Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.050337

ARTICLE

Chaotic CS Encryption: An Efficient Image Encryption Algorithm Based on Chebyshev Chaotic System and Compressive Sensing

Mingliang Sun, Jie Yuan*, Xiaoyong Li and Dongxiao Liu

Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education, Beijing University of Posts and Telecommunications, Beijing, 100876, China

*Corresponding Author: Jie Yuan. Email: yuanjie@bupt.edu.cn

Received: 03 February 2024 Accepted: 03 April 2024 Published: 15 May 2024

ABSTRACT

Images are the most important carrier of human information. Moreover, how to safely transmit digital images through public channels has become an urgent problem. In this paper, we propose a novel image encryption algorithm, called chaotic compressive sensing (CS) encryption (CCSE), which can not only improve the efficiency of image transmission but also introduce the high security of the chaotic system. Specifically, the proposed CCSE can fully leverage the advantages of the Chebyshev chaotic system and CS, enabling it to withstand various attacks, such as differential attacks, and exhibit robustness. First, we use a sparse trans-form to sparse the plaintext image and then use the Arnold transform to perturb the image pixels. After that, we elaborate a Chebyshev Toeplitz chaotic sensing matrix for CCSE. By using this Toeplitz matrix, the perturbed image is compressed and sampled to reduce the transmission bandwidth and the amount of data. Finally, a bilateral diffusion operator and a chaotic encryption operator are used to perturb and expand the image pixels to change the pixel position and value of the compressed image, and ultimately obtain an encrypted image. Experimental results show that our method can be resistant to various attacks, such as the statistical attack and noise attack, and can outperform its current competitors.

KEYWORDS

Image encryption; chaotic system; compressive sensing; arnold transform

1 Introduction

With the advancement of technology and the continuous development of society, modern individuals are increasingly concerned about the security of information and data. As the primary medium for conveying information, the security of digital images is of paramount importance, encompassing not only personal data but also sensitive areas such as military, political, medical, and commercial domains. Consequently, the encrypted transmission of image information has emerged as a rapidly growing and intriguing field, garnering significant attention within the realms of image processing, data transmission, and computer science [1–4].

Unlike text encryption technology, image encryption techniques often possess unique characteristics, such as high pixel correlation and substantial data storage requirements. Traditional encryption methods typically encompass the advanced encryption standard (AES) [5], international data encryption algorithm (IDEA) [6], and data encryption standard (DES) [7]. However, due to the distinctive features of images, these methods are generally unsuitable for image encryption. Consequently, numerous researchers have proposed various methods to mitigate redundancy in image content during encryption, such as chaos-based encryption methods.

Chaos theory is a method that involves both qualitative discussion and quantitative analysis to examine the characteristics of dynamic systems, such as chemical reactions, weather changes, and social behaviors. It was initially proposed by the meteorologist Lorenz and later rigorously defined mathematically by Li et al. in 1975 [8]. Subsequently, Feigenbaum summarized the universality of common characteristics of chaotic mapping systems, such as the ergodic theorem [9]. Following these developments, chaos theory began to be applied in various fields, including weather forecasting and the study of social behavior. Since then, researchers in diverse disciplines have sought to uncover correlations among internal elements from various irregular phenomena [10,11]. Consequently, chaos has become a prominent research topic.

It is well-known that chaotic systems exhibit several characteristic properties, including pseudo-randomness, ergodicity, unpredictability, and sensitivity to initial conditions and system parameters. These attributes make chaotic systems a promising alternative to traditional image encryption algorithms [12]. Additionally, chaotic systems offer a large key space and can be efficiently implemented in parallel using hardware. Motivated by these advantages, researchers have introduced several chaos-based approaches for image encryption [13–17]. For instance, Talhaoui et al. proposed a real-time image encryption framework utilizing their fractional one-dimensional chaotic map, which significantly enhances both the security and speed of encryption [13]. Tamang et al. utilized chaotic ion-acoustic waves in space plasma to develop a robust image encryption method. By incorporating SHA-512 hash computation and DNA coding, the proposed encryption method demonstrates high resistance against various decryption techniques [18].

While chaotic-based encryption algorithms often exhibit strong encryption performance, it is important to acknowledge that the image encryption process typically involves compression operations for image transmission or storage [19]. Additionally, the order of encryption and compression directly impacts the overall efficiency of digital image performance. For example, encrypted image data may not be compressible [20], posing a challenge in balancing security and compression performance. Common image compression techniques, such as discrete wavelet transform, Fourier transform, and the joint photographic experts group (JPEG) standard, may affect encryption effectiveness. For instance, the size of encrypted bitstreams may vary in JPEG-based compression-encryption approaches due to the removal of JPEG marker codes [21]. To address this challenge, many researchers have proposed encryption-then-compression (ETC) frameworks that aim to satisfy both requirements. However, compared to state-of-the-art image coders without encryption, existing ETC methods often exhibit lower performance [22]. Furthermore, the security of these approaches is susceptible to attacks from jigsaw puzzle solvers when dealing with large images. This issue may arise from the perception of compression and encryption as distinct operations.

As a result, integrating compression into image encryption has become an intriguing topic. Building upon this foundation, several methods based on number theory and chaotic theory have been proposed for image encryption [23,24]. However, these encryption algorithms may be susceptible to plaintext and differential attacks, and the achievable compression may be marginal or even negative [25]. Recently, Candes et al. introduced a sampling and compression framework known as compressive sensing (CS), which overcomes the limitations of the Nyquist sampling theorem [26]. Given the high correlation among adjacent pixels and the strong redundancy in images, several CS-based image encryption methods have emerged [27,28], enabling encryption and compression during the image sampling process. Moreover, the choice of sensing matrix plays a crucial role in these encryption schemes. For instance, Chai et al. proposed an efficient image encryption method based on CS using chaotic principles [27]. Although this encryption algorithm demonstrates effective encryption, it may increase transmission costs due to the utilization of Gaussian random sampling matrices. More recently, some researchers have demonstrated that chaotic sensing matrices can not only ensure the sampling efficiency of CS but also reduce memory complexity, making them easily implementable in software and hardware [29–31]. Consequently, a natural question arises: Can we develop an efficient image encryption algorithm directly based on chaotic systems and CS?

To address this query, we propose a novel image encryption algorithm named chaotic CS encryption (CCSE) in this paper, which combines the strengths of the Chebyshev chaotic system and CS. Our proposed CCSE exhibits resilience against various attacks, including statistical and noise attacks, and outperforms current competitors in terms of performance. Additionally, CCSE can be readily implemented in both software and hardware. The proposed CCSE algorithm first employs a sparse transform to sparsify the plaintext image, followed by applying the Arnold transform to perturb the image pixels. Subsequently, we design a Chebyshev Toeplitz chaotic sensing matrix, which significantly reduces memory and computational complexity and can be easily implemented in hardware. Utilizing the customized Chebyshev Toeplitz sensing matrix, we sample and compress the perturbed image to reduce transmission bandwidth and data volume. Finally, a bilateral diffusion operator and a chaotic encryption operator are utilized to perturb and expand the image pixels, altering both the pixel position and value of the compressed image, thereby producing the encrypted image. The main contributions of this paper are summarized as follows:

(1) We propose a novel image encryption algorithm based on Chebyshev chaotic system and CS, which can not only improve the efficiency of image transmission, but also introduce the high security.

(2) We introduce a Chebyshev Toeplitz chaotic sensing matrix to sample and compress the perturbed image for image encryption, which can obtain considerable encryption and compression performance in the proposed CCSE framework.

(3) We verify that the proposed CCSE algorithm is highly secure and effective through abundant numerical tests, including histogram, robustness, correlation analysis, and statistical attack.

The rest of this paper is organized as follows. Section 2 introduces the related work. Section 3 designs the proposed CCSE framework. Section 4 shows the experimental evaluation. Section 5 concludes the work.

2 Related Work

2.1 Chebyshev Chaotic Systems

Chebyshev chaotic system of degree μ is defined as:

$$z_{i+1} = \tau(z_i) = \cos(\mu \cdot \arccos(z_i)), \tag{1}$$

where $z_i = \tau^i(z_0)$ $(i \in N)$, z_0 is a seed and $-1 \leq z_0 \leq 1$, $1 < \mu \in N^+$.

By iterating Eq. (1), we can obtain a set of Chebyshev chaotic sequence $\{z_i\}_{i=0}^{\infty}$. It is well-known that $\{z_i\}_{i=0}^{\infty}$ has the following characteristic: Mean $E(z) = 0$ and variance $\delta^2(z) = 0.5$. Let $d \in N^+$ denote the sampling step size of $\{z_i\}_{i=0}^{\infty}$. Then the $i^{th}(i \in N^+)$ moment z_i and $(i+d)^{th}$ moment z_{i+d} of the

Chebyshev chaotic sequence $\{z_i\}_{i=0}^{\infty}$ can be treated as approximately independent. Fig. 1 illustrates the joint probability function for $\{z_i\}_{i=0}^{\infty}$ with $d = 6$.

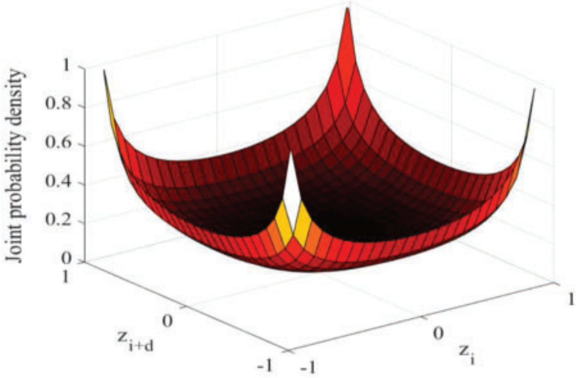


Figure 1: Joint probability function for Chebyshev chaotic sequence $\{z_i\}_{i=0}^{\infty}$, where $d = 6$ denotes the sampling step size

Moreover, Gan et al. have verified that the Chebyshev map's transient time is zero, which indicates that the Chebyshev's sequence $\{z_i\}_{i=0}^{\infty}$ can better build the chaotic sensing matrix [29]. Note that other chaotic systems may exhibit transient time, which can affect the speed at which the chaotic system reaches a stable state, consequently rendering the chaotic sequence unsuitable for constructing a sensing matrix, such as Tent and Logistic chaotic systems. In addition, the Chebyshev chaotic sequence possesses several advantages, including its excellent ergodicity, low sensitivity to initial conditions, superior statistical properties, and wide chaotic range, making it well-suited for applications in various fields, such as secure communications and pseudo-random number generation. As a result, we can use the Chebyshev chaotic sequence $\{z_i\}_{i=0}^{\infty}$ to customize the Toeplitz Chebyshev chaotic sensing matrix for our proposed CCSE framework, which can not only obtain considerable encryption and compression performance during the image sampling process, but also reduce memory consumption in hardware and software implementation due to the Toeplitz Chebyshev chaotic matrix has the following advantages: 1) efficient multiplication support using the FFT algorithm, leading to accelerated image acquisition and recovery; 2) a well-structured Toeplitz architecture that aligns with practical hardware implementation; and 3) a notable reduction in memory requirements.

2.2 Chaotic-Based Image Encryption Methods

As mentioned in the introduction, strengthening security and enforcing authorized access to sensitive data is the major challenge for digital image services. A straightforward solution to this problem is to make the image less intuitive. To this end, different chaotic-based image encryption methods have been introduced for image security in recent years [13–17,32–34].

For example, Enayatifar et al. designed a chaos-based image encryption by using a hybrid model based on a Logistic chaotic system and deoxyribonucleic acid (DNA) masking [17]. Similar to this work, Zhen et al. proposed a secure image encryption method based on Logistic and spatiotemporal chaotic systems [33]. Due to the extreme sensitivity of chaotic system, the proposed approach can greatly increase the complexity of the cracking algorithm. Motivated by this work, Wang et al. then introduced an image encryption algorithm using cycle shift and chaotic system. The proposed method is proven to be capable of defending against attacks [16]. Following this work, Talhaoui and Wang introduced a real-time image encryption scheme by using their fractional one-dimensional chaotic map, which can significantly improve the security and speed of encryption [13]. To increase the security performance, Alawida et al. designed a hybrid chaotic system, and then applied this chaotic system to image encryption, which is verified to be highly resistant to different attacks [15]. In addition, different researchers have also proposed various image encryption schemes based on one or multiple chaotic systems [32,34].

Although the above chaotic-based encryption methods often have good encryption performance, modern communication systems typically own dual requirements of encryption and compression [26–28]. As a result, it is necessary to embed compression into image encryption in order to satisfy the double requirements. In this work, our proposed CCSE method is such a scheme, which can not only retain the high security of chaotic-based image encryption, but also introduce the advantages of compressive sensing.

2.3 Compressive Sensing

Mathematically, let $\mathrm{x} \in \mathrm{R}^{\mathrm{n}}$ denote the signal of interest. As prior information, x is typically k-sparse or compressible in a transform domain, i.e., $\mathrm{x} = \mathrm{Bc}$, where $\mathrm{B} \in \mathrm{R}^{\mathrm{n}\times\mathrm{n}}$ is an orthonormal basis or a frame, and $\mathrm{c} \in \mathrm{R}^{\mathrm{n}}$ is the corresponding k-sparse vector. Let $\mathrm{A} \in \mathrm{R}^{\mathrm{m}\times\mathrm{n}}(\mathrm{m} \ll \mathrm{n})$ and $\tau = (m/n)$ be the sensing matrix and measurement rate, respectively. Then, CS can be modeled as:

$$\mathrm{y} = \mathrm{Ax}, \tag{2}$$

where $\mathrm{y} \in \mathrm{R}^{\mathrm{m}}$ denotes the measurement vector, which can be treated as the linear projection of x.

Because of $\mathrm{m} \ll \mathrm{n}$, Eq. (2) has infinite solutions. Fortunately, if the sensing matrix A satisfies restricted isometry property (RIP), one can exactly recover x from y via some optimization problems, such as l_1-optimization problem:

$$\tilde{\mathrm{x}} = \arg\min ||\mathrm{x}||_{\mathrm{l}_1} \text{ subject to } \mathrm{Ax} = \mathrm{y}. \tag{3}$$

To solve the problem of Eq. (3), there exist many CS optimization algorithms, such as basis pursuit [35], deep optimization-inspired network [36,37]. The RIP offers a distinct geometrical explanation and gives an exactly united architecture to deal with signal recovery. For images, it is a typical compressed signal and can be directly applied to CS theory.

3 The Proposed CCSE Framework

In this section, we first design the Chebyshev Toeplitz chaotic sensing matrix that meets the RIP, and then introduce the proposed CCSE framework.

3.1 Chebyshev Toeplitz Chaotic Sensing Matrix

We first use Eq. (1) to generate a Chebyshev chaotic sequence $\{\mathrm{z}_{\mathrm{i}}\}_{i=0}^{\infty}$. And then, similar to random matrix, we can obtain the Chebyshev Toeplitz chaotic sensing matrix (CTsM), $\mathrm{A} \in \mathrm{R}^{\mathrm{m}\times\mathrm{n}}$, via $\{\mathrm{z}_{\mathrm{i}}\}_{i=0}^{\infty}$ by column and column, i.e.,

$$A = \frac{1}{\delta\sqrt{m}}\begin{pmatrix} z_0 & z_{md} & \cdots & z_{(m+n-2)d} \\ z_d & z_0 & \cdots & z_{(m+n-3)d} \\ \vdots & \vdots & \ddots & \vdots \\ z_{(m-1)d} & z_{(m-2)d} & \cdots & z_{(n-1)d} \end{pmatrix}, \tag{4}$$

where δ^2 represents the variance of $\{z_i\}_{i=0}^{\infty}$ and d is the sampling step size of $\{z_i\}_{i=0}^{\infty}$. Note that the CTsM's correlation is greatly reduced as the adjacent elements in each row of CTsM are separated by a distance of m × d. According to that the i^{th} moment z_i and $(i+d)^{th}$ moment z_{i+d} of $\{z_i\}_{i=0}^{\infty}$ are approximately independent, thus CTsM can be treated as a sub-Gaussian-like matrix. Following the work of [38,39], we can easily obtain the following theorem for CTsM, i.e., CTsM satisfies the RIP with high probability.

Theorem 1. *The CTsM, $A \in R^{m\times n}$, with the form of Eq. (4), generated by $\{z_i\}_{i=0}^{\infty}$, satisfies restricted isometry property with probability $Pro \geq 1 - e^{-g_1 \cdot m}$ for any $m \geq (g_2 \cdot k \cdot \log(n/k))$, where g_1 and g_2 rely only on σ_k, respectively.*

According to Theorem 1, we can easily obtain that CTsM meets the RIP, which can grantee the sampling efficiency of CS. Moreover, due to the Toeplitz structure of CTsM, this Toeplitz-based matrix A has the following advantages: 1) A only need store (m+n−2) elements that can significantly decrease memory requirement, compared to Gaussian sensing matrix or other chaotic matrices (need (m × n) elements); 2) A can support fast multiplication, such as FFT, and 3) CTsM is a deterministic sensing matrix that corresponds to feasible hardware implementation, that is, linear time invariant systems.

3.2 Overall Framework of CCSE

Fig. 2 presents the framework of the proposed CCSE method. CCSE is composed of an encryption process and a decryption process, and they present an inverse relationship. To be more specific, the encryption process includes image sparse representation, an Arnold scrambling operator, a compressive sensing operator, a bilateral diffusion operator, a chaotic scrambling operator. Correspondingly, the decryption process consists of the reverse operation of the above steps.

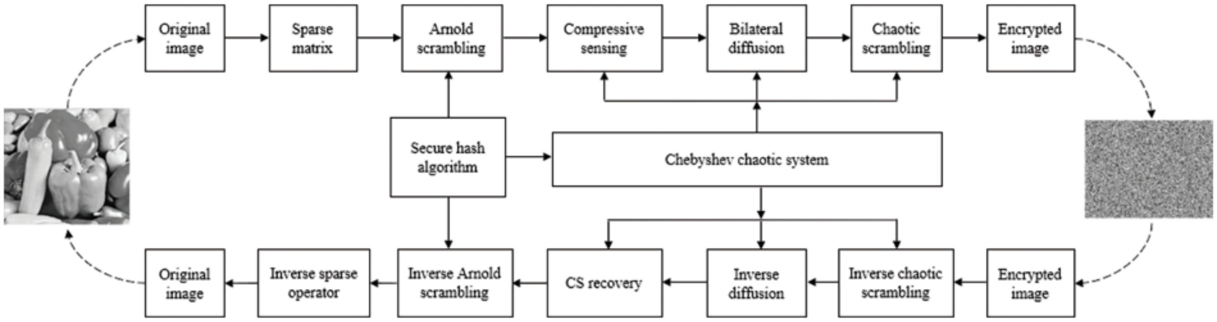


Figure 2: The CCSE framework, which consists of an encryption process and a decryption process, where the decryption process is the reverse of the encryption process

Moreover, the CS operator, bilateral diffusion operator, chaotic scrambling operator are based on Chebyshev chaotic sequence generated by Eq. (1), as shown in Fig. 2. Let x be an image of size n × n. We use the plaintext image x as the parameter to generate the key, and then adopt the secure hash algorithm SHA-256 [40] to generate three sets of keys, i.e., $(\mu^{(1)}, d^{(1)}, z_0^{(1)})$, $(\mu^{(2)}, d^{(2)}, z_0^{(2)})$, and $(\mu^{(3)}, d^{(3)}, z_0^{(3)})$. After that, the first three sets of parameters, regarded as stream cipher for CCSE, are used as the initial value and parameters of the Chebyshev chaotic system to generate the corresponding chaotic sequence, i.e., T_1, T_2, T_3.

The secure hash algorithm is designed by National institute of standards and technology, and has very high security. Therefore, this operation can increase the correlation between the key and the plaintext image, which can better prevent plaintext attack.

3.2.1 The Encryption Process

Moreover, the encryption process of the proposed CCSE can be summarized as the following steps:

Step 1 Sparse representation: We use a sparse basis $\mathrm{B} \in \mathrm{R}^{\mathrm{n \times n}}$, such as discrete wavelet transform (DWT), to sparse the original image and then obtain the corresponding sparse coefficient matrix $\mathrm{C} \in \mathrm{R}^{\mathrm{n \times n}}$ via:

$$\mathrm{B}^{-1}\mathrm{x} = \mathrm{C}. \tag{5}$$

Note that B can be many sparse transforms, such as Fourier transform and discrete cosine domain.

The sparse coefficients of the image are predominantly comprised of numerous zeros, accompanied by a limited number of larger coefficients. This characteristic results in a sparse representation that effectively reduces the overall complexity associated with processing images. Note that the sparsification defined by Eq. (5) is reversible.

Step 2 Arnold scrambling operator: We utilize the Arnold scrambling operator F_{as} on sparse coefficient matrix C and then obtain the scrambled coefficient matrix. The Arnold scrambling operator can be modeled as:

$$\mathrm{D} = \mathrm{F}_{as}(\mathrm{C}), \tag{6}$$

where $\mathrm{D} \in \mathrm{R}^{\mathrm{n \times n}}$ is the scrambled coefficient matrix. The Arnold scrambling, i.e., cat face transformation, is used to uniformly distribute the energy of an image, which is widely applied in digital watermarking. The two-dimensional Arnold transformation F_{as} for an image of order P is defined as:

$$\begin{pmatrix} \mathrm{r}' \\ \mathrm{t}' \end{pmatrix} = \mathrm{F}_{\mathrm{as}}(\cdot) = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} \mathrm{r} \\ \mathrm{t} \end{pmatrix} \bmod \mathrm{P}, \tag{7}$$

where (r, t) and (r', t') are the pixels' position of C and D, respectively, and $r, t \in \{0, 1, 2, \ldots, \mathrm{P} - 1\}$.

The Arnold scrambling operator plays a crucial role in evenly distributing the high-frequency information of matrix C across the D space. This redistribution effectively mitigates the block effect, leading to improved outcomes in image CS. Consequently, this operator contributes to a more uniform distribution of information, thereby enhancing the effectiveness of the image compression and reconstruction processes.

Step 3 Compressive sensing: Using $(\mu^{(1)}, d^{(1)}, \mathrm{z}_0^{(1)})$ and the generated sequence T_1, we first construct a sensing matrix CTsM, $\mathrm{A} \in \mathrm{R}^{\mathrm{m \times n}}$. Then we use the CTsM to sample and compress the scrambled coefficient matrix, which can be formalized as:

$$\mathrm{y} = \mathrm{AD}, \tag{8}$$

where $\mathrm{y} \in \mathrm{R}^{\mathrm{m \times n}}$ represents the measurements. The measurement rate is $\tau = (m/n)$. As the data dimension can be reduced from $\mathrm{R}^{\mathrm{n \times n}}$ to $\mathbb{R}^{\mathrm{m \times n}}$, thus the proposed CCSE scheme can obtain considerable compression performance.

Step 4 Bilateral diffusion operator: This operator consists of a forward diffusion function F_{fd} and a counter diffusion function F_{cd}, which are based on modulo addition operation. First of all, we straighten $y \in \mathbb{R}^{m \times n}$ into a vector y' with size of $1 \times mn$. Then, we use F_{fd} and F_{cd} to act on the vector y', respectively. The forward diffusion function F_{fd} can be modeled as:

$$w = F_{fd}(y'). \tag{9}$$

Specifically, for an element of w, w_j, we have:

$$\left(\begin{array}{r} w_j = \left(w_{j-1} + T_2^{(j)} + y_j'\right) \bmod 256 \\ y_j' = \left(2 \times 256 + w_j - w_{j-1} - T_2^{(j)}\right) \bmod 256 \end{array}\right., \tag{10}$$

where $T_2^{(j)}$ denotes the j^{th} element of the generated Chebyshev chaotic sequence, and $j \in \{1, 2, 3, \ldots, mn\}$. Similar to F_{fd}, the counter diffusion function F_{cd} is:

$$q = F_{cd}(w), \tag{11}$$

where q is the output of F_{fd}. Specifically, for an element of q, q_j, we have:

$$\left(\begin{array}{r} q_j = \left(q_{j+1} + T_2^{(j)} + w_j\right) \bmod 256 \\ w_j = \left(2 \times 256 + q_j - q_{j+1} - T_2^{(j)}\right) \bmod 256 \end{array}\right.. \tag{12}$$

After the bilateral diffusion operator, the extraction of information related to the original image from the ciphertext image q becomes a challenging task, consequently enhancing the overall security of the encryption process. The inherent difficulty introduced by this operation serves as a robust protective measure, making it arduous for unauthorized entities to retrieve meaningful details from the encrypted data.

Step 5 Chaotic scrambling operator: We use the Chaotic scrambling operator F_{cs} to scramble the ciphertext image q, which can be defined as:

$$y_s = F_{cs}(q) = \mathrm{sort}(\mathrm{Corr}\{\mathrm{vect}(q), T_3\}), \tag{13}$$

where y_s is the ultimate ciphertext image, $\mathrm{sort}(\cdot)$ and $\mathrm{vect}(\cdot)$ denote the sorting and vectorization operations, respectively, and the $\mathrm{Corr}(\cdot)$ function is used to establish a one-to-one correspondence between q and the chaotic sequence T_3.

3.2.2 The Decryption Process

As descripted in Fig. 2, the decryption process of the proposed CCSE is the reverse of the encryption process. Specially, the decryption process consists of an inverse sparse operator, an inverse Arnold scrambling operator, a CS recovery, an inverse bilateral diffusion operator, and an inverse chaotic scrambling operator. Note that the inverse sparse operator, the inverse Arnold scrambling operator, the inverse bilateral diffusion operator, and the inverse chaotic scrambling operator is the corresponding reverse operations of step 1, step 2, step 4, and step 5 in the encryption process.

For example, the inverse sparse operator can be formed as:

$$x = BC, \tag{14}$$

which is the inverse of Eq. (5). By using this inverse sparse operator, we can obtain the reconstructed and decrypted image $\tilde{x}$. All other reverse operations are reverse operations of their corresponding formulas.

Specially, the CS recovery can be converted to some optimization problems, most famously, l_1-optimization problem defined by Eq. (3). One can use many CS algorithms to solve this problem, such as basis pursuit [35]. Please see the reference [26] for more details. To save space, we omit the detailed description of the decryption process.

4 Numerical Experiments

In this section, the encryption performance of the proposed CCSE is investigated via numerical experiments. For a fair comparison, we also use several image chaotic encryption methods as the comparison algorithms of CCSE. The results of the compared algorithms are obtained using the author's publicly available code or by reproducing the methods (in cases where the codes are not available).

4.1 Experimental Setup and Environment

We use the standard test images to test the performance of CCSE. The standard test images include "Lena", "Pepper", "Cameraman". In addition, these numerical experiments are implemented on the MATLAB 2018(R2018b) platform on a computer PC with Intel(R) Xeon(R) Silver 4110 CPU @ 2.10 GHz, 64 G memory, Windows 10 system. In particular, we adopt basis pursuit method [35] as the CS recovery algorithm for CCSE. The quality metric for image recovery is the commonly used peak signal-to-noise ratio (PSNR) defined as:

$$\mathrm{PSNR} = 10\ \log_{10} 255 \times 255\mathrm{MSE}\ \ \mathrm{dB},$$

where

$$\mathrm{MSE} = \frac{1}{\mathrm{n} \times \mathrm{n}} \Sigma_{\mathrm{r}=1}^{\mathrm{n}} \Sigma_{\mathrm{t}=1}^{\mathrm{n}} \left(|\mathrm{x}\,(\mathrm{r},\mathrm{t}) - \tilde{\mathrm{x}}\,(\mathrm{r},\mathrm{t})\,| \right),$$

where $x(r,t)$ and $\tilde{x}\,(r,t)$ denote the pixel values of the original image and the decrypted image, respectively, and $\mathrm{n} \times \mathrm{n}$ is the size of the original image.

4.2 Encrypted Data and CS Recovery

We take images ("Lena", "Pepper", "Cameraman") of size 256×256 as the original images, which are depicted in Figs. 3a, 3d and 3g, respectively. Assume that the measurement rate $\tau = 0.8$. Then, we follow the encryption steps of CCSE to obtain the corresponding compressed and encrypted data, as shown in Figs. 3b, 3e and 3h. Based on the decryption process, we can obtain these decrypted images, i.e., Figs. 3c, 3f and 3i. The corresponding PSNRs are 38.11, 38.62, and 37.75 dB. According to these results, we can observe that CCSE can reconstruct the original images with high quality.

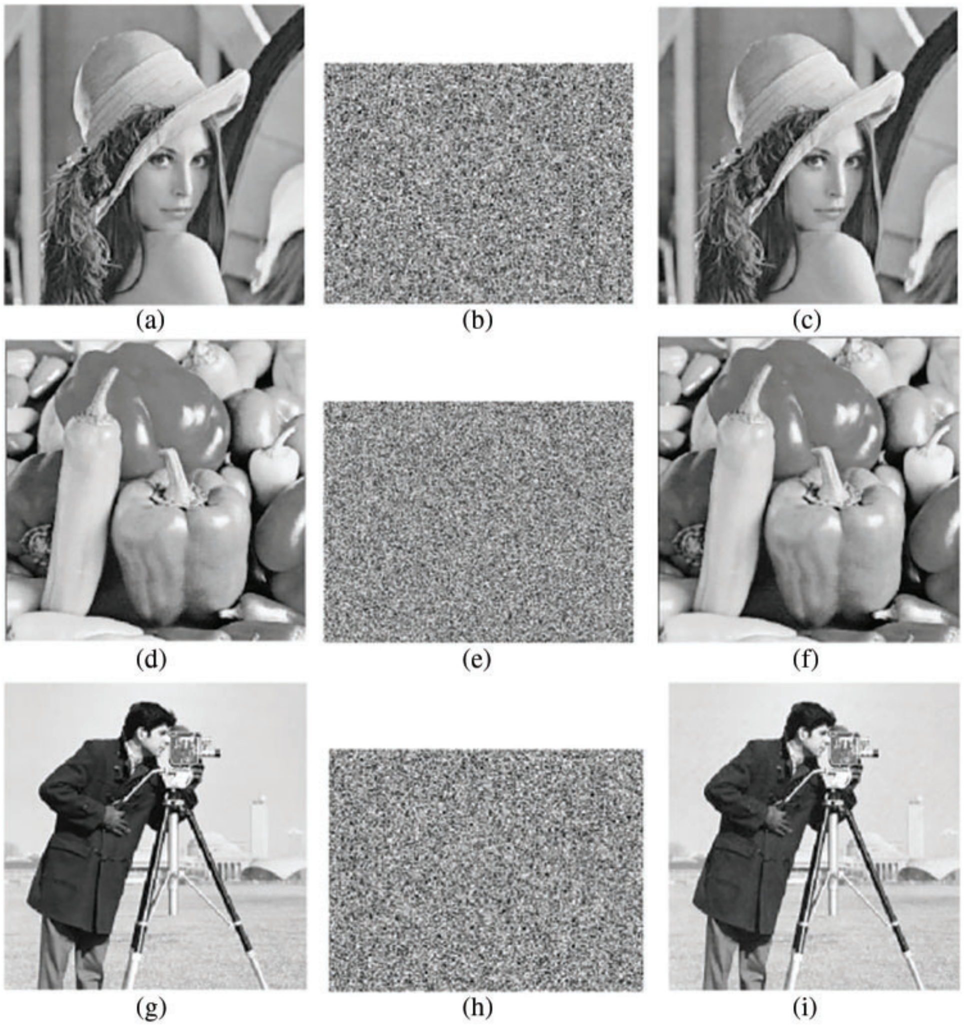


Figure 3: Original image, encrypted image, and decrypted image. (a) Original "Lena", (b) encrypted "Lena", (c) decrypted "Lena"; (d) Original "Pepper", (e) encrypted "Pepper", (f) decrypted "Pepper"; (g) Original "Cameraman", (h) encrypted "Cameraman", (i) decrypted "Cameraman"

In addition, to observe in more detail, we adopt various CTsMs with different sizes for CCSE, i.e., $\tau \in \{0.4, 0.6, 0.8\}$. Fig. 4 shows the encrypted data and CS recovery for "Lena". The PSNRs for $\tau = 0.4$, $\tau = 0.6$, $\tau = 0.8$ are 24.76, 31.39, and 38.11 dB, respectively. According to this figure, we can see that as τ is higher, the reconstruction quality of CCSE is better. Moreover, although τ is as low as 0.4, CCSE can still reconstruct the image better. This also confirms that CCSE can compress the image while encrypting the image, which can improve the efficiency of image transmission.

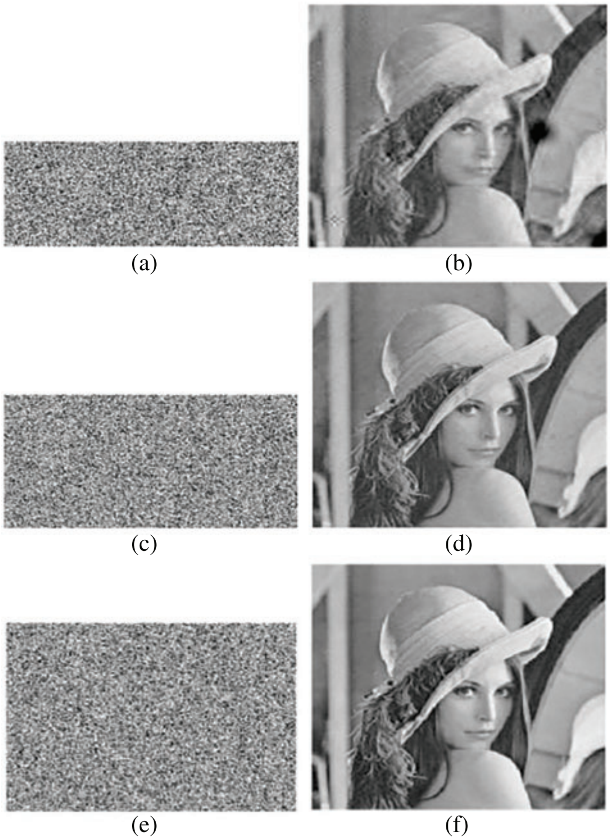


Figure 4: Encrypted images and decrypted images at different measurement rates. (a) Encrypted "Lena" at $\tau = 0.4$, (b) decrypted "Lena" at $\tau = 0.4$; (c) encrypted "Lena" at $\tau = 0.6$, (d) decrypted "Lena" at $\tau = 0.6$; (e) encrypted "Lena" at $\tau = 0.8$; (f) decrypted "Lena" at $\tau = 0.8$

4.3 Key Space

The proposed CCSE adopts the secure hash algorithm SHA-256 to generate the keys, therefore, the key space for CCSE is $S_{key} = 2^{256}$. Table 1 compares the key space of CCSE with other image encryption algorithms. According to Table 1, we can see that the proposed CCSE has a larger key space than other algorithms. Moreover, it is well-known that if the encryption method's key space is larger than 2^{100}, then this approach is easily resistant to all kinds of brute force crack or attack key.

Table 1: Comparison of key space for CCSE and other methods

Method	Ref. [16]	Ref. [17]	Ref. [27]	Ref. [28]	Ref. [32]
Key space	$>2^{64}$	2^{120}	10^{70}	10^{53}	2^{208}
Method	Ref. [33]	Ref. [34]	Ref. [41]	Ref. [42]	CCSE
Key space	$>10^{69}$	2^{256}	$>2^{256}$	2^{100}	2^{256}

4.4 Histogram Analysis

Histogram is a statistical method of data distribution, which is also an efficiency tool to measure the encryption performance of a method. We illustrate the histograms for our proposed CCSE on images "Lena", "Pepper", and "Cameraman" in Fig. 5. The second column and fourth column are the histograms of original images and the encrypted images, respectively. According to Fig. 5, we can see that the histogram of the original image exhibits a Gaussian phenomenon, which is unevenly distributed. However, the histogram of encrypted image has no high and low features, which is flat. Moreover, the distribution characteristics of a histogram can be quantitatively verified by calculating the variance of the histogram [43,44]. It can be expressed as:

$$\mathrm{Var(X)} = \frac{\Sigma_{\mathrm{i=1}}^{\mathrm{n}}\Sigma_{\mathrm{j=1}}^{\mathrm{n}}(\frac{1}{2}\times(x_i - x_j))}{\mathrm{n}\times\mathrm{n}}\times 100,$$

where $\mathrm{X} = \{x_0, x_1, \ldots, x_{i=n-1}\}$ is a vector, and x_i and x_j denote i-th and j-th corresponding gray value, respectively. The smaller the variance of a histogram, the flatter the histogram becomes, indicating a more equal distribution of gray-level pixels in the image. The ideal value of Var(X) is 0, signifying $x_i = x_j$ for all i and j.

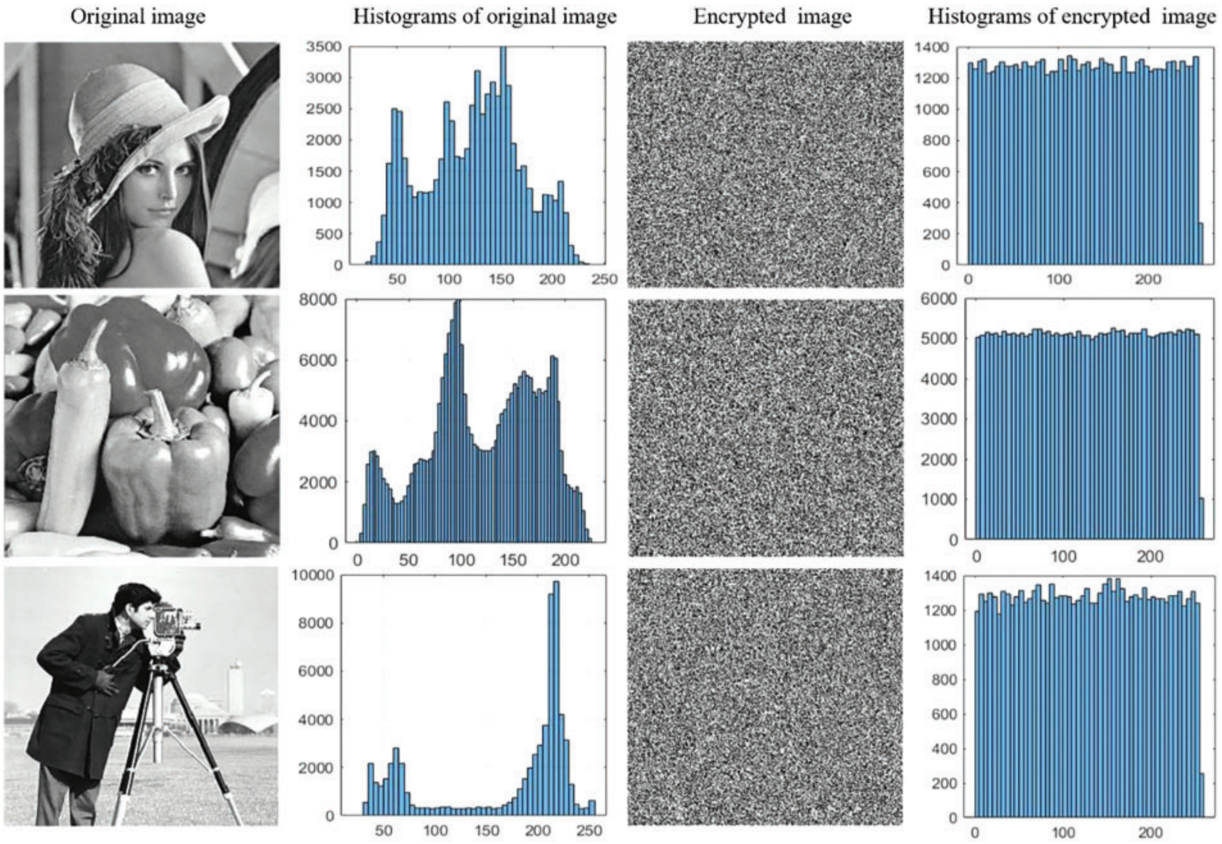


Figure 5: Histograms of original images and the encrypted images. First column: Original images; Second column: Histograms of original images; Third column: The encrypted images; Fourth column: Histograms of encrypted images

We calculated the histogram variances for the proposed scheme concerning plain images with a size of 256 × 256 pixels and their corresponding visually encrypted images. As shown in Table 2, we can see that the Var(X) of the cipher image is smaller than the original image, which indicates that the histogram of encrypted image for CCSE is flat.

Table 2: Variances of histograms of the encrypted images

Lena		Cameraman	
Original image	Cipher image	Original image	Cipher image
30665.70	260.47	110973.40	200.85

Because the histogram of encrypted image for CCSE is flat, the attackers cannot collect effective information through pixel statistical analysis. As a result, the proposed CCSE can resist statistical analysis.

4.5 Differential Attack Analysis

Typically, an attacker may make slight modifications to the original image (e.g., changing only one pixel) and observe the corresponding changes in the encrypted results. Through this approach, the attacker may discover meaningful relationships between two ciphered images and the original image. To assess the impact of this attack on the encryption algorithm, we use two evaluation metrics [16,17], i.e., Number of pixels change rate (NPCR) and Unified average changing intensity (UACI), which are described as following:

$$\mathrm{NPCR} = \frac{\Sigma_{r=1}^{n}\Sigma_{t=1}^{n} D(r,t)}{n \times n} \times 100,$$

and

$$\mathrm{NPCR} = \frac{\Sigma_{r=1}^{n}\Sigma_{t=1}^{n} |x(r,t) - \tilde{x}(r,t)|}{n \times n \times 256} \times 100.$$

Note that if $x(r,t) = \tilde{x}(r,t)$, $D(r,t) = 0$, otherwise $D(r,t) = 1$. For all cryptographic systems, the ideal outcomes for NPCR and UACI are 100% and 33.33%, respectively. We utilize the encrypted version of the original image (Lena) and the modified encrypted version of the image, and compute the values for NPCR and UACI, which are presented in Table 3. From the Table 3, it can be observed that compared to other benchmark algorithms, our proposed CCSE exhibits better NPCR and UACI values, and is also closer to the ideal values. As a result, CCSE demonstrates robust resistance against differential attacks.

Table 3: Comparison of correlation coefficients of different images for different methods

Test image	Method	NPCR %	UACI %
Peppers	Ref. [16]	99.821	33.460
	Ref. [17]	99.299	33.391
	Ref. [27]	96.341	35.614
	Ref. [28]	99.615	33.559

(Continued)

Table 3 (continued)

Test image	Method	NPCR %	UACI %
	Ref. [32]	99.582	33.623
	Ref. [33]	99.601	33.512
	Ref. [34]	99.733	33.725
	Ref. [41]	99.884	35.315
	Ref. [42]	99.607	33.495
	CCSE	**99.885**	**33.384**
Boat	Ref. [16]	99.782	33.682
	Ref. [17]	98.923	33.494
	Ref. [27]	96.761	34.997
	Ref. [28]	99.638	33.455
	Ref. [32]	99.251	33.682
	Ref. [33]	99.581	33.441
	Ref. [34]	99.483	33.875
	Ref. [41]	99.350	36.539
	Ref. [42]	99.617	33.661
	CCSE	**99.485**	**33.406**

4.6 Information Entropy Analysis

Information entropy is commonly used to evaluate the randomness of an image, and its definition is

$$\mathrm{I}\,(\mathrm{s}) = -\Sigma_{\mathrm{j}=0}^{255}\mathrm{p}(\mathrm{s}_\mathrm{j})\,\log_2(\mathrm{p}\,(\mathrm{s}_\mathrm{j})),$$

where s denotes a collection of pixels, and $\mathrm{p}(\mathrm{s}_j)$ is the occurrence probability of s. If an encryption method is closer to the upper limit of 8, then it is safer. Table 4 compares the information entropy for CCSE and other image encryption methods. According to Table 4, we can see that the information entropy of our proposed CCSE is higher than that of the literatures [32] and [34]. These results mean that our proposed CCSE algorithm can effectively scramble the original image and obtain a ciphertext image with better randomness.

Table 4: Comparison of correlation coefficients of different images for different methods

Method	Information entropy		
	Lenna	Pepper	Cameraman
Original image	7.441	7.594	6.905
Ref. [16]	7.971	7.985	7.912
Ref. [17]	7.991	7.993	7.981
Ref. [27]	7.994	7.992	7.986
Ref. [28]	7.990	7.989	7.982
Ref. [32]	7.987	7.993	7.988

(Continued)

Table 4 (continued)

Method	Information entropy		
	Lenna	Pepper	Cameraman
Ref. [33]	7.991	7.994	7.984
Ref. [34]	7.994	7.992	7.986
Ref. [41]	7.991	7.990	7.985
Ref. [42]	7.992	7.991	7.990
CCSE	**7.996**	**7.997**	**7.995**

4.7 Correlation Analysis

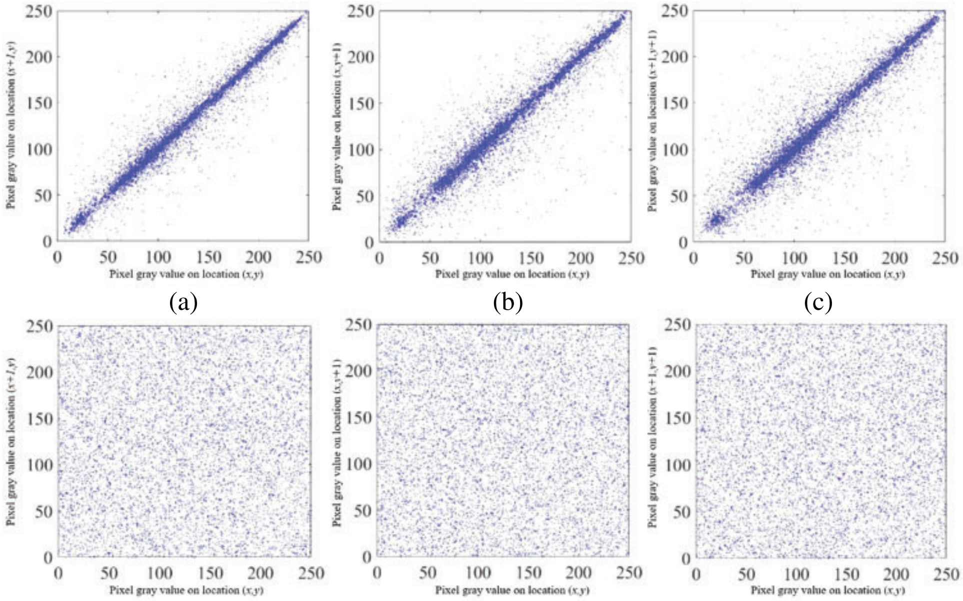
The correlation coefficients of vertical, horizontal and diagonal adjacent pixels are important metrics to measure the encryption performance of a method. Specially, correlation coefficient of adjacent pixels of an encrypted image obtained by an excellent encryption algorithm should be small, close to zero. In this experiment, we randomly choose 10000 pairs of adjacent pixels of an original image and its corresponding encrypted image, and compute the correlation coefficient via

$$\mathrm{Corr(x, y)} = \frac{\mathrm{cov(x, y)}}{\sqrt{\mathrm{D(x)}} \times \sqrt{\mathrm{D(y)}}},$$

where $\mathrm{cov}\,(x, y) = \frac{1}{n}\Sigma_{i=1}^{n}(x_i - E(x))(y_i - E(y)), E\,(x) = \frac{1}{n}\Sigma_{i=1}^{n}x_i, E\,(y) = \frac{1}{n}\Sigma_{i=1}^{n}y_i, D\,(x) = \frac{1}{n}\Sigma_{i=1}^{n}(x_i - E\,(x))^2, D\,(y) = \frac{1}{n}\Sigma_{i=1}^{n}(y_i - E\,(y))^2.$

Fig. 6 illustrates the correlation distribution of "Lena" and its ciphertext image in three directions for our proposed CCSE. According to Fig. 6, we can see that the correlation distributions of vertical, horizontal and diagonal adjacent pixels for the original "Lena" are linear, however, they have become disorganized, and evenly distributed after encryption. In other words, the correlation coefficients of the encrypted image are weak, and thus the proposed CCSE can resist correlation analysis.

Moreover, Table 5 presents the correlation coefficients of different plaintext images and their encrypted images in three directions. From Table 5, we can see that the original image's the correlation coefficients generally exceed 0.9. Moreover, compared to other encryption methods, our proposed CCSE owns smaller correlation coefficients in three directions, indicating that CCSE has better encryption characteristics.



(a) (b) (c)

(d) (e) (f)

Figure 6: The correlation distribution of “Lena” and its ciphertext image in three directions. (a)–(c) denote the horizontal, vertical, and diagonal correlation distributions of the original “Lena”, respectively; (d)–(f) are the horizontal, vertical, and diagonal correlation distributions of the encrypted “Lena”, respectively

Table 5: Comparison of correlation coefficients of “Lena” for different methods

Method	Correlation coefficients		
	Horizontal	Vertical	Diagonal
Original “Lena”	0. 938	0. 969	0. 913
Ref. [16]	0.007	0.006	0.003
Ref. [17]	0.010	0.034	0.021
Ref. [27]	0.013	0.007	−0.008
Ref. [28]	0.015	0.016	0.010
Ref. [32]	0.009	0.028	0.006
Ref. [33]	0.021	0.466	−0.009
Ref. [34]	0.024	0.031	0.007
Ref. [41]	0.273	0.017	0.007
Ref. [42]	0.006	0.004	0.003
CCSE	**−0.005**	**−0.003**	**−0.002**

4.8 Analysis of Visual Strength

In this part, we conduct tests on Homogeneity, Energy, and Contrast analysis to assess the strength of the proposed CCSE, as shown in Table 6. Homogeneity analysis is used to assess the closeness of distribution from the diagonal of GLCM (Grey Level Co-occurrence Matrix) [45]. Energy analysis is employed to quantify the disorderliness within the texture of the cipher image by is employed to quantify the disorderliness within the texture of the cipher image by summing the squared values of GLCM [46]. Contrast analysis can capture the variations among the pixels in the image [47]. According to Table 6, we can see that our proposed CCSE exhibits excellent encryption performance, effectively ensuring high-quality encryption of images.

Table 6: Homogeneity, energy, and contrast analysis of our proposed CCSE

Image		Test		
		Homogeneity	Energy	Contrast
Lena	Original image	0. 7635	0. 0645	1.1303
	Encrypted image	0.3942	0.0160	10.487
Cameraman	Original image	0.8564	0.1618	1.2014
	Encrypted image	0.4041	0.0165	9.7857

4.9 Noise Attack and Robustness

As we all know, images are easily affected by noise during transmission, and may even be maliciously attacked, thus we need to explore the robustness analysis for the encryption method. Based on this observation, we will use Gaussian noise and salt and pepper noise to perform noise attack on the ciphertext images to test the robustness of the algorithm. The Gaussian noise level has mean zero and is controlled by its variance $\in \left\{1 \times 10^{-6}, 3 \times 10^{-6}, 5 \times 10^{-6}, 9 \times 10^{-6}\right\}$, respectively, as shown in first row of Fig. 7. The level of salt and pepper noise is determined by its density $\{0.2, 0.1, 0.05, 0.01\}$, as illustrated in third row of Fig. 7. The second and fourth rows in Fig. 7 present the encrypted images with various noise.

According to Fig. 7, it clearly shows that we can still decrypt the original image from the ciphertext image with different noises, which indicates that the proposed CCSE encryption scheme has good robustness.

4.10 Analysis of Chosen-Plaintext Attacks and Known-Plaintext

As described in before, CCSE use the plaintext image x as the parameter to generate the key, and then adopt the secure hash algorithm SHA-256 to generate three sets of keys. Therefore, a slight change in the initial value, i.e., key, will give rise to a completely different Chebyshev chaotic sequence, consequently leading to distinct the CS operator, bilateral diffusion operator, chaotic scrambling operator. Hence, CCSE generates entirely disparate cipher images, rendering an eavesdropper incapable of decrypting a specific image utilizing the computed initial conditions. Consequently, the proposed CCSE scheme exhibits robust resistance against both chosen-plaintext attacks and known-plaintext attacks.

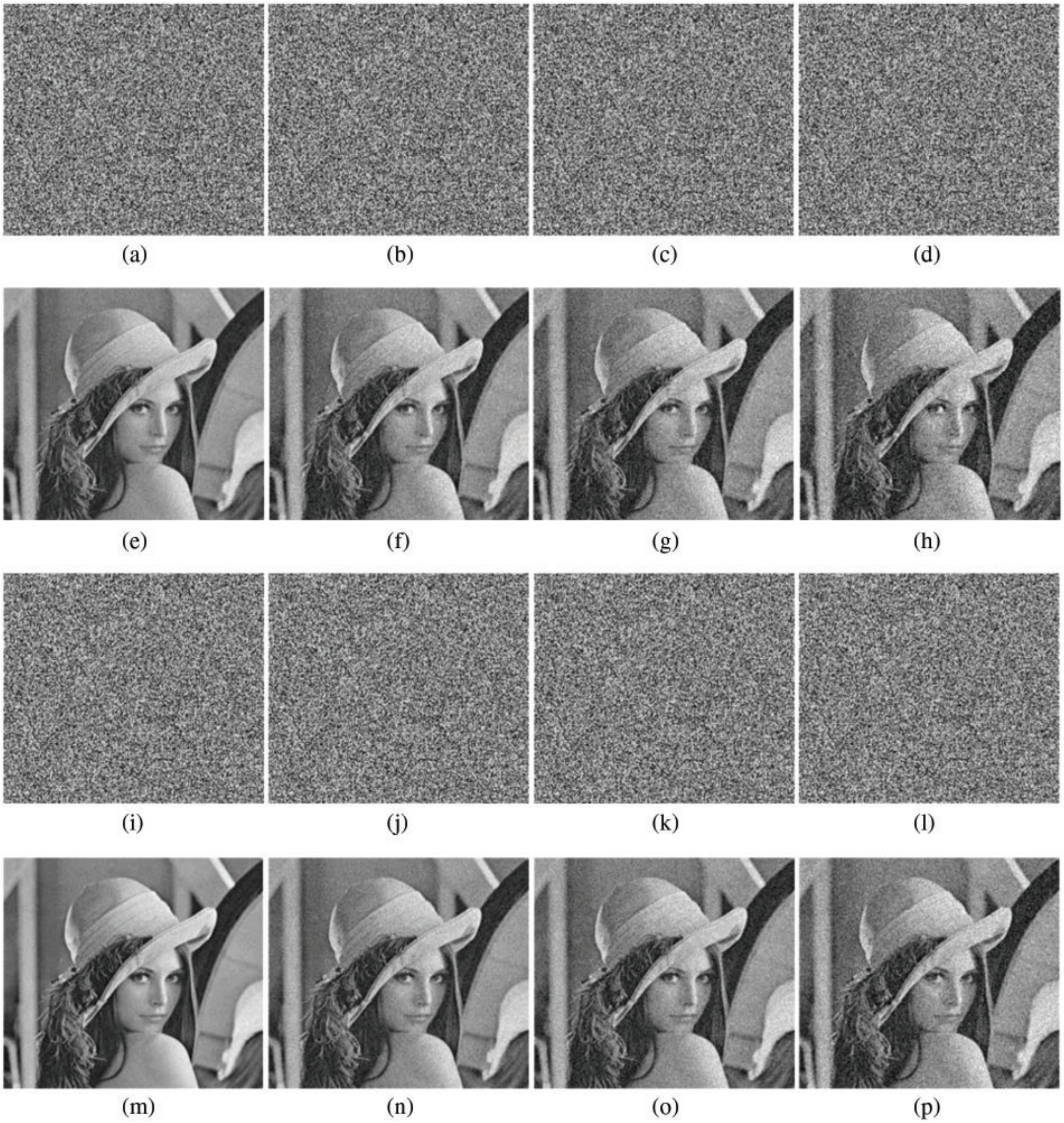


Figure 7: Different noises and their decrypted images. First row, (a)–(d) are the Gaussian noise with variance $\{1 \times 10^{-6}, 3 \times 10^{-6}, 5 \times 10^{-6}, 9 \times 10^{-6}\}$, respectively; Second row, (e)–(h) are the encrypted image with Gaussian noise depicted in (a)–(d); Third row, (i)–(l) are the salt and pepper noise with density $\{0.01, 0.05, 0.1, 0.2\}$, respectively; Fourth row, (m)–(p) are the encrypted image with salt and pepper noise depicted in (i)–(l)

4.11 Analysis of Computational Time Complexity

We selected Lena as the test image to assess the time required for the proposed encryption and decryption methods. The encryption time represents the duration from the original image to the ciphertext image, while the decryption time signifies the time to restore the original image from the ciphertext image. For the Lena image, the proposed CCSE exhibits an encryption time of 0.4323 s and a decryption time of 0.5745 s. While the encryption time of [32,34] and [45] are 0.6892 s, 0.7521, and 4.4282 s, and the corresponding decryption time are 0.8754 s, 0.7965, and 3.4532 s, respectively. Compared to the method in [32], our proposed CCSE is 37.28% faster in encryption time and 52.38% faster in decryption time. It is evident that this proposed CCSE allows for rapid encryption and decryption of images.

5 Conclusions

In conclusion, this paper introduces a novel image encryption algorithm, termed chaotic compressive sensing (CS) encryption (CCSE), which addresses the increasing concerns regarding information security in the digital age. The significance of secure image transmission spans across personal privacy, political communications, medical data, and commercial interests. Recognizing these implications, CCSE emerges as a promising solution by combining the efficiency of CS with the robust security provided by chaotic systems. As a result, CCSE can withstand various attacks, such as differential attack, and exhibit robustness. The proposed CCSE employs a sequence of transformations, including sparse transformation, Arnold transformation, and the integration of a Chebyshev Toeplitz chaotic sensing matrix. These transformations collectively facilitate image perturbation, sampling, and compression, thereby reducing transmission bandwidth and data volume without compromising security. Moreover, the incorporation of bilateral diffusion and chaotic encryption operators further enhances the security of CCSE by perturbing and expanding pixel values and positions within the encrypted image. Through extensive experimental validation, CCSE exhibits robustness against statistical and noise attacks, surpassing existing competitors in terms of security and performance. CCSE represents a significant advancement in the field of image encryption, offering a viable solution to the pressing challenges of information security in an increasingly digitized world. Its effectiveness in safeguarding sensitive data across diverse domains underscores its potential for practical implementation and further research exploration.

Our proposed CCSE is more suitable for regular images. However, once the image size becomes too large, it leads to excessive complexity in our approach. In future work, we will develop a more lightweight image chaotic compression encryption scheme based on CCSE. Additionally, CCSE requires collaboration with traditional CS reconstruction algorithms to recover images. However, the slow recovery speed of traditional CS reconstruction algorithms imposes a time constraint on our proposed CCSE. By integrating deep learning techniques with CCSE, we will explore novel image chaos encryption methods aimed at enhancing security and adaptability. Through real-world application validation, especially in areas such as communication and cloud storage, we will assess the performance of these algorithms, ensuring their effectiveness and feasibility in practical scenarios.

Acknowledgement: The authors appreciate the reviewers and editors for their valuable feedback on this work.

Funding Statement: This work was supported by the National Natural Science Foundation of China (Nos. 62002028, 62102040 and 62202066).

Author Contributions: Mingliang Sun: Conceptualization, Methodology, Writing-original and Editing; Jie Yuan: Software, Investigation; Xiaoyong Li: Investigation, Supervision and Writing-original draft; Dongxiao Liu: Funding acquisition and Experimental verification. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data available on request from the authors.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] R. J. Al-Azawi, N. Al-Saidi, H. A. Jalab, R. Ibrahim, and D. Baleanu, "Image splicing detection based on texture features with fractal entropy," *Comput. Mater. Contin.*, vol. 69, no. 3, pp. 3903–3915, 2021. doi: 10.32604/cmc.2021.020368.

[2] S. Boopathi, B. K. Pandey, and D. Pandey, "Advances in artificial intelligence for image processing: Techniques, applications, and optimization," in *Handbook of Research on Thrust Technologies' Effect on Image Processing*. Hershey, USA: IGI Global, 2023, pp. 73–95.

[3] Y. Hu and L. Nan, "A novel 2D hyperchaotic with a complex dynamic behavior for color image encryption," *Comput. Mater. Contin.*, vol. 74, no. 3, pp. 6555–6571, 2023. doi: 10.32604/cmc.2023.036090.

[4] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, and M. F. Ijaz, "Analytical study of hybrid techniques for image encryption and decryption," *Sensors*, vol. 20, no. 18, pp. 5162, 2020. doi: 10.3390/s20185162.

[5] V. Rijmen and J. Daemen, "The advanced encryption standard," in *Proc. Federal Inform. Process. Standards Pub., Nat. Institute Standards Technol.*, 2001, vol. 26, pp. 137–139.

[6] S. Basu, "International data encryption algorithm (IDEA)–a typical illustration," *J. Global Res. Comput. Sci.*, vol. 2, pp. 116–118, 2011.

[7] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," *IBM J. Res. Dev.*, vol. 38, no. 3, pp. 243–250, 1994. doi: 10.1147/rd.383.0243.

[8] T. Li and J. Yorke, "Period three implies chaos," *Am. Math. Month.*, vol. 82, no. 10, pp. 985–992, 1975.

[9] M. Ayedi, W. H. ElAshmawi, and E. Eldesouky, "Hybrid chaotic salp swarm with crossover algorithm for underground wireless sensor networks," *Comput. Mater. Contin.*, vol. 72, no. 2, pp. 2963–2980, 2022. doi: 10.32604/cmc.2022.025741.

[10] B. Sivakumar, "Chaos theory in geophysics: Past, present and future," *Chaos Solitons & Fractals*, vol. 19, no. 2, pp. 441–462, 2004. doi: 10.1016/S0960-0779(03)00055-9.

[11] R. Zhao, Y. Zhang, S. Li, W. Wen, S. Yi and R. Lan, "3D mesh encryption with differentiated visual effect and high efficiency based on chaotic system," *Expert. Syst. Appl.*, vol. 238, no. 2, pp. 122140, 2024. doi: 10.1016/j.eswa.2023.122140.

[12] R. Zhao, Y. Zhang, Y. Nan, W. Wen, X. Chai and R. Lan, "Primitively visually meaningful image encryption: A new paradigm," *Inf. Sci.*, vol. 613, pp. 628–648, 2022. doi: 10.1016/j.ins.2022.08.027.

[13] M. Z. Talhaoui and X. Wang, "A new fractional one dimensional chaotic map and its application in high-speed image encryption," *Inf. Sci.*, vol. 550, no. 2, pp. 13–26, 2021. doi: 10.1016/j.ins.2020.10.048.

[14] Y. Hong *et al.*, "A novel approach for image encryption with chaos-RNA," *Comput. Mater. Contin.*, vol. 77, no. 1, pp. 139–160, 2023. doi: 10.32604/cmc.2023.043424.

[15] R. Zhao, Y. Zhang, R. Lan, Z. Hua, and Y. Xiang, "Heterogeneous and customized cost-efficient reversible image degradation for green IoT," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2630–2645, 2022. doi: 10.1109/JIOT.2022.3213875.

[16] X. Wang, S. Gu, and Y. Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," *Opt. Lasers Eng.*, vol. 68, no. 6, pp. 126–134, 2015. doi: 10.1016/j.optlaseng.2014.12.025.

[17] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, “Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence,” *Opt. Lasers Eng.*, vol. 56, pp. 83–93, 2014. doi: 10.1016/j.optlaseng.2013.12.003.

[18] J. Tamang *et al.*, “Dynamical properties of ion-acoustic waves in space plasma and its application to image encryption,” *IEEE Access*, vol. 9, pp. 18762–18782, 2021. doi: 10.1109/ACCESS.2021.3054250.

[19] H. L. Gururaj, M. Almeshari, Y. Alzamil, V. Ravi, and K. V. Sudeesh, “Efficient SCAN and chaotic map encryption system for securing E-Healthcare images,” *Information*, vol. 14, no. 1, pp. 47, 2023. doi: 10.3390/info14010047.

[20] J. Jain and A. Jain, “Securing e-healthcare images using an efficient image encryption model,” *Scientific Programming*, vol. 2022, no. 6489331, pp. 1–11, 2022. doi: 10.1155/2022/6438331.

[21] N. Mao, H. He, F. Chen, P. Bellavista, and Y. Yang, “Reversible data hiding of JPEG images based on block sorting and segmented embedding,” *Biomed. Signal Process. Control*, vol. 87, no. 2, pp. 105555, 2024. doi: 10.1016/j.bspc.2023.105555.

[22] T. Chuman, W. Sirichotedumrong, and H. Kiya, “Encryption-then-compression systems using grayscale-based image encryption for JPEG images,” *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 6, pp. 1515–1525, 2018. doi: 10.1109/TIFS.2018.2881677.

[23] S. Pankaj and M. Dua, “Chaos based medical image encryption techniques: A comprehensive review and analysis,” *Inform. Secur. J.: A Global Perspect.*, vol. 33, no. 3, pp. 1–27, 2024. doi: 10.1080/19393555.2024.2312975.

[24] M. Preishuber, T. Hütter, S. Katzenbeisser, and A. Uhl, “Depreciating motivation and empirical security analysis of chaos-based image and video encryption,” *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 9, pp. 2137–2150, 2018. doi: 10.1109/TIFS.2018.2812080.

[25] S. Bai, G. Zhu, and X. Ji, “Comments on a novel image encryption-compression scheme using hyper-chaos and chinese remainder theorem,” *Appl. Mech. Mater.*, vol. 743, pp. 333–337, 2015. doi: 10.4028/www.scientific.net/AMM.743.333.

[26] R. Vershynin, Y. Eldar, and G. Kutyniok, “Compressed sensing, theory and applications,” in *Introduction to the Non-Asymptotic Analysis of Random Matrices*, Cambridge, UK: Cambridge University Press, 2012, pp. 210–268.

[27] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, “An image encryption algorithm based on chaotic system and compressive sensing,” *Signal Process.*, vol. 148, no. 9, pp. 124–144, 2018. doi: 10.1016/j.sigpro.2018.02.007.

[28] L. Gong, K. Qiu, C. Deng, and N. Zhou, “An image compression and encryption algorithm based on chaotic system and compressive sensing,” *Opt. Laser Technol.*, vol. 115, no. 1, pp. 257–267, 2019. doi: 10.1016/j.optlastec.2019.01.039.

[29] H. Gan, S. Xiao, Y. Zhao, and X. Xue, “Construction of efficient and structural chaotic sensing matrix for compressive sensing,” *Signal Process.: Image Commun.*, vol. 68, pp. 129–137, 2018.

[30] H. Gan, S. Xiao, and F. Liu, “Chaotic binary sensing matrices,” *Int. J. Bifurcat. Chaos*, vol. 29, no. 9, pp. 1950121, 2019. doi: 10.1142/S0218127419501219.

[31] H. Gan, S. Xiao, Z. Zhang, S. Shan, and Y. Gao, “Chaotic compressive sampling matrix: Where sensing architecture meets sinusoidal iterator,” *Circuits Syst. Signal Process.*, vol. 39, no. 3, pp. 1581–1602, 2020. doi: 10.1007/s00034-019-01223-w.

[32] S. Wang, “Research on digital image encryption technology based on chaotic system,” Master thesis, Hangzhou Dianzi University, Hangzhou, China, 2020.

[33] P. Zhen, G. Zhao, L. Min, and X. Jin, “Chaos-based image encryption scheme combining DNA coding and entropy,” *Multimed. Tools Appl.*, vol. 75, no. 11, pp. 6303–6319, 2016. doi: 10.1007/s11042-015-2573-x.

[34] X. Wang, “Digital image compression algorithm based on multi-chaotic system,” Master thesis, Taiyuan University of Technology, Taiyuan, China, 2021.

[35] P. Wu and J. Cheng, “Deep unfolding basis pursuit: Improving sparse channel reconstruction via data-driven measurement matrices,” *IEEE Trans. Wirel. Commun.*, vol. 21, no. 10, pp. 8090–8105, 2022. doi: 10.1109/TWC.2022.3164091.

[36] H. Gan, Y. Gao, C. Liu, H. Chen, T. Zhang and F. Liu, "AutoBCS: Block-based image compressive sensing with data-driven acquisition and noniterative reconstruction," *IEEE Trans. Cybern.*, vol. 53, no. 4, pp. 2558–2571, 2023. doi: 10.1109/TCYB.2021.3127657.

[37] M. Shen, H. Gan, C. Ning, Y. Hua, and T. Zhang, "TransCS: A Transformer-based hybrid architecture for image compressed sensing," *IEEE Trans. Image Process.*, vol. 31, pp. 6991–7005, 2022. doi: 10.1109/TIP.2022.3217365.

[38] J. Haupt, W. U. Bajwa, G. Raz, and R. Nowak, "Toeplitz compressed sensing matrices with applications to sparse channel estimation," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5862–5875, 2010. doi: 10.1109/TIT.2010.2070191.

[39] R. Baraniuk, M. Davenport, R. DeVore, and M. Wakin, "A simple proof of the restricted isometry property for random matrices," *Constr. Approx.*, vol. 28, no. 3, pp. 253–263, 2008. doi: 10.1007/s00365-007-9003-x.

[40] R. Fotohi and F. S. Aliee, "Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT," *Comput. Netw.*, vol. 197, no. 3, pp. 108331, 2021. doi: 10.1016/j.comnet.2021.108331.

[41] R. Ponuma and R. Amutha, "Compressive sensing based image compression-encryption using novel 1D-chaotic map," *Multimed. Tools Appl.*, vol. 77, no. 15, pp. 19209–19234, 2018. doi: 10.1007/s11042-017-5378-2.

[42] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Process.*, vol. 153, no. 7, pp. 11–23, 2018. doi: 10.1016/j.sigpro.2018.06.008.

[43] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020. doi: 10.1109/ACCESS.2020.2970806.

[44] J. S. Khan and S. K. Kayhan, "Chaos and compressive sensing based novel image encryption scheme," *J. Inf. Secur. Appl.*, vol. 58, no. 4, pp. 102711, 2021. doi: 10.1016/j.jisa.2020.102711.

[45] J. S. Khan *et al.*, "DNA and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, pp. 159732–159744, 2020. doi: 10.1109/ACCESS.2020.3020917.

[46] P. Kiran and B. D. Parameshachari, "Resource optimized selective image encryption of medical images using multiple chaotic systems," *Microprocess. Microsyst.*, vol. 91, no. 10, pp. 104546, 2022. doi: 10.1016/j.micpro.2022.104546.

[47] F. Masood *et al.*, "A novel image encryption scheme based on Arnold cat map, Newton-Leipnik system and Logistic Gaussian map," *Multimed. Tools Appl.*, vol. 81, no. 21, pp. 30931–30959, 2022. doi: 10.1007/s11042-022-12844-w.