OPEN

Image compression-encryption method based on two-dimensional sparse recovery and chaotic system

Aboozar Ghaffari

In this paper, we propose an image compression-encryption method based on two-dimensional (2D) sparse representation and chaotic system. In the first step of this method, the input image is extended in a transform domain to obtain a sparse representation. To achieve better performance of image compression by 2D sparse recovery, the sparse representation is scrambled via a chaotic confusion. This step helps the satisfaction of the uniqueness conditions for sparse recovery, and the security level of encryption is increased. Then, two orthogonal measurement matrices are generated using the chaotic time series. The singular value decomposition is used to compress the sparse scrambled representation in two dimensions. Finally, to reduce the correlation between adjacent pixels in the compressed matrix, and obtain a uniform distribution in the encrypted image, a compressed scrambling matrix based on chaotic confusion is used. Then, XOR operation is applied for final encryption. In the decryption process, to improve the compression efficiency, the total variation constraint is added to the 2D sparse recovery problem based on the smoothed norm. The simulation results demonstrate the satisfying performance of the proposed method for different compression ratios. Security analysis describes the effectiveness of the proposed encryption approach.

Recently, by the development of technology and network, images are widely used in various applications. Since the images are usually needed to transmit in an insecure channel such as the internet, protection of images from various attacks by hackers is an essential task in various applications such as health care^{1,2}, multimedia systems, and military³. Image encryption is an important approach to convert data to a meaningless form that its understanding is difficult^{3,4}. Image encryption approaches are categorized into symmetric and asymmetric key cryptography^{5,6}. Recently, different architectures were proposed to encryption images such as optical image encryption^{7,8}, DNA coding^{9,10}, XOR operation^{11,12} and quantum image encryption^{13–16}. Since chaotic systems are sensitive to the initial conditions, various encryption algorithms based on chaotic systems were proposed. So, their initial conditions are used as a key in the encryption process^{13,17–20}. Usually, the encrypted image is like a noisy image or texture image. Recently, the visually meaningful encryption schemes were proposed that have used a carrier image to encrypt and transmit the original image^{21,22}.

In the transmission network, the original image should be encrypted and compressed due to the limited bandwidth and illegal eavesdropping. Recently, the image encryption based on compressed sensing (CS) or sparse representation has been a hot topic^{23–26}. These approaches have assumed that the original image has a sparse representation in a transform domain such as wavelet or discrete cosine transform (DCT). Then the sparse representation is compressed by a measurement matrix, which is a part of the encryption key. In the decryption process, the original image is recovered by an optimization problem of sparse recovery. To obtain better security performance, sparse representation and traditional approaches were combined. Visually meaningful encryption schemes^{22,27,28}, chaotic map^{29–36}, cellular automata^{37,38}, and discrete fractional random transform³⁹ are some examples.

An essential measure of CS-based encryption schemes is compression and reconstruction performance. Hence, many works have been done to obtain better reconstruction. In sparse recovery, the transform which is used to obtain sparse representation has a critical role. Many different transforms, such as wavelet^{34,40}, DCT³⁸, and learned dictionary³⁵, were used in different approaches. The transforms also can be categorized into block-based transform³⁵ and global-based transform^{21,34}. In Ref.⁴¹, it was shown that the scrambling of sparse coefficients could improve compression and reconstruction performance. Some approaches have used the zigzag scan for random permutation of the sparse coefficients^{38,41,42}. To reduce the computational complexity and required memory, in the sparse recovery literature, sparse decomposition of the two-dimensional signal⁴³ or

Department of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran. email: aboozar_ghaffari@iust.ac.ir

Kronecker compressed sensing⁴⁴ based on two measurement matrices in two directions has been proposed. Hence, some proposed encryption approaches have used two measurement matrices to obtain better compression and reconstruction performance^{34,39,45}. Also, designing the measurement matrix is a modification approach to obtain better performance. Usually, CS-based encryption approaches use chaotic systems to generate this matrix. Some approaches construct the measurement matrix based on the combination of the Hadamard transform and chaotic map^{22,38,39,45}.

In this paper, an image encryption approach based 2D sparse recovery is proposed. In Ref.⁴³, the uniqueness conditions of 2D sparse recovery were investigated based on the spark definition. The main properties of these conditions are that the uniformity of sparse coefficients in rows and columns improves the uniqueness conditions to obtain better compression and sparse reconstruction. Based on this theory, a random permutation using a chaotic Lorenz system is proposed. Random orthogonal measurement matrices are constructed via the Lorenz system and singular value decomposition. Simulation results show that the proposed method has an acceptable performance. In this algorithm, the total variation is proposed in the sparse recovery problem based on smoothed ℓ_0 norm SLO^{43,46}. In the decryption process, a sparse recovery approach based on the SLO, total variation, and scrambling of sparse coefficients is proposed. This approach improves the compression and reconstruction performance effectively in comparison with other approaches at the same compression ratio. The results show that the proposed approach is robust in the presence of a cropping attack. To obtain the meaningless image in the encryption process, XOR operation and the Lorenz system are used. Security analyses illustrate the effectiveness of the proposed encryption approach. In the section of preliminaries, the concept of 2D sparse recovery and Lorenz system are described. The main idea and the proposed method are stated in the section of the proposed encryption method. The section of experimental results provides security analyses. Finally, the paper is concluded, and the future work direction is pointed out.

Preliminaries

Sparse representation. An important core of signal processing is signal decomposition representing a signal vector $\mathbf{y} \in R^n$ using a linear combination of some basis functions $\phi_i, 1 \leq i \leq m$, that is $\mathbf{y} = s_1\phi_1 + \dots + s_m\phi_m = \Phi\mathbf{s}$, where $\Phi = [\Phi_1, \dots, \Phi_m]$, and $\mathbf{s} = [s_1, \dots, s_m]^T$. Recently, the sparsity assumption on signal and image representation ($\mathbf{s}$) has been used for various applications such as image denoising⁴⁷, blind source separation⁴⁸, compressed sensing²⁴, pattern recognition⁴⁹, and image registration^{50,51}. It is assumed that the signal is k -sparse, which means it has at most k non-zero entries in a learned dictionary or a transform domain such as discrete cosine transform or wavelet.

Sparsity assumption is the basis of compressed sensing. It has a crucial role in our proposed method of image encryption. The goal of compressed sensing is to recover an unknown sparse signal $\mathbf{s} \in R^m$ from a set of under-determined measurements $\mathbf{y} = \Phi\mathbf{s} \in R^n (m < n)$ where $\Phi \in R^{n \times m}$ is the measurement matrix. Sparse recovery problem can be formulated as:

$$P_0^{1D} : \text{Minimize} \|\mathbf{s}\|_0 \text{ s.t. } \mathbf{y} = \Phi\mathbf{s} \quad (1)$$

where $\|\mathbf{s}\|_0$ stands for the ℓ_0 norm of $\mathbf{s}$ that is the number of non-zero elements of $\mathbf{s}$. In this problem, there are two fundamental questions as follows:

1. Uniqueness: does the problem P_0^{1D} have a unique solution?
2. Practical solver: does the optimization problem of the sparsest solution have a practical solver?

In reply to the first question, it has been shown that under some conditions, the sparsest solution is unique. Here, we state the uniqueness theorem based on the spark definition.

Theorem (Uniqueness⁵²): Let $\text{spark}(\Phi)$ denote the minimum number of columns of Φ that are linearly dependent. Then if the equation $\mathbf{y} = \Phi\mathbf{s}$ has a solution $\mathbf{s}_0$ for which $\|\mathbf{s}_0\|_0 < \text{spark}(\Phi)/2$, it is its unique sparsest solution.

Although the sparsest solution of (1) may be unique, finding it requires a combinatorial search and is generally NP-hard. Several methods have been developed in recent years such as matching pursuit⁵³, basis pursuit⁵⁴ and smoothed ℓ_0 (SLO)⁴⁶.

In some application, we need to use compressive sensing on two dimensional (2D) signal. To achieve this goal, a trivial approach is to convert the 2D problem to the above one-dimensional (1D) problem. Two disadvantages of this approach are the computational load and the high required memory. To overcome these problems, two measurement matrices $\Phi_1 \in R^{n_1 \times m_1}$ and $\Phi_2 \in R^{n_2 \times m_2}$ were used to compress a sparse matrix $\mathbf{S} \in R^{m_1 \times m_2}$ in the form of $\mathbf{Y} = \Phi_1\mathbf{S}\Phi_2^T \in R^{n_1 \times n_2}$ ⁴³. The sparse recovery based on two measurement matrices can be obtained by solving the following optimization problem.

$$P_0^{2D} : \text{Minimize} \|\mathbf{S}\|_0 \text{ s.t. } \mathbf{Y} = \Phi_1\mathbf{S}\Phi_2^T \quad (2)$$

The uniqueness of this problem has been shown in some researches^{43,55,56}. In Ref.⁴³, the uniqueness conditions of this sparse recovery problem based on spark definition were investigated. It has been shown that the necessary (but not sufficient) conditions about the distribution of non-zero entries of $\mathbf{S}$ are as follows:

- $\|\mathbf{S}_0\|_0 < \frac{\text{spark}(\Phi_1)\text{spark}(\Phi_2)}{4}$
- $(\ell_0 \text{ norm of each column}) < \frac{\text{spark}(\Phi_1)}{2}$
- $(\ell_0 \text{ norm of each row}) < \frac{\text{spark}(\Phi_2)}{2}$

Figure 1. Chaotic attractor of Lorenz system in parameters $\sigma = 10$, $\beta = \frac{8}{3}$ and $\rho = 28$, and initial conditions $[x_{01}, y_{01}, z_{01}] = [-0.823, 3.423, 0.178]$; (a) 2D projection of chaotic attractor in $X - Y$ plane; (b) 2D projection of chaotic attractor in $X - Z$ plane; (c) 2D projection of chaotic attractor in $Y - Z$ plane; (d) 3D chaotic attractor; these attractors are generated by ODE15s in MATLAB 2018a.

Some sparse recovery algorithms have been proposed to solve 2D compressed sensing such as 2D orthogonal matching pursuits (2D-OMP)⁵⁷, 2D projected gradient (2DPG) algorithm⁵⁸, and 2D smoothed ℓ_0 (2D-SL0)⁴³.

In this paper, a new approach of image encryption based on 2D smoothed ℓ_0 norm is proposed. The idea of SL0 is to replace ℓ_0 norm with a smooth approximation of ℓ_0 norm such as $S_0 \approx S_{\sigma 0} = \sum_{i,j} \left(1 - \exp \left(-\frac{s_{ij}^2}{2\sigma^2} \right) \right)$. 2DSL0 tries to solve directly P_0^{2D} problem. The smoothed ℓ_0 norm is equivalent to ℓ_0 norm when $\sigma \rightarrow 0$. 2DSL0 minimizes $S_{\sigma 0}$ for a small σ , subject to $\mathbf{Y} = \Phi_1 \mathbf{S} \Phi_2^T$. In this paper, to improve the performance of sparse recovery, the 2DSL0 problem is regularized with the total variation (TV).

Lorenz system. Lorenz system is one of the well-known chaotic systems which is highly sensitive to initial conditions⁵⁹. It means that a small change in initial values can cause a considerable change in the final state of the time series. The Lorenz system is presented in Eq. (3). The chaotic attractor of the Lorenz system in parameters $\sigma = 10$, $\beta = \frac{8}{3}$ and $\rho = 28$, and initial conditions $[x_{01}, y_{01}, z_{01}] = [-0.823, 3.423, 0.178]$ is shown in Fig. 1.

$$\begin{aligned} \dot{x} &= \sigma(y - x) \\ \dot{y} &= x(\rho - z) - y \\ \dot{z} &= xy - \beta z \end{aligned} \quad (3)$$

Figure 2. The block diagram of the proposed encryption approach.

The proposed encryption method. In this section, we propose a new image encryption algorithm based on two-dimensional compressed sensing and the chaotic Lorenz system. The proposed algorithm consists of two steps: compression via 2D compressed sensing and scrambling based on pixel shuffling and XOR operator. Figure 2 illustrates the block diagram of the image compression-encryption algorithm. In the rest of this section, at first two blocks of confusion based on chaotic and constructing measurement matrix are demonstrated, then the encryption process is described.

Chaotic confusion. In the previous section, we investigate the uniqueness conditions of 2D sparse representation based on the distribution of non-zero entries of the sparse representation matrix. To achieve these conditions, the sparse coefficient matrix is confused by shuffling based on the chaotic system. This confusion also decreases the correlation among elements of the sparse matrix to increase the security level of image encryption. The steps of chaotic confusion (CC) are described as follows:

1. Generating the sequence $X = \{x_i\}$ of the Lorenz system for an initial condition with a suitable step size in the Runge–Kutta method. The length of X is equal to the number of sparse matrix elements.
2. Transforming the sequence $X = \{x_i\}$ into integer sequence $X^* = \{x_i^*\}$:

$$x_i^* = \text{mod}(x_i \times 10^{15}, 2^{16})$$

3. Sorting the sequence X^* :

$$[X_s^*, \text{idx}_s^X] = \text{sort}(X^*)$$

where $[\cdot, \cdot] = \text{sort}(\cdot)$ is the sequencing operator, X_s^* is the sorted sequence, idx_s^X is the index sequence of X_s^* containing a sequence of integer numbers with a random perturbation.

4. Shuffling the entries of the sparse matrix according to the sequence idx_s^X .

We also use this approach in the scrambling step of the image encryption algorithm.

Chaotic measurement matrix generation. The measurement matrix has a crucial task in compressed sensing. In the proposed method, at first, the original image is transformed into a sparse domain via DWT. Then the sparse matrix $S \in R^{n_1 \times n_2}$ is measured and compressed using two measurement matrices $\Phi_1 \in R^{m_1 \times n_1}$ and $\Phi_2 \in R^{m_2 \times n_2}$. Here, to generate the measurement matrices, we use a unitary matrix constructed by a random matrix based on the chaotic system. The state variables $Y = \{y_i\}$ and $Z = \{z_i\}$ of the Lorenz system are used to generate measurement matrices Φ_1 and Φ_2 , respectively. The generation process of the two matrices is similar. Five steps of matrix generation for Φ_1 are describes as follows:

1. Generating the sequence $Y = \{y_i\}$ of the Lorenz system for an initial condition with a suitable step length in the Runge–Kutta method. The length of Y is equal to n_1^2 .

- Transforming the sequence $Y = \{y_i\}$ into integer sequence $Y^* = \{y_i^*\}$:

$$y_i^* = \text{mod}(y_i \times 10^{15}, 2^{16})$$

- Reshaping the sequence Y^* to construct the matrix $\mathbf{Y}_M \in R^{n_1 \times n_1}$ which is a random matrix generated by a chaotic system.
- Computing the singular value decomposition:

$$\mathbf{Y}_M = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^T$$

where $\mathbf{\Sigma} \in R^{n_1 \times n_1}$ is a diagonal matrix containing singular values. The matrices $\mathbf{U} \in R^{n_1 \times n_1}$ and $\mathbf{V} \in R^{n_1 \times n_1}$ are unitary in which their columns are singular vectors.

- Constructing the measurement matrix Φ_1 by selecting the first m_1 rows of matrix $\mathbf{U}$.

Image encryption and compression based on 2D sparse representation. Here, we investigate the proposed encryption process (Fig. 2) as follows:

Step 1: The original image $\mathbf{I} \in R^{n_1 \times n_2}$ is extended in a transform domain Ψ such as DWT, to obtain the sparse representation $\mathbf{S}$:

$$\mathbf{S} = \Psi^T \mathbf{I} \Psi \in R^{n_1 \times n_2}$$

Step 2: The chaotic confusion is used to scramble the sparse matrix $\mathbf{S}$:

$$\mathbf{S}_s = CC\{\mathbf{S}\}$$

where $CC\{\cdot\}$ is a chaotic confusion operator.

Step 3: The sparse matrix $\mathbf{S}_s$ is measured using two chaotic measurement matrices $\Phi_1 \in R^{m_1 \times n_1}$ and $\Phi_2 \in R^{m_2 \times n_2}$:

$$\mathbf{S}_M = \Phi_1 \mathbf{S}_s \Phi_2^T \in R^{m_1 \times m_2}$$

In our simulation, it is assumed that the compression ratio is the same in two dimensions, i.e. $\frac{m_1}{n_1} = \frac{m_2}{n_2}$. Hence total compression ratio (CR) is equal to the square of the CR in each dimension.

Step 4: The measured matrix $\mathbf{S}_M$ is mapped and quantized in the range of [0,255] using the following formula:

$$\mathbf{S}_Q = \left\lceil \frac{255(\mathbf{S}_M - \min(\mathbf{S}_M))}{\max(\mathbf{S}_M) - \min(\mathbf{S}_M)} \right\rceil$$

where $\lceil x \rceil$ rounds the entry of x to the nearest integer value. In this mapping, each pixel of $\mathbf{S}_Q$ can be represented by one byte.

Step 5: The chaotic confusion is used to scramble the quantized matrix $\mathbf{S}_Q$:

$$\mathbf{S}_{QS} = CC\{\mathbf{S}_Q\}$$

This step increases security level by reducing the correlation among the elements of the quantized matrix $\mathbf{S}_Q$.

Step 6: In the final step, to obtain a uniform distribution for the encrypted image, the scrambled matrix $\mathbf{S}_{QS}$ is XORed with a random sequence generated by the Lorenz system. This step is investigated as follows:

Generating the sequences $Y = \{y_i\}$ and $Z = \{z_i\}$ of Lorenz system for an initial condition with a suitable step length in the Runge–Kutta method. The length of Y and Z is equal to $m_1 m_2$.

Two sequences Y and Z are transformed into integer number in the range of [0,255]:

$$y_i^* = \text{mod}(y_i \times 10^{15}, 2^8)$$

$$z_i^* = \text{mod}(z_i \times 10^{15}, 2^8)$$

The matrix $\mathbf{S}_{QS}$ and sequences $Y^* = \{y_i^*\}$ and $Z^* = \{z_i^*\}$ are converted to the binary with 8 bits. Then the encrypted image is obtained by XOR operator:

$$\mathbf{I}_E = \mathbf{S}_{QS} \oplus [Y^* \oplus Z^*]$$

Finally, the image is converted to the decimal.

In the proposed image encryption, the Lorenz system with two different sets of initial conditions is used to generate six chaotic sequences.

The decryption process and sparse recovery. The decryption process is the inverse operator of the encryption to recover the original image. Here, we assume that the receiver has the initial conditions and step size of the chaotic system to generate random sequences required for the construction of the measurement matrix and the scrambling operators. This process is described as follows:

Step 1: Obtaining $\mathbf{S}_{QS}$ from $\mathbf{I}_E$ by the XOR operator:

$$\mathbf{S}_{\mathbf{Q}\mathbf{S}} = \mathbf{I}_{\mathbf{E}} \oplus [\mathbf{Y}^* \oplus \mathbf{Z}^*]$$

Step 2: After the inverse chaotic confusion of image $\mathbf{S}_{\mathbf{Q}\mathbf{S}}$, the measured matrix $\mathbf{S}_{\mathbf{M}}$ is obtained by the inverse mapping as follows:

$$\mathbf{S}_{\mathbf{M}} = \frac{CC^{-1}\{\mathbf{S}_{\mathbf{Q}\mathbf{S}}\}(\max(\mathbf{S}_{\mathbf{M}}) - \min(\mathbf{S}_{\mathbf{M}}))}{255} + \min(\mathbf{S}_{\mathbf{M}})$$

where $CC^{-1}\{\cdot\}$ is the inverse operator of chaotic confusion. $\max(\mathbf{S}_{\mathbf{M}})$ and $\min(\mathbf{S}_{\mathbf{M}})$ are also gotten from the sender.

Step 3: The sparse matrix $\mathbf{S}_{\mathbf{s}}$ is obtained from the measured matrix $\mathbf{S}_{\mathbf{M}}$ using a sparse reconstruction algorithm based on the 2DSL0 algorithm. In this paper, we improve the performance of sparse recovery by adding total variation (TV) regularization term to the cost function of 2DSL0. This step is investigated in the next subsection.

Step 4: After the inverse chaotic confusion of the sparse matrix $\mathbf{S}_{\mathbf{s}}$, the original image $\mathbf{I}$ is obtained by the inverse transform Ψ (IDWT), and the decryption process is finished.

Sparse recovery based on 2D smoothed ℓ_0 norm and total variation. In this subsection, we propose 2D sparse recovery based on smoothed ℓ_0 norm and total variation. We know that the natural images are usually smooth, hence we add this information to the 2D sparse recovery problem via total variation. To obtain the better performance of sparse reconstruction, the search space of the sparse optimization problem is limited by adding the TV regularization to the cost function of sparse measure. Here, the following definition of TV is used to measure the smoothness of the estimated original image $\hat{\mathbf{I}}$:

$$TV(\hat{\mathbf{I}}) = \sum_{i,j} \left| \frac{\partial \hat{\mathbf{I}}}{\partial x}(i,j) \right| + \left| \frac{\partial \hat{\mathbf{I}}}{\partial y}(i,j) \right| \quad (4)$$

where the image $\hat{\mathbf{I}}$ is the inverse transform of the estimated sparse matrix $\hat{\mathbf{S}}$, i.e. $\hat{\mathbf{I}} = \Psi \hat{\mathbf{S}} \Psi^T$. The absolute function is not differentiable at the origin; hence we replace the absolute function of x with the smoothed function $\sqrt{x^2 + \delta}$ where δ is a small value such as 0.001. The derivative is estimated discretely via forwarding difference. Let the square matrix $\mathbf{D}$ be in the following form:

$$\mathbf{D} = \begin{bmatrix} -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & \ddots & \ddots & 0 \\ 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (5)$$

The derivative of the estimated original image $\hat{\mathbf{I}}$ can be written in the following matrix form:

$$\begin{aligned} \frac{\partial \hat{\mathbf{I}}}{\partial x} &= \mathbf{D}_x \hat{\mathbf{I}} = \mathbf{D}_x \Psi \hat{\mathbf{S}} \Psi^T \\ \frac{\partial \hat{\mathbf{I}}}{\partial y} &= \hat{\mathbf{I}} \mathbf{D}_y^T = \Psi \hat{\mathbf{S}} \Psi^T \mathbf{D}_y^T \end{aligned} \quad (6)$$

where $\mathbf{D}_x \in R^{n_1 \times n_1}$ and $\mathbf{D}_y \in R^{n_2 \times n_2}$ have the form of matrix $\mathbf{D}$. Based on the above definition, the regularized 2D sparse recovery using SL0 is proposed in the following form:

$$\arg \min_{\mathbf{S}_{\mathbf{s}}} J_{\sigma}(\mathbf{S}_{\mathbf{s}}) = \sum_{i,j} \left(1 - \exp \left(-\frac{s_{ij}^2}{2\sigma^2} \right) \right) + \lambda TV(\mathbf{I}), \text{ subject to } \mathbf{S}_{\mathbf{M}} = \Phi_1 \mathbf{S}_{\mathbf{s}} \Phi_2^T, \mathbf{I} = \Psi \times CC^{-1}\{\mathbf{S}_{\mathbf{s}}\} \times \Psi^T \quad (7)$$

where $\lambda > 0$ is the Lagrange coefficient to quantify the trade-off between sparsity in the transform domain and TV. In this problem, to recover the original image, two sparsity constraints are used in two different domains of the transform Ψ and the image gradient. In this optimization, the final two steps of image decryption (Steps 3 and 4) are combined with the TV regularization. Inspired by Refs.^{43,46}, to escape from trapping into local minima, the sparsity measure is optimized iteratively by using a decreasing sequence of σ . The minimizer of $J_{\sigma}(\mathbf{S}_{\mathbf{s}})$ is used as a starting point to minimize $J_{\sigma}(\mathbf{S}_{\mathbf{s}})$ for the smaller σ . To optimize $J_{\sigma}(\mathbf{S}_{\mathbf{s}})$ for a fixed σ subject to the condition $\mathbf{S}_{\mathbf{M}} = \Phi_1 \mathbf{S}_{\mathbf{s}} \Phi_2^T$, the optimizer is based on the steepest descent approach in which each of its iteration ($\mathbf{S}_{\mathbf{s}} \leftarrow \mathbf{S}_{\mathbf{s}} - \mu \nabla_{\mathbf{S}_{\mathbf{s}}} J_{\sigma}(\mathbf{S}_{\mathbf{s}})$) followed by projection onto the feasible set $\{\mathbf{S}_{\mathbf{s}} | \mathbf{S}_{\mathbf{M}} = \Phi_1 \mathbf{S}_{\mathbf{s}} \Phi_2^T\}$. The more details about this optimization approach can be found in the literature^{43,46}. Required gradient of the TV for this optimization can be computed with simple calculations as follows:

$$\begin{aligned}\frac{\partial \left(\frac{\partial \mathbf{I}}{\partial x} \right)}{\partial S_s} &= CC \left\{ \Psi^T D_x^T \hat{S} \Psi \right\} \\ \frac{\partial \left(\frac{\partial \mathbf{I}}{\partial y} \right)}{\partial S_s} &= CC \left\{ \Psi^T \hat{S} D_y \Psi \right\} \\ \hat{S} &= CC^{-1} \left\{ \frac{S_s}{\sqrt{S_s^2 + \delta}} \right\}\end{aligned}\quad (8)$$

To consider the noise effect in the proposed sparse recovery problem, the equality constraint $\mathbf{S}_M = \Phi_1 \mathbf{S}_s \Phi_2^T$ is used in the relaxed form $\mathbf{S}_M - \Phi_1 \mathbf{S}_s \Phi_2^T \leq \epsilon$. Inspired by Ref.⁶⁰, this condition is considered by performing the projection process when the constraint $\mathbf{S}_M - \Phi_1 \mathbf{S}_s \Phi_2^T \leq \epsilon$ is not satisfied. The parameter ϵ is set dependent on the noise level. The image decryption approach based of 2DSL0 and total variation is illustrated in Algorithm 1. The parameters for the proposed approach are empirically selected as follows: $\lambda = 0.01$, $L = 5$, $\mu = 0.5$, $\delta = 0.001$, $\epsilon = 0.001$. The parameter $\sigma = [\sigma_1, \dots, \sigma_J]$ is selected as $\sigma_1 = \max \left(\left| \hat{S}_{s0} \right| \right)$, and $\sigma_j = \sigma_1 (1 - 0.003j)$ which is a geometric decreasing sequence.

Algorithm. 1 The proposed sparse recovery based on 2DSL0 and total variation for the decryption process;

<p>Inputs: $\mathbf{S}_M, \Phi_1, \Phi_2, CC\{.\}, CC^{-1}\{.\}$</p> <p>Initialization:</p> <p>(1) Choose a suitable decreasing sequence for $\sigma = [\sigma_1, \dots, \sigma_J]$</p> <p>(2) $\hat{S}_{s0} = \Phi_1^T (\Phi_1 \Phi_1^T)^{-1} \mathbf{S}_M (\Phi_2^T (\Phi_2 \Phi_2^T)^{-1})^T$</p> <p>For $j = 1, \dots, J$</p> <p>(1) $\sigma = \sigma_j$</p> <p>(2) Initialization: $\mathbf{S} = \hat{S}_{sj}$</p> <p>(3) For $l = 1 \dots L$ (loop L times)</p> <p>(a) Let $\Delta_s = [\delta_{ij}]$, where $\delta_{ij} = s_{ij} \exp \left(-\frac{s_{ij}^2}{2\sigma^2} \right)$.</p> <p>(b) Let $\Delta_x = CC \left\{ \Psi^T D_x^T \times CC^{-1} \left\{ \frac{S}{\sqrt{S^2 + \delta}} \right\} \times \Psi \right\}$</p> <p>(c) Let $\Delta_y = CC \left\{ \Psi^T \times CC^{-1} \left\{ \frac{S}{\sqrt{S^2 + \delta}} \right\} \times D_y \Psi \right\}$</p> <p>(d) Let $\mathbf{S} \leftarrow \mathbf{S} - \mu \left(\Delta_x + \lambda (\Delta_x + \Delta_y) \right)$ (μ is a small positive constant).</p> <p>(e) Projection $\mathbf{S}$ onto the feasible set $\{\mathbf{S} \mathbf{S}_M = \Phi_1 \mathbf{S} \Phi_2^T\}$</p> <p>• If $\ \mathbf{S}_M - \Phi_1 \mathbf{S} \Phi_2^T\ _F > \epsilon$</p> <p>$\mathbf{S} \leftarrow \mathbf{S} - \Phi_1^T (\Phi_1 \Phi_1^T)^{-1} (\Phi_1 \mathbf{S} \Phi_2^T - \mathbf{S}_M) (\Phi_2^T (\Phi_2 \Phi_2^T)^{-1})^T$</p> <p>End if</p> <p>End for</p> <p>End For</p> <p>Outputs: $\hat{S} = \hat{S}_j$, $\hat{\mathbf{I}} = \Psi \times CC^{-1}\{\hat{S}\} \times \Psi^T$</p>

Experimental results

In this section, the proposed method is evaluated by different measures. All the experiments are performed on a personal computer with Intel Core i7 2.2 GHz and 8 GB RAM. The images of Cameraman, Pepper, Baboon and Brain with a size of 256×256 are used for evaluation. The DWT is used as a sparsifying transform. In the simulations, the parameters of the Lorenz system are constant as $\sigma = 10$, $\beta = \frac{8}{3}$ and $\rho = 28$, respectively. The initial values of the two Lorenz systems are $[x_{01}, y_{01}, z_{01}] = [-0.823, 3.423, 0.178]$ and $[x_{02}, y_{02}, z_{02}] = [-1.804, -0.631, -1.512]$, respectively.

To evaluate the quality of the decrypted image, we use two measures of the peak signal-to-noise ratio PSNR and the mean square deviation MSE defined as follows:

$$\begin{aligned}MSE &= \frac{1}{n_1 n_2} \sum_{i,j} \left(\mathbf{I}(i,j) - \hat{\mathbf{I}}(i,j) \right)^2 \\ PSNR &= 10 \log_{10} \left(\frac{255^2}{MSE} \right)\end{aligned}\quad (9)$$

where $\mathbf{I} \in R^{n_1 \times n_2}$ and $\hat{\mathbf{I}} \in R^{n_1 \times n_2}$ are the original image and the decrypted image, respectively. Figure 3 shows the results of image encryption for test images. In these examples, the histogram of the original image and encrypted image is also shown. These results indicate that all images have the same results visually and statistically. The decrypted images also have an acceptable quality.

Figure 3. Experimental results: (a1–a4) original images; (b1–b4) the corresponding histograms of the original images; (c1–c4) the corresponding encrypted images of the original images; (d1–d4) the corresponding histograms of the encrypted images; (e1–e4) the corresponding decrypted images; Cameraman is used from the website <https://homepages.cae.wisc.edu/~ece533/images/>; Pepper and Baboon are used from the website <http://sipi.usc.edu/database/>; Brain scan is used from the website <https://medicalxpress.com/news/2017-02-mri-brain-scans-adolescent-substance.html>.

Figure 4. Performance of the sparse reconstruction approaches with considering the effects of TV and chaotic confusion in the encryption process: The PSNR values of the decrypted test images for different CRs.

Compression ratio	0.1	0.3	0.5	0.7
2DSL0	4.4	6.9	9.1	10.6
2DOMP	5.1	22.4	284.1	3753
2DPG	102.6	104.3	105.7	105.4
Proposed method	22.4	27.1	30.3	33.6

Table 1. The computation time (s) for the different compression ratios.

Compression performance. In this section, the decrypted image quality is evaluated for different compression ratios based on the PSNR measure. In the proposed method, to obtain better performance of the image reconstruction, two techniques are used. The first one is based on the uniqueness analysis. The chaotic confusion is applied to the sparse representation of the original image. Also, TV is added to the cost function of sparse recovery. Here, the effect of these terms on the quality of the decrypted image is investigated. Figure 4 shows the PSNR value for different CRs. Here, the proposed approach is also compared with 2DOMP⁵⁷ and 2DPG⁵⁸ algorithms. We also evaluate the effect of chaotic confusion on these reconstruction approaches. The reconstruction results demonstrate that the technique of chaotic confusion improves the reconstruction performances of 2DSL0, 2DOMP, and 2DPG methods, especially for small compression ratios. These curves show that the image

Image	Compression ratio	Proposed method	Ref. ⁴⁵	Ref. ³⁰	Ref. ⁴⁰	Ref. ²⁶
Cameraman	0.25	29.58	–	–	25.23	24.24
	0.50	34.97	≈ 25.08	≈ 25.64	29.43	30.66
	0.75	38.61	26.81	27.45	28.93	31.08
Pepper	0.50	37.03	≈ 27.33	≈ 27.94	–	32.09
	0.75	39.70	28.67	29.19	–	–

Table 2. PSNR (dB) values of the encrypted images with different approaches for the different compression ratios.

recovery quality has been enhanced with two applied techniques in 2D sparse representation. The proposed approach outperforms 2D-OMP and 2DPG reconstruction methods. Here, we also present the average computation time to compare the computational complexity of different reconstruction approaches in Table 1. Since the runtime depends on the programming skill and the programming languages, this criterion is not appropriate for a computation cost comparison.

Table 2 presents the performance of different schemes based on compressed sensing in comparison with the proposed approach. It can be seen that the proposed encryption approach has a better performance for the same CR. Table 3 shows the performance of the decrypted images for different CRs visually. The qualities are entirely acceptable.

Performance evaluation of the proposed measurement matrix. In this section, we evaluate the effectiveness of the proposed measurement matrix. This matrix is a partial orthogonal matrix generated by the chaotic sequence and SVD. Here, we compare the proposed measurement matrix with the partial Hadamard matrix and the Gaussian random matrix. Partial Hadamard matrix, a famous measurement matrix, has been used in encryption schemes^{22,35,38,39,45}. Table 4 shows the effectiveness of these measurement matrices in the proposed encryption process for the different CRs. It can be observed that the proposed measurement matrix has better performance than the Gaussian matrix in this application. Also, this presents similar PSNR values compared with that of the partial Hadamard matrix. Therefore, the proposed measurement matrix achieves good performance and effectiveness in compressed sensing and increases image encryption security.

Security performance analyses. In this section, the security performance of the proposed approach is analyzed by two measures. The initial value of the chaotic system is keystream used to encrypt different images. To increase the image encryption security level in different attacks, it is appropriate to generate a keystream related to the original image. To obtain this purpose, many approaches can be proposed. For example, inspired by Ref.³⁰, we can use the SHA-256 hash value of the original image to generate the chaotic system's initial value. Hence, when different images are encrypted, the corresponding measurement matrices and chaotic confusion operators are different. This can ensure that the proposed approach can resist various attacks, such as the chosen-plaintext attack, which is the strongest attack.

Key sensitivity. The key sensitivity analysis shows the effect of a tiny difference between decryption and encryption keys on the quality of the decrypted image. In a secure cryptosystem, a tiny variation in the secret key causes to obtain a decrypted image, which is entirely different from the original image. In the proposed approach, the sensitivity of the chaotic system to the initial conditions results in a secure scheme to the keys $[x_{01}, y_{01}, z_{01}, x_{02}, y_{02}, z_{02}]$. Figure 5 shows the decrypted Cameraman images for different wrong keys. In each key set, only one key has a tiny variation of 10^{-15} , and the other keys are correct. It is obvious that the decrypted image has been significantly distorted. Figure 6 illustrates the key sensitivity based on the MSE measure for the variation of each key. It can be seen that the minimum of MSE is obtained when the keys are correct. Put it in a nutshell, the proposed method is highly sensitive to the secret keys.

Key space. An essential requirement of a secure cryptosystem is the key space. The larger key space makes the brute force attack infeasible. According to the research⁶¹, the key space should be larger than 2^{100} . The precision of the double-precision number is about 10^{-15} . Therefore, the total key space of the proposed encryption approach is $(10^{15})^6 = 10^{90} \approx 2^{300}$ which is large enough. This key space prevents the exhaustive searching. Table 5 compares the key space of different approaches.

Original Image	Compression Ratio	Encrypted Image	Decrypted Image	PSNR (dB)
0.1			24.40
	0.25			29.56
	0.75			39.65
0.1			23.23
	0.25			28.45
	0.75			38.51

Table 3. The results of different compression ratios.

Image	CR	Proposed measurement matrix	Gaussian random matrix	Partial hadamard matrix
Cameraman	0.1	24.40	23.50	24.59
	0.3	30.83	28.18	30.71
	0.5	34.97	29.66	35.66
Pepper	0.1	26.25	25.19	25.97
	0.3	33.46	29.39	32.79
	0.5	37.03	30.46	37.80
Baboon	0.1	22.48	22.38	22.03
	0.3	25.21	24.25	24.87
	0.5	28.03	25.47	27.86
Brain	0.1	23.23	22.19	22.99
	0.3	29.75	28.80	29.21
	0.5	33.90	29.34	34.02

Table 4. PSNR (dB) values of the encrypted images with different measurement matrices.

Figure 5. Decrypted Cameraman image with incorrect keys: (a) decrypted image with $x_{01} + 10^{-15}$; (b) decrypted image with $y_{01} + 10^{-15}$; (c) decrypted image with $z_{01} + 10^{-15}$; (d) decrypted image with $x_{02} + 10^{-15}$; (e) decrypted image with $y_{02} + 10^{-15}$; (f) decrypted image with $z_{02} + 10^{-15}$.

Statistical analyses. In this subsection, the effectiveness of the proposed encryption scheme is investigated from the statistical viewpoint.

Histogram. A histogram is a measure to evaluate the performance of the encryption approach. An appropriate histogram of a secure cryptosystem is a uniform distribution that makes the encryption process resistant to the statistical attack. Figure 3 shows the histograms of original and encrypted images. It can be seen that the pro-

Figure 6. MSE curves concerning the variation of each key: (a) $x_{01} + \delta_{x1}$; (b) $y_{01} + \delta_{y1}$; (c) $z_{01} + \delta_{z1}$; (d) $x_{02} + \delta_{x2}$; (e) $y_{02} + \delta_{y2}$; (f) $z_{02} + \delta_{z2}$.

Algorithm	Proposed method	Ref. ⁴⁵	Ref. ³⁰	Ref. ⁴⁰	Ref. ²⁶
Key space	2^{300}	2^{276}	2^{300}	2^{232}	2^{398}

Table 5. Key space of the proposed method and other approaches.

	Original image	Encrypted image
Cameraman	7.0097	7.9945
Pepper	7.7721	7.9949
Baboon	7.5703	7.9941
Brain	6.9868	7.9939

Table 6. The entropy of the original and encrypted images.

posed method changes approximately the histogram of all test images to the uniform. These results demonstrate the effectiveness of the proposed approach.

Entropy. Information entropy is another measure to calculate the randomness of the encrypted image. The larger value of entropy means the better performance of encrypted images. For a discrete variable, the Shannon entropy is maximized for the uniform distribution. The maximum value is equal to $\log_2 M$ where M is the number of discrete variable states. In the encryption scheme, this value is equal to 8 by considering 8 bits for each pixel. Table 6 shows the entropy of the original and encrypted images for $CR = 0.5$. The results describe that the entropy after encryption is approximately equal to the ideal value.

Figure 7. The correlation distribution of two adjacent pixels in the horizontal direction for the original and encrypted images. (a) Original “Cameraman”; (b) encrypted “Cameraman”; (c) original “Pepper”; (d) encrypted “Pepper”; (e) original “Baboon”; (f) encrypted “Baboon”; (g) original “Brain”; (h) encrypted “Brain”.

Image	Algorithms	Horizontal	Vertical	Diagonal
Cameraman	Original image	0.9592	0.9337	0.9079
	Proposed method	0.0014	− 0.0044	− 0.0031
	Ref. ⁴⁵	−	−	−
	Ref. ³⁶	− 0.0044	− 0.0054	0.0025
	Ref. ²⁶	0.0040	− 0.0027	− 0.0084
Pepper	Original image	0.9714	0.9644	0.9388
	Proposed method	0.0033	− 0.0016	− 0.000058
	Ref. ⁴⁵	− 0.0005	− 0.0062	0.0036
	Ref. ³⁶	0.0074	0.0035	0.0041
	Ref. ²⁶	− 0.0117	0.0039	− 0.0012

Table 7. Correlation coefficients of adjacent pixels.

Correlation. Two previous measures investigate the uniformity of the distribution while they do not calculate the correlation among pixels. For a natural image, there is a high correlation between adjacent pixels in all directions. The minimum correlation among pixels is appropriate for secure image encryption. Figure 7 shows the joint distribution of adjacent pixels in the horizontal direction for the original and encrypted images. These distributions show that the correlation between pixels of the encrypted images is reduced effectively. A measure to quantify the relation between the adjacent pixels of the image is the correlation coefficient (CC). Table 7 presents the CC values of different schemes in three directions for comparison. The results show that the proposed encryption method reduces the correlation between pixels, and has better performance.

Robustness analysis. *Noise attack.* Images are usually affected by different noise models in the transmission process. Here, we evaluate the robustness of the proposed approach in the presence of different noise attacks such as Gaussian noise (GN), speckle noise (SN), and salt and pepper noise (SPN). In this simulation, the Cameraman image is used as a test image, and $CR = 0.5$. Figure 8 presents decrypted images in the presence of noise attacks with different intensities. The recovery performance of the proposed encryption approach is shown in Fig. 9 for different noise intensities. We can conclude that: (1) Gaussian noise has the largest effect on the recovery performance, (2) there is a certain robustness to the SN attack, (3) the proposed scheme has the strongest robustness to the SPN attack. These results show that the proposed encryption method has a good ability to recover the original image in the presence of the noise attack.

Cropping attack. An essential challenge in image transmission is the cropping attack in which some pixels of the encrypted image are loosed. Since the proposed image encryption is based on compressed sensing, our approach is robust against data loss and can effectively recover the original image. The proposed approach's performance is evaluated for different cropping masks, and results are shown in Fig. 10. The decrypted images and their PSNR demonstrate the robustness of the proposed method in the presence of a cropping attack.

Conclusion

In this paper, an image cryptosystem was proposed based on two-dimensional sparse recovery to simultaneously achieve encryption and compression. Based on the compressed sensing theory, the original image was compressed via two measurement matrices. To improve the performance of image recovery, a chaotic confusion was added before compression. Also, the total variation was used in the sparse recovery problem based smoothed ℓ_0 norm. The security level was increased by chaotic scrambling and XOR operations. Statistical analyses have shown that the proposed cryptosystem has ample key space, high sensitivity to the tiny variation in the key, maximum entropy, uniform distribution of the encrypted image, and weak correlation between adjacent pixels. These features have demonstrated the robustness of the proposed approach against the statistical analysis and brute-force attack. The simulation results have illustrated that the proposed cryptosystem has high security and excellent compression performance. The proposed approach was also adequately robust against the noise and cropping attacks because of considering the chaotic confusion and the total variation in the two-dimensional sparse recovery. Future work will focus on improving the compression ratio performance based on the dictionary learning to obtain the sparse representation.

Figure 8. Encrypted images and decrypted images in the presence of GN, SN, and SPN with different levels of noise.

Figure 9. PSNR between decrypted images and original images with different noises.

Figure 10. Result of cropping attacks: (a–d) encrypted images with different cropping attacks; (e–h) the decrypted images from (a–d), respectively.

Received: 3 June 2020; Accepted: 10 December 2020

Published online: 11 January 2021

References

1. Bouslimi, D. *et al.* A joint encryption/watermarking system for verifying the reliability of medical images. *IEEE Trans. Inf. Technol. Biomed.* **16**, 891–899 (2012).
2. Haddad, S. *et al.* Joint watermarking-encryption-JPEG-LS for medical image reliability control in encrypted and compressed domains. *IEEE Trans. Inf. Foren. Secur.* **15**, 2556–2569 (2020).
3. Pareek, N. K., Patidar, V. & Sud, K. K. Image encryption using chaotic logistic map. *Image Vis. Comput.* **24**, 926–934 (2006).
4. Wang, R.-Z., Lin, C.-F. & Lin, J.-C. Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recogn.* **34**, 671–683 (2001).
5. Chen, G., Mao, Y. & Chui, C. K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fractals* **21**, 749–761 (2004).
6. Ge, R. *et al.* A novel Chaos-based symmetric image encryption using bit-pair level process. *IEEE Access* **7**, 99470–99480 (2019).
7. Farah, M. B. *et al.* A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. *Opt. Laser Technol.* **121**, 105777 (2020).
8. Zhang, Y. & Wang, B. Optical image encryption based on interference. *Opt. Lett.* **33**, 2443–2445 (2008).
9. Chai, X. *et al.* A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process.* **155**, 44–62 (2019).
10. Belazi, A. *et al.* Novel medical image encryption scheme based on chaos and DNA encoding. *IEEE Access* **7**, 36667–36681 (2019).
11. Boussif, M., Aloui, N. & Cherif, A. Images encryption algorithm based on the quaternion multiplication and the XOR operation. *Multimed. Tools Appl.* **78**, 35493–35510 (2019).

12. Nag, A., Singh, J.P., Khan, S., et al. Image encryption using affine transform and XOR operation. 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies: IEEE 2011, pp. 309–312.
13. Hu, W.-W. et al. Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms. *Quantum Inf. Process.* **19**, 1–29 (2020).
14. Abd El-Latif, A. A. et al. Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. *Sci. Rep.* **10**, 1–16 (2020).
15. Chen, H. et al. Dual paths cryptosystem based on tilt Fresnel diffraction using non-spherical mirror and phase modulation in expanded fractional Fourier transform domain. *Sci. Rep.* **9**, 1–7 (2019).
16. Yang, Y.-G. et al. Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. *Sci. Rep.* **6**, 19788 (2016).
17. Gan, Z.-h et al. A chaotic image encryption algorithm based on 3-D bit-plane permutation. *Neural Comput. Appl.* **31**, 7111–7130 (2019).
18. Wang, X.-Y. et al. A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dyn.* **62**, 615–621 (2010).
19. Li, S., Zheng, X.. Cryptanalysis of a chaotic image encryption method. 2002 IEEE International Symposium on Circuits and Systems Proceedings (Cat No 02CH37353): IEEE 2002:II-II.
20. El-Latif, A. A. A. et al. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. *Signal Process.* **93**, 2986–3000 (2013).
21. Chai, X. et al. A visually secure image encryption scheme based on compressive sensing. *Signal Process.* **134**, 35–51 (2017).
22. Ye, G., Pan, C., & Dong, Y., et al. Image encryption and hiding algorithm based on compressive sensing and random numbers insertion. *Signal Process.* 107563 (2020).
23. Gan, Z., Chai, X., & Zhang, J., et al. An effective image compression–encryption scheme based on compressive sensing (CS) and game of life (GOL). *Neural Comput. Appl.* 1–29 (2020).
24. Donoho, D. L. Compressed sensing. *IEEE Trans. Inf. Theory* **52**, 1289–1306 (2006).
25. Li, J. et al. Compressive optical image encryption. *Sci. Rep.* **5**, 10374 (2015).
26. Xu, Q. et al. An effective image encryption algorithm based on compressive sensing and 2D-SLIM. *Opt. Lasers Eng.* **134**, 106178 (2020).
27. Chai, X. et al. Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy. *Signal Process.* **171**, 107525 (2020).
28. Chai, X. et al. An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding. *Opt. Lasers Eng.* **124**, 105837 (2020).
29. Hu, G. et al. An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications. *J. Vis. Commun. Image Represent.* **44**, 116–127 (2017).
30. Zhu, S., Zhu, C. & Wang, W. A novel image compression-encryption scheme based on chaos and compression sensing. *IEEE Access* **6**, 67095–67107 (2018).
31. Chen, J. et al. Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression. *Opt. Laser Technol.* **99**, 238–248 (2018).
32. Li, X. et al. Joint image compression and encryption based on sparse Bayesian learning and bit-level 3D Arnold cat maps. *PLoS ONE* **14**, 1 (2019).
33. Zhou, N. et al. Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging. *Opt. Lasers Eng.* **110**, 72–79 (2018).
34. Fan, J.-H., Liu, X.-B. & Chen, Y.-B. Image compression and encryption algorithm with wavelet-transform-based 2D compressive sensing. *Opt. Appl.* **49**, 1 (2019).
35. Ponuma, R. & Amutha, R. Image encryption using sparse coding and compressive sensing. *Multidimension. Syst. Signal Process.* **30**, 1895–1909 (2019).
36. Luo, Y. et al. A robust image encryption algorithm based on Chua's circuit and compressive sensing. *Signal Process.* **161**, 227–247 (2019).
37. Chai, X., Fu, X., & Gan, Z., et al. An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata. *Neural Comput. Appl.* 1–28 (2018).
38. Zhu, L. et al. A novel image encryption scheme based on nonuniform sampling in block compressive sensing. *IEEE Access* **7**, 22161–22174 (2019).
39. Deng, J. et al. Image compression-encryption scheme combining 2D compressive sensing with discrete fractional random transform. *Multimedia Tools Appl.* **76**, 10097–10117 (2017).
40. Chai, X. et al. An image encryption algorithm based on chaotic system and compressive sensing. *Signal Processing* **148**, 124–144 (2018).
41. Zhang, Y. et al. Embedding cryptographic features in compressive sensing. *Neurocomputing* **205**, 472–480 (2016).
42. Chen, T. et al. Image encryption and compression based on kronecker compressed sensing and elementary cellular automata scrambling. *Opt. Laser Technol.* **84**, 118–133 (2016).
43. Ghaffari, A., Babaie-Zadeh, M., Jutten, C. Sparse decomposition of two dimensional signals. 2009 IEEE International Conference on Acoustics, Speech and Signal Processing: IEEE 2009, pp. 3157–3160.
44. Duarte, M. F. & Baraniuk, R. G. Kronecker compressive sensing. *IEEE Trans. Image Process.* **21**, 494–504 (2011).
45. Zhou, N. et al. Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing. *Opt. Laser Technol.* **82**, 121–133 (2016).
46. Mohimani, H., Babaie-Zadeh, M. & Jutten, C. A fast approach for overcomplete sparse decomposition based on smoothed ℓ^1 norm. *IEEE Trans. Signal Process.* **57**, 289–301 (2008).
47. Aharon, M., Elad, M. & Bruckstein, A. K-SVD: An algorithm for designing overcomplete dictionaries for sparse representation. *IEEE Trans. Signal Process.* **54**, 4311–4322 (2006).
48. Gribonval, R., Lesage, S. A survey of sparse component analysis for blind source separation: principles, perspectives, and new challenges. 2006.
49. Wright, J. et al. Robust face recognition via sparse representation. *IEEE Trans. Pattern Anal. Mach. Intell.* **31**, 210–227 (2008).
50. Ghaffari, A. & Fatemizadeh, E. Sparse-induced similarity measure: mono-modal image registration via sparse-induced similarity measure. *IET Image Proc.* **8**, 728–741 (2014).
51. Ghaffari, A. & Fatemizadeh, E. Robust Huber similarity measure for image registration in the presence of spatially-varying intensity distortion. *Signal Process.* **109**, 54–68 (2015).
52. Gribonval, R. & Nielsen, M. Sparse decompositions in unions of bases. *IEEE Trans. Inform Theory* **49**, 3320–3325 (2003).
53. Mallat, S. G. & Zhang, Z. Matching pursuits with time-frequency dictionaries. *IEEE Trans. Signal Process.* **41**, 3397–3415 (1993).
54. Chen, S. S., Donoho, D. L. & Saunders, M. A. Atomic decomposition by basis pursuit. *SIAM Rev.* **43**, 129–159 (2001).
55. Eftekhari, A., Babaie-Zadeh, M. & Moghaddam, H. A. Two-dimensional random projection. *Signal Process.* **91**, 1589–1603 (2011).
56. Jökar, S. & Mehrmann, V. Sparse solutions to underdetermined Kronecker product systems. *Linear Algebra Appl.* **431**, 2437–2447 (2009).
57. Fang, Y., Wu, J. & Huang, B. 2D sparse signal recovery via 2D orthogonal matching pursuit. *Sci. China Inf. Sci.* **55**, 889–897 (2012).

58. Chen, G., Li, D. & Zhang, J. Iterative gradient projection algorithm for two-dimensional compressive sensing sparse image reconstruction. *Signal Process.* **104**, 15–26 (2014).
59. Lorenz, E. N. Deterministic nonperiodic flow. *J. Atmos. Sci.* **20**, 130–141 (1963).
60. Eftekhari, A., Babaie-Zadeh, M., Jutten, C., et al. Robust-SL0 for stable sparse representation in noisy settings. 2009 IEEE International Conference on Acoustics, Speech and Signal Processing: IEEE 2009, pp. 3433–3436.
61. Alvarez, G. & Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifur. Chaos* **16**, 2129–2151 (2006).

Author contributions

A.G. developed the algorithm and codes, wrote the manuscript and prepared the figures, and also revised the manuscript.

Competing interests

The author declares no competing interests.

Additional information

Correspondence and requests for materials should be addressed to A.G.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2021