding decimal representation Key_1^d.

$$CP_1 = Key_1^d \mod K \tag{23}$$

where, K represents the total number of pairwise combinations of chaotic maps ($K = 64$ in the proposed system). Converting CP_1 to corresponding octal representation gives the chaotic pair CP_1^c.

The initial values of the chaotic maps in the selected pair is found by using the following mathematical expressions by converting Key_2 and Key_3 into corresponding decimal representations, say Key_2^d and Key_3^d

$$x^1(0) = \left(\frac{Key_2^d}{Key_1^d}\right) - \left\lfloor \frac{Key_2^d}{Key_1^d} \right\rfloor \tag{24}$$

$$x^2(0) = \left(\frac{Key_3^d}{Key_1^d}\right) - \left\lfloor \frac{Key_3^d}{Key_1^d} \right\rfloor \tag{25}$$

where, $x^1(0)$ and $x^2(0)$ represent the initial values of the first and second chaotic maps in the selected pair respectively. The required number of iterations N^1 for the chaotic maps to form the random array of size N^1 is found by using Key_4 based on linear congruential generator (LCG) as follows,

$$N^1 = Z_1 = (aZ_0 + c) \mod L \tag{26}$$

In the proposed approach, it is chosen that $Z_0 = Key_4^d$, $a = 5$, $c = 1$ and $L = 128$, so that the maximum number iterations is 127.

$$N^1 = \left(5Key_4^d + 1\right) \mod 128 \tag{27}$$

Let the chaotic values produced by the first and second chosen chaotic maps and the generated chaotic values from these chaotic maps be $\mathbf{x}^1$, $\mathbf{x}^2$ and $\mathbf{x}_r$ respectively. Then,

$$\mathbf{x}^1 = \left(x^1(0), x^1(1), \ldots., x^1(N^1 - 1)\right)$$
$$\mathbf{x}^2 = \left(x^2(0), x^2(1), \ldots., x^2(N^1 - 1)\right)$$
$$\mathbf{x}_r = \left(x_r(0), x_r(1), \ldots., x_r(N^1 - 1)\right)$$

where,

$$x_r(j) = x^1(j) \oplus x^2(j) \tag{28}$$

One or more values from the generated random array $\mathbf{x}_r = (x_r(0), x_r(1), \ldots., x_r(N^1 - 1))$ act as the random stream which is used to generate each normal value in the Gaussian random measurement matrix with mean zero and variance $\frac{1}{N}$.

$$\phi_B \longleftarrow \frac{1}{N}\text{randn}\,(\mathbf{x}_r, M, N) \tag{29}$$

where N and M represents the number of input samples and measured samples respectively in the CS operation.

Algorithm description of secure measurement matrix generation

The algorithm description of the proposed secure measurement matrix generation for compressive

sensing operation using multiple chaotic maps is described below.

1. Generate the encryption key Key as a hexadecimal number, where

$$Key = Key_1 Key_2 Key_3 Key_4$$

$$s.t. \quad Key_i \nmid Key_j; \quad i \neq j$$

2. Select the chaotic pair CP_1 using the decimal equivalent of Key_1.

$$CP_1 = Key_1^d \mod 64$$
$$CP_1 \xrightarrow{\text{octal}} CP_1^c$$
$$CPIN_1 = CP_1^c$$

3. Find the initial values of the selected chaotic maps using the decimal equivalents of Key_1, Key_2 and Key_3 by using the following relations.

$$x^1(0) = \left(\frac{Key_2^d}{Key_1^d}\right) - \left\lfloor \frac{Key_2^d}{Key_1^d} \right\rfloor$$

$$x^2(0) = \left(\frac{Key_3^d}{Key_1^d}\right) - \left\lfloor \frac{Key_3^d}{Key_1^d} \right\rfloor$$

4. Find the number of iterations using Key_4 based on the following relation,

$$N^1 = \left(5Key_4^d + 1\right) \mod 128$$

5. for $j = 0 : N^1 - 1$
Generate the chaotic values for the first and second chaotic maps $x^1(j)$ and $x^2(j)$ respectively to generate the the random value $x_r(j)$.

$$x_r(j) = x^1(j) \oplus x^2(j)$$

6. Generate the $M \times N$ Gaussian random measurement matrix using the $N^1 \times 1$ array $\mathbf{x}_1^r$ as the random stream.

$$\phi_B \longleftarrow \frac{1}{N}\text{randn}\left(\mathbf{x}_r, M, N\right)$$

The following subsection discusses the BCS technique of images using the secure measurement matrix.

BCS of images using single secure measurement matrix

By using multiple chaotic map based measurement matrix in compressive sensing techniques, sampling, compression and encryption can be achieved in a single step. The measurements $\mathbf{y}$ are a function of sensing matrix. The receiver has to know the information about the key used to generate the measurement matrix Key (128-bit) in order to formulate the optimization problem to reconstruct the signal. This section proposes a cryptographic key based random measurement matrix for block-based compressive sensing techniques.

Algorithm description

In BCS, the $N_1 \times N_2$ image is divided into n non-overlapping blocks of size $B \times B$. Fowler et al. proved experimentally that the suitable block size in the BCS approach is 32×32 [15]. The algorithm description of the single measurement based encryption of BCS techniques is given below.

1. Divide the 2D image $\mathbf{X}$ of size $N_1 \times N_2$ into n blocks of size $B \times B$.
2. Rasterize the 2D blocks $\{\mathbf{X}_i\}_{i=1,\ldots,n}$ into $B^2 \times 1$ vectors $\{\mathbf{x}_i\}_{i=1,\ldots,n}$

$$\{\mathbf{x}_i\}_{i=1,\ldots,n} = \text{Raster}(\{\mathbf{X}_i\}_{i=1,\ldots,n})$$

where, Raster(.) represents the rasterization operator.
3. Generate a secure $M_B \times B^2$ measurement matrix ϕ_B based on a 128-bit key (Key), where $M_B = \lfloor \frac{M}{N} B^2 \rfloor$.

$$\phi_B \longleftarrow \frac{1}{B^2}\text{randn}\left(\mathbf{x}_r, M_B, B^2\right)$$

4. Apply $M_B \times B^2$ measurement matrix ϕ_B on $\{\mathbf{x}_i\}_{i=1,\ldots,n}$ to get the the measured vectors $\{\mathbf{y}_i\}_{i=1,\ldots,n}$

$$\{\mathbf{y}_i\}_{i=1,\ldots,n} = \phi_B\{\mathbf{x}_i\}_{i=1,\ldots,n}$$

5. Apply the reconstruction algorithm to reconstruct the 1D vector representation of the

image, where ϕ_B is generated using 128-bit decryption key (Key).

$$\{\tilde{\mathbf{x}}_i\}_{i=1,\ldots,n} = \text{CS\_Reconstruction}\left(\{\mathbf{y}_i\}_{i=1,\ldots,n}, \phi_B, \psi\right)$$

6. Unrasterize the image from $\{\tilde{\mathbf{x}}_i\}_{i=1,\ldots,n}$

$$\{\tilde{\mathbf{X}}\}_{i i=1,\ldots,n} = \text{Unraster}\left(\{\tilde{\mathbf{x}}_i\}_{i=1,\ldots,n}\right)$$

7. Obtain the reconstructed image $\tilde{\mathbf{X}}$ from $\{\tilde{\mathbf{X}}_i\}_{i=1,\ldots,n}$

Here, the CS_Reconsruction(.) is the reconstruction operator used to reconstruct the CS measured images. TV, SPL or MS-BCS-SPL based BCS approaches can be applied in the proposed method.

Security

The total key size of the proposed encryption system is 128 bits. For image/compressive sensing application point of view, this produce a large key space of 2^{128}. Hence, performing Brute force attack is a tedius task in the proposed system. On an average 2^{127} operations are required to be performed for the Brute force attack. Since two chaotic maps are chosen at random for random number of iterations and the random values of two maps are combined together, performing known plaintext attack is also a difficult task. However, if the information of a single block is available with the attacker, there is a chance of retrieving the complete image.

To avoid this possibility, it is proposed to use separate measurement matrix for different blocks of images in BCS of images. Thus, the modified system can provide high level of security with a marginal increase in computational complexity. The following section proposes a secure BCS of images based on multiple measurement matrices.

BCS of images using multiple secure measurement matrices

To generate multiple measurement matrices for multiple blocks of images, it is proposed to generate different random streams from the random pair of chaotic maps for each measurement matrix. It is based on the fact that from the known random stream it is difficult to find out the chaotic maps used due to the combining effect of these two chaotic maps. That means, CP_1 is unknown for an attacker. In this paper, it is proposed to select the next $CPIN$ based on the current $CPIN$ and number of iterations based on the previous iteration number. The initial values of the newly selected chaotic maps are the final chaotic values of the previous chaotic maps.

Let CP_i be the selected chaotic pairs for the generation of i^{th} measurement matrix. Then, the chaotic pair for the next measurement matrix is found by using LCG, which is given as,

$$CP_{i+1} = (5CP_i + 1) \mod 64 \tag{30}$$

Similarly, if N^i represents the number of iterations of the chaotic maps for the i^{th} measurement matrix, then the number of iterations of next chaotic maps for the next measurement matrix will be,

$$N^{i+1} = (5CP_iN_i + 1) \mod 128 \tag{31}$$

The remaining procedure for generating the measurement matrix is same as that explained in section "Algorithm description of secure measurement matrix generation". The measurement matrix for jth block is given as,

$$\phi_{Bj} \longleftarrow \frac{1}{B^2}\text{randn}\left(\mathbf{x}_{rj}, M_B, B^2\right)$$

Algorithm description of multiple measurement matrices based BCS of images

Assume that the $N_1 \times N_2$ image is divided into n non-overlapping blocks of size $B \times B$. Since there are 'n' blocks present in the original image, 'n' measurement matrices are required to perform the secure compressive sensing operation in the proposed system. The measurement matrix generation can be performed in parallel with the compressive sensing operation of individual blocks so that the effective time of operation can be reduced. Let ϕ_{B1}, ϕ_{B2},...,ϕ_{Bn} be 'n' measurement matrices generated by the LFSR based secure system. Then the overall measurement matrix can

be represented as a block diagonal matrix as given below,

$$\phi = \begin{bmatrix} \phi_{B1} & 0 & \ldots & 0 \\ 0 & \phi_{B2} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & \phi_{Bn} \end{bmatrix}$$

The algorithm description of the above mentioned encryption method is given below.

1. Divide the 2D image $\mathbf{X}$ of size $N_1 \times N_2$ into 'n' blocks of size $B \times B$ (Eg: 32×32).
2. Rasterize the 2D blocks $\{\mathbf{X}_i\}_{i=1,\ldots,n}$ into $B^2 \times 1$ vectors $\{\mathbf{x}_i\}_{i=1,\ldots,n}$

   $$\{\mathbf{x}_i\}_{i=1,\ldots,n} = \text{Raster}\left(\{\mathbf{X}_i\}_{i=1,\ldots,n}\right)$$

   where, Raster(.) represents the rasterization operator.
3. For the ith block, generate the measurement matrix $\{\phi_{Bi}\}_{i=1,\ldots,n}$ using the proposed multiple chaotic map based approach mentioned in section "Algorithm description of secure measurement matrix generation" based on the encryption key Key, where, the chaotic maps used and the number of chaotic maps can be decided by the following relations.

   $$CP_{i+1} = (5CP_i + 1) \mod 64$$

   $$N^{i+1} = (5CP_i N_i + 1) \mod 128$$

4. Apply $M_B \times B^2$ measurement matrix $\{\phi_{Bi}\}_{i=1,\ldots,n}$ on $\{\mathbf{x}_i\}_{i=1,\ldots,n}$ to generate

   $$\{\mathbf{y}_i\}_{i=1,\ldots,n} = \{\phi_{Bi}\mathbf{x}_i\}_{i=1,\ldots,n}$$

   where, the subrate $S = \frac{M_B}{B^2}$
5. Apply the reconstruction algorithm to reconstruct the 1D vector representation of the image, by generating the measurement matrices $\{\phi_{Bi}\}_{i=1,\ldots,n}$ based on multiple chaotic maps using the decryption key Key.

   $$\{\tilde{\mathbf{x}}_i\} = \text{CS\_Reconstruction}(\{\mathbf{y}_i\}, \{\phi_{Bi}\}, \psi)_{i=1,\ldots,n}$$

6. Unrasterize the image from $\{\tilde{\mathbf{x}}_i\}_{i=1,\ldots,n}$

   $$\{\tilde{\mathbf{X}}_i\}_{i=1,\ldots,n}) = \text{Unraster}(\{\tilde{\mathbf{x}}_i\}_{i=1,\ldots,n})$$

7. Obtain the reconstructed image $\tilde{\mathbf{X}}$ from $\{\tilde{\mathbf{X}}_i\}_{i=1,\ldots,n}$

Even though, the proposed multiple measurement matrix based encryption technique for BCS of images takes higher computational time than single measurement matrix based encryption technique, the complexity of both the proposed approaches are simple and can maintain the robustness of the compressive sensing system to noise.

Analysis of the proposed encryption system

The different BCS approaches for images are considered for evaluating the performance of the proposed encryption system. Both the single and the multiple measurement matrices based encryption methods are validated through BCS-TV, BCS-SPL-DCT, BCS-SPL-DWT, BCS-SPL-DDWT and MS-BCS-SPL techniques. Experimentally it is proved that the proposed system maintains the reconstruction quality and the robustness of these approaches with high level of security.

Experimental analysis of the proposed encryption system is performed on several images. For analysis standard images of size 512×512 divided into non-overlapping blocks of 32×32 are considered. Thus, each block can be converted into a column vector of 1024×1 and the total number of blocks for each image is 256. For multiple measurement matrix based encryption system, 256 measurement matrices are required. In MS-BCS-SPL, DWT transform with 3 decomposition levels is considered and each level is divided into 32×32 blocks. The proposed system is performed with different subrates, $S = 0.1, 0.2, 0.3, 0.4$ and 0.5 for various images. In hard thresholding, the convergence factor λ is chosen as 6 whereas in bivariate shrinkage the convergence factor λ is selected as 25.

Security analysis

The proposed encryption system is tested against various forms of attacks and proved to be resistant against the same. The main problem with the chaotic maps is its vulnerability to known plaintext attack. In the proposed system, the random selection of chaotic maps and combining their

outputs make it capable of withstanding known plaintext attack.

Known plaintext attack

In the proposed system, instead of random selection of a single chaotic map, it is proposed to select a pair of chaotic maps based on a secret key. The number of iterations for these chaotic maps is also determined by another secret key. Thus, there is a randomization in the chaotic map selection from 64 combinations and number of random elements used for generating the measurement matrix. In the proposed approach, the randomly selected chaotic maps are run for random number iterations to form two sets of random arrays. The corresponding elements of these arrays are XORed to form new random array.

$$x_r(j) = x^1(j) \oplus x^2(j)$$

Thus, the newly generated random array depends on initial values of both the selected chaotic maps. From the known random elements, it is very difficult to find out the chaotic maps used in this combination and corresponding initial values. Moreover, the process of finding out the random stream used for generating the measurement matrix becomes a tedious task.

If the plaintext-ciphertext pairs of a single block are available with the attacker, the only possible way to find out the measurement matrix used for that block will be the Brute force search approach. This rare chance of attack can be negated, if all blocks are measured with different measurement matrices. In the proposed approach, the chaotic maps for the next measurement matrix and the number iterations used for generating the random array to form the measurement matrix are based on the relations.

$$CP_{i+1} = (5CP_i + 1) \mod 64$$

$$N^{i+1} = (5CP_iN_i + 1) \mod 128$$

The chaotic pair selection is dependent on the previous chaotic pair selection. That is not known for the attacker. Moreover, the number of iterations depends on the previous number of iterations as well as the previous chaotic pair map number. Even though, the attacker has the knowledge about the number of iterations without knowing the previously used chaotic pair map number, he will not be able to find the number of iterations for the current pair of chaotic maps. Thus, the proposed encryption system can withstand known plaintext attack.

Cipher text-only attack

Cipher text-only attack (COA) or known ciphertext attack is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts. The attack is completely successful if the corresponding plaintexts can be deduced, or even better, the key. Since the attacker has only minimum information about the message, the ciphertext only attack is much more difficult than known plaintext attack. In this case, the only possibility to retrieve plaintext is to make Brute force trials on both keys, which is very complex. Thus, a system, which is capable of resisting known plaintext attack can withstand against ciphertext only attack.

Brute force attack

In the proposed approach, the external secret key has a size of 128-bit. Thus, the key space for the proposed encryption system for BCS of images is 2^{128}. For image application, this accounts to very large key space. For successful Brute force attack, on an average $(2^{128}/2)$ operations are required to retrieve the key used for encryption. Hence the security of the proposed encryption for BCS of images against Brute force attack is very high.

Reconstruction performance of the proposed encryption system

The quality analysis of reconstructed images of the proposed encryption system for BCS of images is performed. Various test images are considered for evaluating the performance of the proposed encryption system. Different BCS approaches like, BCS-TV, BCS-SPL-DCT, BCS-SPL-DWT, BCS-SPL-DDWT and MS-BCS-SPL are applied to these images to check the reconstruction quality, which is measured in terms of

the peak signal to noise ratio (PSNR) value of the reconstructed images with the corresponding original images. The PSNR for an $N_1 \times N_2$ image can be calculated as,

$$PSNR = 10log_{10}\left(X^2_{\max}/MSE\right) \tag{32}$$

where, $X_{\max}$ is the maximum possible pixel value of the image. The MSE can be calculated as,

$$MSE = \frac{1}{N_1 N_2}\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}(X(i,j) - Y(i,j))^2 \tag{33}$$

where $X(i, j)$ and $Y(i, j)$ represent corresponding pixel values of the original and reconstructed images respectively.

The rate can be calculated by using the following relation,

$$\text{Rate} = \frac{M}{N}H_y \tag{34}$$

where, H_y is the entropy of the measured data y after quantization in bits per pixel, where the problem of unused quantisation values can be avoided by considering that these values occurred at once [35]. For single measurement matrix approach, DPCM is incorporated to get quantized BCS instead of only scalar quantization [29]. The PSNR and the rate at different subrates for the test images Lena, Goldhill and Barbara are given in Table 2. Comparable PSNR values as that of the results given in [15] are obtained from the proposed system, which shows that the proposed encryption system can maintain the quality level.

The rate-distortion characteristics of the Lena, Goldhill and Barbara images for different BCS reconstruction approaches are given in Fig. 2a–c. The reconstructed images under different reconstruction methods for 'Peppers' image at a subrate $S = 0.2$ are shown in Fig. 3a–e. The construction qualities in PSNR for Peppers image under different reconstruction methods are 31.41

Table 2 Reconstruction performance of the proposed encryption system for 512 × 512 images

Lena					
Subrate	0.1	0.2	0.3	0.4	0.5
Rate	0.75	1.47	2.08	2.89	3.51
	PSNR (dB)				
BCS-TV	27.62	30.58	32.69	34.4	35.95
BCS-DCT	27.42	30.47	32.56	34.22	35.81
BCS-DWT	27.78	30.81	32.93	34.59	36.13
BCS-DDWT	27.96	31.37	33.44	35.19	36.71
MS-BCS-SPL	31.82	33.84	35.48	37.03	38.62
Goldhill					
Rate	0.74	1.44	2.22	2.91	3.51
	PSNR (dB)				
BCS-TV	26.72	28.81	30.41	31.89	33.32
BCS-DCT	26.31	28.29	29.78	31.11	32.58
BCS-DWT	26.71	28.64	30.16	31.49	32.76
BCS-DDWT	27.01	28.86	30.36	31.65	33.06
MS-BCS-SPL	29.15	30.61	31.92	33.26	34.71
Barbara					
Rate	0.76	1.53	2.27	3.02	3.69
	PSNR (dB)				
BCS-TV	22.31	23.52	24.89	26.21	27.84
BCS-DCT	22.57	23.82	25.26	26.78	28.43
BCS-DWT	22.37	23.81	25.21	26.51	28.05
BCS-DDWT	22.65	24.19	25.59	27.22	28.81
MS-BCS-SPL	23.31	24.92	26.45	28.04	29.68

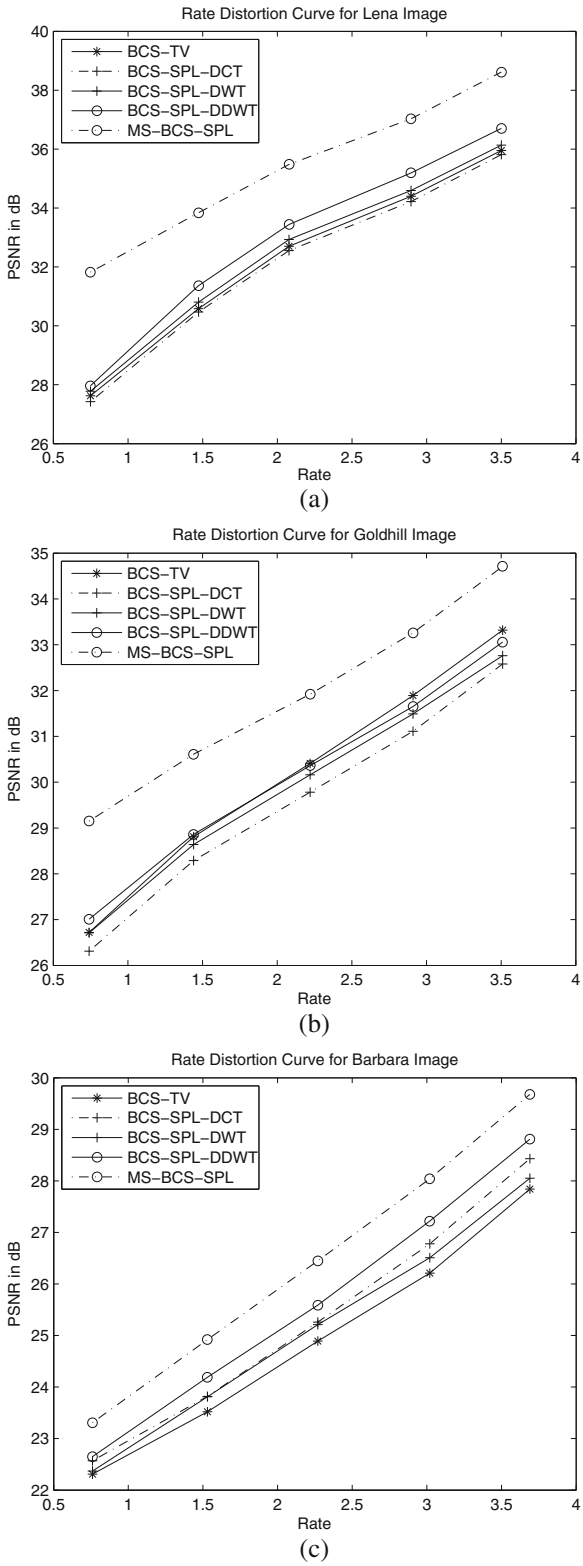

Fig. 2 Rate distortion curves for the proposed encryption system (**a**) Lena, (**b**) Goldhill, (**c**) Barbara images

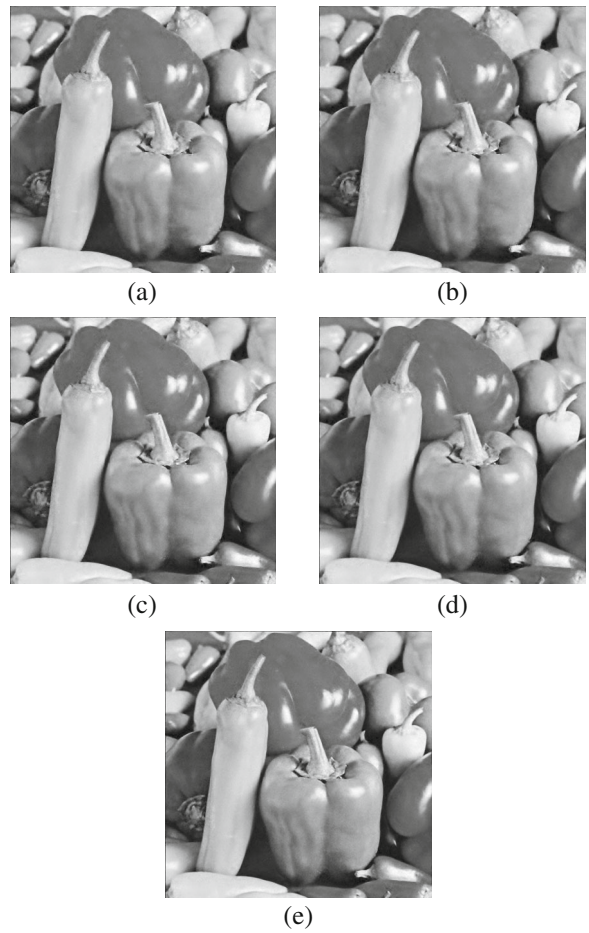

Fig. 3 Reconstruction using **a** BCS-TV (31.41 dB), **b** BCS-SPL-DCT (31.11 dB), **c** BCS-SPL-DWT (31.72 dB), **d** BCS-SPL-DDWT (32.09 dB), **e** MS-BCS-SPL (32.96 dB) for "Peppers" image at $S = 0.2$

dB (Fig. 3a), 31.11 dB (Fig. 3b), 31.72 dB (Fig. 3c), 32.09 dB (Fig. 3d) and 32.96 dB (Fig. 3e) for BCS-TV, BCS-SPL-DCT, BCS-SPL-DWT, BCS-SPL-DDWT and MS-BCS-SPL respectively.

Robustness to noise of the proposed system

In [4], it is mentioned that the compressive sensing paradigm provides perfect reconstruction in the presence of added noise in the real-application by solving it as an optimization problem. In the proposed encryption system, the key based generation of random measurement matrix maintain the robustness of the compressive sensing system. The empirical evaluation of the robustness can

be performed by finding the characteristics between the PSNR and normalized noise perturbation power. The normalized noise perturbation power ($nPERT_y$) on y is given as [31],

$$nPERT_y = 10log\frac{\|\tilde{y} - y\|^2}{\|y\|^2} \tag{35}$$

where, $\tilde{y}$ represents the noisy version of measurement vector. The robustness of the proposed system can be evaluated from normalized noise perturbation power versus PSNR characteristics.

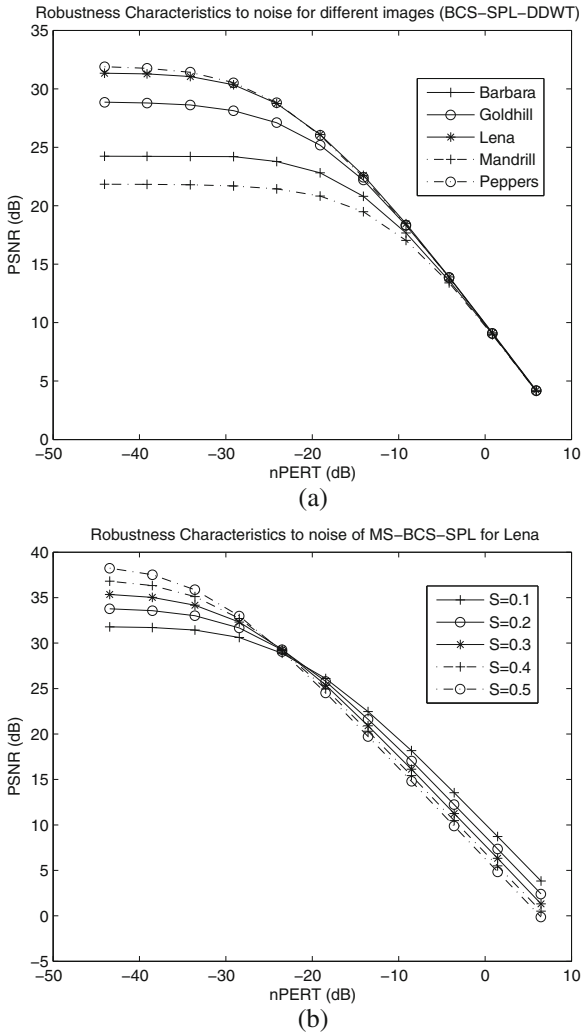

Fig. 4 **a** Robustness characteristics to noise of the proposed encryption system for different images under BCS-SPL-DDWT reconstruction at $S = 0.2$, **b** Robustness characteristics to noise for MS-BCS-SPL reconstruction approach for Lena image

Figure 4a shows the robustness characteristics of the proposed encryption method to noise for various standard images of size 512×512 at $S = 0.2$, where BCS-SPL-DDWT approach is adopted. From the characteristics, it can be understood that the proposed encryption system can maintain the robustness of the compressive sensing approach for any image. Even at -20 dB of normalized noise perturbation power ($nPERT_y$), the proposed encryption method for BCS-SPL approaches give good PSNR value. Thus, the proposed encryption system maintains robustness to noise as that of the ordinary compressive sensing system for BCS-SPL reconstruction approaches. Figure 4b represents the robustness characteristics to noise for Lena image for MS-BCS-SPL reconstruction approach. In general, the proposed encryption system maintains the robustness to noise in the compressive sensing framework at any subrate for any reconstruction approach.

Conclusion

In this paper, a novel approach for secure compressive sensing of images is presented by generating random measurement matrix based on multiple chaotic maps so that the encryption system can maintain the robustness of the compressive sensing system to noise. For the generation of measurement matrix, eight one dimensional chaotic maps are chosen from which two are randomly selected based on a secret key. The number of iterations of these chaotic maps are also decided by an external key and the chaotic values obtained from these maps are combined together to form a new random array. To improve the security, key based decision of initial values of the chaotic maps are incorporated. The generated random stream is used to generate each normal value of the random measurement matrix. Since the chaotic values of two randomly selected chaotic maps are combined together, it is very difficult to mount a successful known plaintext attack. To improve the security further, it is proposed to use different measurement matrices for different blocks of images. The chaotic map selection and its number of iterations are determined by the previous chaotic maps and its number of iterations. The proposed encryption

system is validated through different reconstruction approaches of BCS and it was found that it maintains the reconstruction quality and robustness of the compressive sensing with high level of security.

References

1. A.A. Abd El-Latif, L. Li, T. Zhang, N. Wang, X. Song, X. Niu, Digital image encryption scheme based on multiple chaotic systems. Sens. Imaging **13**(2), 67–88 (2012)
2. R. Baraniuk, Compressive sensing [lecture notes]. IEEE Signal Proc. Mag. **24**(4), 118–121 (2007)
3. E. Candès, J. Romberg, T. Tao, Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. IEEE Trans. Inf. Theory **52**(2), 489–509 (2006)
4. E. Candes, J. Romberg, T. Tao, Stable signal recovery from incomplete and inaccurate measurements. Commun. Pur. Appl. Math. **59**(8), 1207–1223 (2006)
5. E. Candes, T. Tao, Near-optimal signal recovery from random projections: Universal encoding strategies? IEEE Trans. Inf. Theory **52**(12), 5406–5425 (2006)
6. E. Candès, M. Wakin, An introduction to compressive sampling. IEEE Signal Proc. Mag. **25**(2), 21–30 (2008)
7. C. Deng, W. Lin, B. Lee, C. Lau, Robust image compression based on compressive sensing. in *Proc. IEEE International Conference on Multimedia and Expo (ICME)*(2010), pp. 462–467
8. C. Deng, W. Lin, B. Lee, C. Lau, Robust image coding based upon compressive sensing. IEEE Trans. Multimedia **14**(2), 278–290 (2012)
9. M. Do, M. Vetterli, The contourlet transform: an efficient directional multiresolution image representation. IEEE Trans. Image Process. **14**(12), 2091–2106 (2005)
10. D. Donoho, De-noising by soft-thresholding. IEEE Trans. Inf. Theory **41**(3), 613–627 (1995)
11. D. Donoho, Compressed sensing. IEEE Trans. Inf. Theory **52**(4), 1289–1306 (2006)
12. M. Duarte, M. Davenport, D. Takhar, J. Laska, T. Sun, K. Kelly, R. Baraniuk, Single-pixel imaging via compressive sampling. IEEE Signal Proc. Mag. **25**(2), 83–91 (2008)
13. M.F. Duarte, Y.C. Eldar, Structured compressed sensing: From theory to applications. IEEE Trans. Signal Proc. **59**(9), 4053–4085 (2011)
14. S. Etemadi Borujeni, M. Eshghi, M.S. Boroujeni, Mehrab maps: One-dimensional piecewise nonlinear chaotic maps. Int. J. Bifur. Chaos **22**(05), 1–11 (2012)
15. J. Fowler, Block-based compressed sensing of images and video. Found. Trends Signal Proc. **4**(4), 297–416 (2012)
16. J. Fowler, S. Mun, E. Tramel, Multiscale block compressed sensing with smoother projected landweber reconstruction. in *Proceedings of the European Signal Processing Conference* (2011), pp. 564–568
17. L. Gan, Block compressed sensing of natural images. in *Proc. 15th International Conference on Digital Signal Processing* (2007), pp. 403–406
18. D. Gao, D. Liu, Y. Feng, Q. An, F. Yu, A robust image transmission scheme for wireless channels based on compressive sensing. in *Proc. Advanced Intelligent Computing Theories and Applications with Aspects of Artificial Intelligence* (2010), pp. 334–341
19. H. Gao, Y. Zhang, S. Liang, D. Li, A new chaotic algorithm for image encryption. Chaos, Solitons Fractals **29**(2), 393–399 (2006)
20. V. Goyal, A. Fletcher, S. Rangan, Compressive sampling and lossy compression. IEEE Signal Proc. Mag. **25**(2), 48–56 (2008)
21. B. Han, F. Wu, D. Wu, Image representation by compressive sensing for visual sensor networks. J. Vis. Commun. Image Represent. **21**(4), 325–333 (2010)
22. J. Haupt, R. Nowak, Signal reconstruction from noisy random projections. IEEE Trans. Inf. Theory **52**(9), 4036–4048 (2006)
23. R. Huang, K. Sakurai, A robust and compression-combined digital image encryption method based on compressive sensing. in *Proc. Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*(2011), pp. 105–108
24. N. Kingsbury, Complex wavelets for shift invariant analysis and filtering of signals. Appl. Comput. Harmon. Anal. **10**(3), 234–253 (2001)
25. A. Kumar, A. Makur, Lossy compression of encrypted image by compressive sensing technique. in *TENCON 2009–2009 IEEE Region 10 Conference* (IEEE, 2009), pp. 1–5
26. C. Li, An efficient algorithm for total variation regularization with applications to the single pixel camera and compressive sensing. Ph.D. thesis, Citeseer, 2009
27. P. Lu, Z. Xu, X. Lu, X. Liu, Digital image information encryption based on compressive sensing and double random-phase encoding technique. Optik–Int. J. Light Electron Opt. **124**(16), 2514–2518 (2012)
28. S. Mun, J. Fowler, Block compressed sensing of images using directional transforms. in *16th IEEE International Conference on Image Processing (ICIP), 2009* (IEEE, 2009), pp. 3021–3024
29. S. Mun, J.E. Fowler, Dpcm for quantized block-based compressed sensing of images. in *Proceedings of the 20th European Signal Processing Conference (EUSIPCO), 2012* (IEEE, 2012), pp. 1424–1428
30. M.A. Neifeld, J. Ke, Optical architectures for compressive imaging. Appl. Opt. **46**(22), 5293–5303 (2007)
31. A. Orsdemir, H. Altun, G. Sharma, M. Bocko, On the security and robustness of encryption via compressed sensing. in *Proc. Military Communications Conference (MILCOM)*(2008), pp. 1–7
32. N. Pareek, V. Patidar, K. Sud, Cryptography using multiple one-dimensional chaotic maps. Commun. Nonlinear Sci. Numer. Simul. **10**(7), 715–723 (2005)

33. Y. Rachlin, D. Baron, The secrecy of 1027 compressed sensing measurements. in *Proc. 46th Annual Allerton Conference on Communication, Control, and Computing* (2008), pp. 813–817
34. J. Romberg, Imaging via compressive sampling. IEEE Signal Proc. Mag. **25**(2), 14–20 (2008)
35. A. Schulz, L. Velho, E.A. Da Silva, On the empirical rate-distortion performance of compressive sensing. in *Proc. 16th IEEE International Conference on Image Processing (ICIP)*(2009), pp. 3049–3052
36. L. Sendur, I. Selesnick, Bivariate shrinkage functions for wavelet-based denoising exploiting interscale dependency. IEEE Trans. Signal Proc. **50**(11), 2744–2756 (2002)
37. K. Soman, Secrecy of cryptography with compressed sensing. in *International Conference on Advances in Computing and Communications (ICACC), 2012* (IEEE, 2012), pp. 207–210
38. D. Takhar, J.N. Laska, M.B. Wakin, M.F. Duarte, D. Baron, S. Sarvotham, K.F. Kelly, R.G. Baraniuk, A new compressive imaging camera architecture using optical-domain compression. in *Proc. Electronic Imaging* (2006), pp. 43–52
39. A.G. Tomida, Matlab toolbox and gui for analyzing one-dimensional chaotic maps. in *International Conference on Computational Sciences and Its Applications, 2008*. ICCSA'08 (IEEE, 2008), pp. 321–330
40. D. Venkatraman, A. Makur, A compressive sensing approach to object-based surveillance video coding. in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, 2009 (ICASSP)*(2009), pp. 3513–3516
41. X.Y. Wang, L. Yang, Design of pseudo-random bit generator based on chaotic maps. Int. J. Mod. Phys. B **26**(32), 1–9 (2012)
42. L.l. Xiao, K. Liu, D.p. Han, CMOS low data rate imaging method based on compressed sensing. Opt. Laser Technol. **44**(5), 1338–1345 (2012)
43. L. Zhang, X. Liao, X. Wang, An image encryption approach based on chaotic maps. Chaos, Solitons Fractals **24**(3), 759–765 (2005)