Journal of Engineering and Sustainable Development
Vol. 28, No. 05, September 2024
https://jeasd.uomustansiriyah.edu.iq/index.php/jeasd
ISSN 2520-0917
Research Article
https://doi.org/10.31272/jeasd.28.5.11

Hybrid Block Chaotic Compressive Sensing and Chaotic Scrambling Algorithms for Color Image Encryption System

Asaad H. Sahar[1], Hussein A. Hussein Al-Delfi[2], Ali F. Hassoon[3*]

[1] Department of Electronics and Communication Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq
[2,3] Electrical Engineering Department, College of Engineering, Mustansiriyah University, Baghdad, Iraq

[1]https://orcid.org/0000-0003-3655-06162
[2]https://orcid.org/0009-0009-5304-9514
[3]https://orcid.org/0000-0002-4981-8407
[*]Email: alifattah@uomustansiriyah.edu.iq

Article Info

Received	25/12/2023
Revised	15/08/2024
Accepted	20/08/2024

Abstract

This paper suggests a new image encryption algorithm based on block compressive sensing (BCS) and chaotic scrambling techniques. With compressive sensing (CS), signals can be sampled much lower than the Nyquist-Shannon rate while preserving their information content. BCS can be used as a one-step process by using a 3D logistic chaotic map, the measurement matrix is used as a secret key for encryption. BCS algorithm used an individual image reconstruction algorithm that leverages l_1norm minimization to promote signal sparsity, and a smoothing operator to enhance image quality. An encrypted image is first decomposed into three sub-images based on the tricolor theory; then, a discrete wavelet transform is used to sparsely process the three decomposed images. A 2D Henon map is used to scramble the compressed image after compression. This process further enhances the security of the system by increasing the complexity of the encryption process. The results showed that the proposed system provides better security and has a lower computational complexity than other methods. Furthermore, the proposed system is resistant to known attacks such as brute force and statistical attacks.

Keywords: Block Compressive Sensing; Scrambling; Chaotic System; Image Encryption

1. Introduction

In recent years, information security has received more and more attention due to the development of science and technology. AL-Hussain and Mahmood [1] presented the spectrum sensing techniques with wideband signals and discussed energy detection with compressive sensing (CS). AlAzawi and Kadhim [2] used speech scrambling with chaotic techniques to decrease the Segmental Spectral Signal to Noise ratio. While Hatem [3] used CS in one step to present a combine's compression and encryption Moreover, various methods of information encryption have been proposed to prevent leakage of information during transmission and storage. There is also an important role for image encryption in this field. Double random phase encryption was first proposed by Refregier and Javidi in 1995[4]. As a consequence, Image encryption systems use a variety of optical transformations [5]-[8]. Abdul-Kareem and Al-Jawher [9] proposed a new algorithm based on two chaotic systems, GWO, and CS for image compression and encryption to provide effective image protection and reduce redundant data. Decryption can be accomplished by attacking the image outline when the ciphertext and other data are known [10]. There have been several new image encryption methods proposed over the past few years [11]-[22] to increase the security of encryption systems. Fourier transforms with phase-truncation have been used in cryptosystems, Photon-counting polarimetric methods, ghost imaging theory, and optical interference techniques have been proposed [11]-[17]. The field of image encryption has seen several new principles and techniques proposed in recent years, some of them using QR code and digital holography for quadrature phase coding [18]-[22]. The QR Code principle has been used for many purposes, but it has also been suggested for use in image encryption. QR Code can be used to encrypt image information to ensure its security and difficulty for hackers to decode. This type of encryption makes it possible to effectively protect the data in images. As for digital holography, quadrature phase encryption refers to the use of encryption techniques in the stages of digital image processing, such as converting images into three-dimensional holograms, which adds a layer of complexity and security to the data contained in the images [23].

These innovations and principles in the field of image encryption reflect the ongoing development in the field of information security and the ongoing quest to develop more effective and secure encryption techniques to protect sensitive data.

Using diffraction imaging, researchers have recently discovered an optical image encryption and conversion method proposed by Unde et al [24]. Several optical encryption schemes have been proposed in the field of compressed sensing theory and optical encryption methods at present, and both of these fields are very active fields [25]-[26]. In 2006, compressive sensing [27] was introduced in the field of digital image processing. The Nyquist sampling theorem is broken by compressive sensing because it allows us to reconstruct original signals from just a few measurements. Signal processing has benefited greatly from it. As a result, the original signal can be reduced to a few small measurements, saving time and space in transmission and storage. Since with the information contained in these measurements [28], the original signal can be recreated. Image encryption also uses compressed sensing [29], [30]. The signal itself must be sparse or be able to be sparsely processed for compressive sensing to be successful. To implement sparse processing, it is necessary to process the original signal sparsely first if it is not sparse but can be sparsely processed. There are many redundant details in an image that can be compressed using compressed sensing in the field of image processing. Grayscale images make up the plaintext of images encrypted using compressed sensing, while measurement matrices provide the key information.

The contribution of this work can be summarized as:

1. The first step in the decomposition process is to decompose the original color image into three sub-images (R, G, and B) by the theory of tricolor. A discrete wavelet transform (DWT) is used to decompose the sub-images sparsely.
2. Block Compressive Sensing (BCS) can be used as a one-step process for encryption by using the measurement matrix as a secret key which is generated using the 3D logistic chaotic map. BCS algorithm used an individual image reconstruction algorithm that leverages l_1 norm minimization to promote signal sparsity, and a smoothing operator to enhance image quality.
3. Scrambling technique based on 2D Henon chaotic map is used as second-level security which is applied for the compressed image.
4. The proposed system is compared with traditional image encryption based on CS in PSNR, SSIM, key space analysis, and time encryption.

The remainder of the paper is organized as follows: CS and chaotic systems are discussed in Section 2; Compressive Sensing and Scrambling Algorithms are explained in Section 3.

2. Compressive Sensing

A mathematical theory of compressive sensing (CS) [31] is considered in this section. The theory of CS is founded on the principle of signal sparsity. Consider a real-valued n-dimensional signal $x \in \mathbb{R}^n$ with a sparsifying transform$\Psi \in \mathbb{R}^{n\times n}$. The n-dimensional coefficient vector θ is calculated by $\theta = \Psi x$. We say that x is a k-sparse signal in the transform domain Ψ if the coefficient vector θ has k non-zero coefficients (k << n). The k value is calculated as $k = \|\theta\|_0$ where $\|.\|_p$ represents the $l_p$norm.

The theory of CS shows that it is possible to efficiently capture the important information contained within a signal that has a sparse nature, by using only a limited number of measurements. If $\Phi \in \mathbb{R}^{m\times n}$ is a measurement matrix with m less than n, then the signal x can be acquired through non-adaptive, linear measurements. This is represented by $y = \Phi x$, where $y \in \mathbb{R}^m$ (m < n) is the set of the compressive sensing measurements. The problem of retrieving the sparse signal x from the measurement vector y is challenging because m < n and the equations are underdetermined. This leads to an infinite number of solutions, making efficient signal reconstruction impossible without adding the signal sparsity as a constraint.

CS theory states that the k-sparse signal x can be reconstructed exactly with great probability through convex optimization, if $m \geq ck\ ln(n)$, where c is a constant value. Let's define the ratio m/n as the compression ratio in the CS. then the correct signal recovery is achieved by solving the following optimization problem,

$$\underset{\theta}{\mathrm{Min}}\|\theta\|_0 \quad subject\ to\ \ y = \Phi x = \Phi\Psi^{-1}\theta \tag{1}$$

Where $\Psi^{-1}$is the inverse transform of Ψ matrix.

It has been demonstrated that the limited isometry property (RIP) of a measurement matrix Φ can aid in signal recovery [31] when the measurement matrix is maximally incoherent concerning the transform matrix Ψ.

3. Block Compressive Sensing and Scrambling Algorithms

3.1. Creation of the Measurement Matrix

The matrix of measurement Φ is produced using the three-dimensional chaotic logistic map [32], which is described by:

$$\begin{cases} x_{i+1} = \alpha x_i(1-x_i) + \beta y_i^2 x_i + \gamma z_i^3 \\ y_{i+1} = \alpha y_i(1-y_i) + \beta z_i^2 y_i + \gamma x_i^3 \\ z_{i+1} = \alpha z_i(1-z_i) + \beta x_i^2 z_i + \gamma y_i^3 \end{cases} \tag{2}$$

Where $x_i, y_i, z_i \in [0,1]$ are the values of the ith iteration of the 3D logistic map. α, β, γ are the control parameters that satisfy the range [3.53, 3.81], [0, 0.022], and [0, 0.015], respectively to get the 3D logistic map as chaotic behavior.

To maintain the variables of the 3D chaotic logistic map within the range of 0 and 255, the three variables are multiplied by the factor 10^7 and then take the mod operation with 256 as follows:

$$\begin{cases} x_{i+1} = mod\left((x_{i+1} * 10^7), 256\right) \\ y_{i+1} = mod\left((y_{i+1} * 10^7), 256\right) \\ z_{i+1} = mod\left((z_{i+1} * 10^7), 256\right) \end{cases} \tag{3}$$

The z_i variable is used as a switching control to select either x_i or y_i and the following modification is applied to it:

$$sel = mod(floor(z_{i+1}), 2) \quad (4)$$

In each ith iteration, if sel =0 the measurement matrix Φ takes x_{i+1}, else (sel=1) y_{i+1} is taken. Therefore, the matrix Φ takes either x or y depending on the z value, and the result is written as:

$$\Phi = \begin{pmatrix} (x_1, y_1) & \dots & (x_{m(n-1)+1}, y_{m(n-1)+1}) \\ \vdots & \ddots & \vdots \\ (x_m, y_m) & \cdots & (x_{mn}, y_{mn}) \end{pmatrix} \quad (5)$$

3.2. Block Compressive Sensing-Based Image Reconstruction

A block compressive sensing (BCS) method is an iterative reconstruction algorithm proposed in [24] by Unde. in which the image I∈ $\mathbb{R}^{N_1 \times N_2}$ is divided into A×A blocks which are sampled independently with identical or unlike measurement matrices. Suppose s_i is a vector representation of ith A×A block with n =A2 pixels after raster scanning. Suppose Φ_A is a $m_A \times n$ measurement matrix, where m_A is the number of measurements occupied per block. The projection of s_i onto Φ_A is $z_i = \Phi_A s_i$.

FOCUSS (FOcal Underdetermined System Solver) is an iterative algorithm commonly used in compressed sensing for sparse signal reconstruction. It is often used in conjunction with the BCS framework. In some cases, the straightforward application of FOCUS in the BCS framework can lead to severe blocking artifacts. This is because FOCUS assumes that the signal is sparse in the time domain and uses a soft thresholding technique to enforce sparsity. However, when applied to individual blocks, this can result in sharp edges at the block boundaries, which can cause noticeable artifacts. In problem in the FOCUS algorithm can be expressed as [20]:

$$\min_{\theta_i} \|\theta_i\|_1 \quad s.t. \quad z_i = \Phi_A \Psi^{-1} \theta_i \quad (6)$$

To solve this problem, the Lagrangian method is proposed to recover the original signal according to $s_i = \Psi^{-1}\theta_i$, where each block is solved independently. For each iteration, the reconstruction problem as depicted in [20] is expressed as

$$\min_{s_i} f(s_i) = \|\Psi s_i\|_1 \quad s.t. \quad z_i = \Phi_A s_i \quad (7)$$

Eq. (8) As a result, sparse solutions are obtained by minimization of the l_1 norm of the signal relative to the sparsity basis Ψ under equality constraints. For each iteration, the Lagrangian method is used to solve Eq. (8), and Wiener filtering is utilized for the smoothing operator. The recursive form of the reconstructed signal for ith iteration is derived in [20] and can be expressed as

$$s_i^{(K+1)} = \Psi^{-1}\Pi^{-1}\left(s_\psi^{(K)}\right) B_{\psi\phi}^T \left(B_{\psi\phi}\Pi^{-1}\left(s_\psi^{(K)}\right) B_{\psi\phi}^T\right)^{-1} z_i \quad (8)$$

Where Ψ is sparsifying transform, $\Pi^{-1}\left(s_\psi^{(K)}\right) = diag\left(\left|s_\psi^{(K)}\right|\right)$, $B_{\psi\phi} = \Phi_A \Psi^{-1}$, and $s_\psi = \Psi s_i$. Algorithm 1 shows the BSC-based FOCUSS algorithm for the Kth iteration in conjunction with the Wiener filtering.

Algorithm 1 : BCS-FOCUSS Algorithm

```
function $s^{(K+1)}$=BCS_FOCUSS ($s^{(K)}$, z, $\Phi_A$, Ψ)
    $\hat{s}^{(K)} = Wiener\ (s^{(K)})$
    for each block i
    $B_{\psi\phi} = \Phi_A \Psi^{-1}$
    $s_\psi = \Psi \hat{s}_i$
    $\Pi^{-1}(s_\psi^{(K)}) = diag(|s_\psi^{(K)}|)$
        $s_i^{(K+1)} = \Psi^{-1}\Pi^{-1}(s_\psi^{(K)})B_{\psi\phi}^T\ (B_{\psi\phi}\Pi^{-1}\ (s_\psi^{(K)})B_{\psi\phi}^T)^{-1} z_i$
```

3.3. Scrambling-based 2D Henon-Sine chaotic map

The 2D Henon-Sine chaotic map that is described in [33] is used to generate the permutation index for scrambling the signal which is defined by:

$$\begin{cases} x_{i+1} = (1 - a\ sin^2(x_i) + y_i)\ mod\ 1 \\ y_{i+1} = b\ x_i\ mod\ 1 \end{cases} \quad (9)$$

where the a and b parameters have the range $(-\infty, +\infty)$.

The algorithm of scrambling and descrambling functions is described in algorithm 2. In the first, the initialization of x(1), y(1), a, and b of the 2D Henon-Sine chaotic map is set. Then equation (9) is used to generate the chaotic sequence of length t1*t2, where t1 and t2 are the row and column number of the input matrix sin. sort function is applied to the x sequence to produce the index permutation (IP) vector that is used to scramble the input matrix after being converted to a 1D vector using the reshape function when sel=0. When sel=1 the algorithm is used to descramble the input matrix. The same key, IP, is used to descramble the scrambling matrix.

Algorithm 2: Scrambling and Descrambling algorithm

```
function $s_{out}$=scrambling_descrambling ($s_{in}$, sel)
 [t1,t2]=size($s_{in}$)
 % initialization $x(1), y(1)$, a, b, L=t1*t2
for each i=1:L-1
 applied equation (6)
[~, IP]=sort (x)
if sel=0
xr=reshape($s_{in}$, 1, t1*t2);
xs=xr(IP);
$s_{out}$=reshape(xs, t1, t2);
else
sr=reshape($s_{in}$, 1, t1*t2);
sd(IP)=sr;
sout=reshape(sd, t1,t2);
end
```

4. Proposed Image Encryption System Based on Compressive Sensing

Fig. 1 shows the proposed image encryption and decryption algorithm based on CS and scrambling techniques that are explained in the previous section.

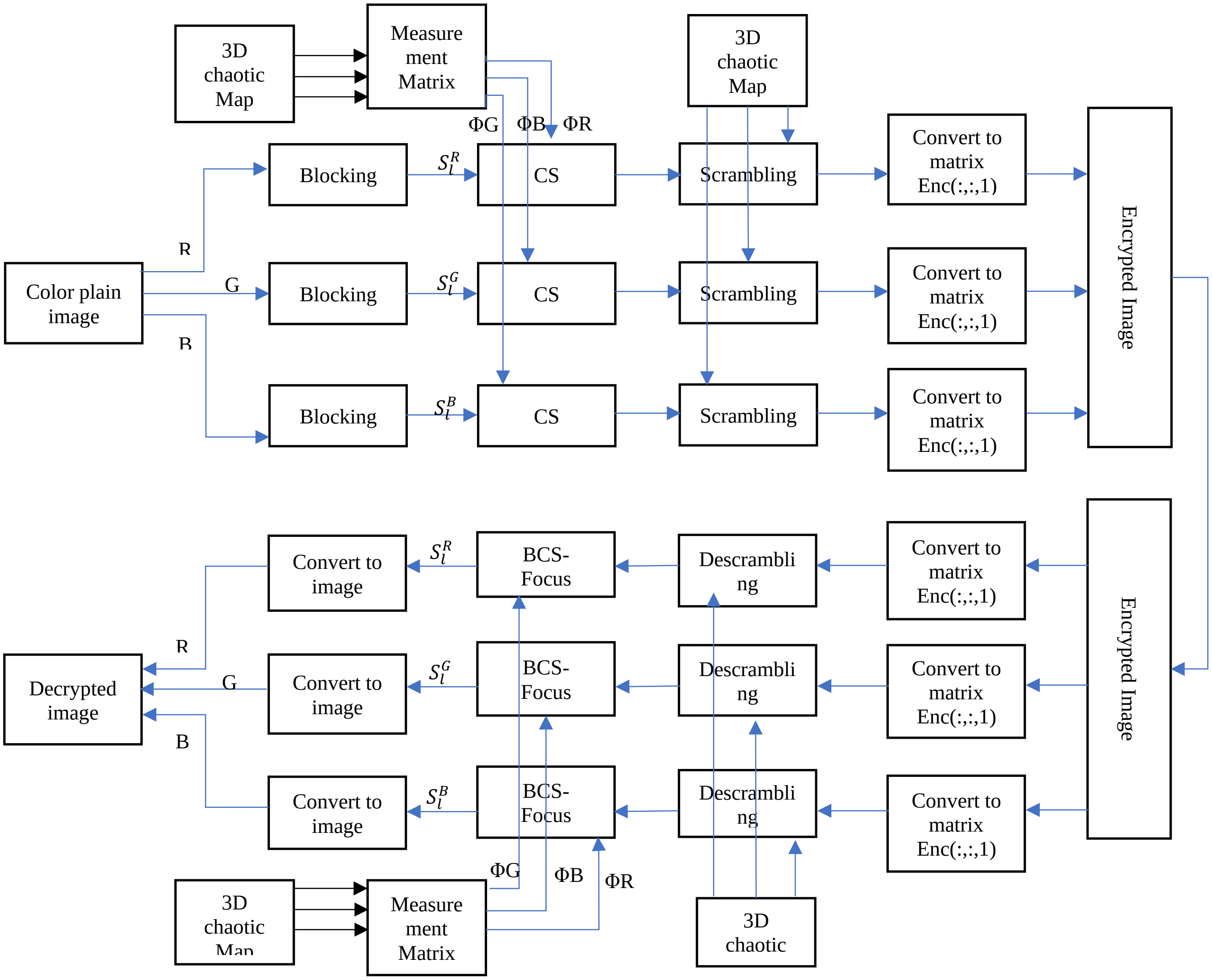

Figure 1. Image encryption and decryption system.

4.1. Encryption Algorithm

The encryption process comprises several steps:

Step 1: Color image decomposition. According to tricolor theory, color images are divided into three sub-images (R, G, and B).

Step 2: The input three channels I1, I2, I3 of size (N1×N2) for each is divided into non-overlapping blocks of a specified size (A×A) and each block is reshaped to a column vector, s_i, i=1,.., A2.

Step 3: In the domain of Discrete Wavelet Transforms (DWT), sparse representation is present. Sub-images are treated using DWT according to Eq. (2), where I1, I2, and I3 exhibit sparsity, meaning that a significant portion of their elements are zero. The small number of non-zero coefficients in these transformed sub-images indicates that most of the information in the sub-images is concentrated in one or a few coefficients.

Step 4: The random measurement matrix (Φ_A) is generated according to subsection (4.1) and used to compress the image block by projecting it onto a lower-dimensional subspace, reducing the amount of data needed to represent the image. The compressed image is expressed as $z_i = \Phi_A s_i \in \mathbb{R}^{1\times CR.A^2}$, where CR is the compression ratio.

Step 5: The ith compressed image, z_i, is then scrambled using a proposed scrambling algorithm based on the 2D Henon map that is explained in Algorithm 2. The ith scrambled vector, c_i, is defined as

$c\_i = scrambling\_descrambling\ (z\_i, 1)$ (10)

Step 4: The ith encrypted image is obtained by reshaping the scrambling vector to the matrix of size (A×A), Ei $\in \mathbb{R}^{A\times A}$.

4.2. Decryption Algorithm

The decryption process comprises several steps:

Step 1: The ith encrypted image is reshaped to vector, $\hat{c}_i \in \mathbb{R}^{1\times(A^2)}$.

Step 2: The ith encrypted vector, $\hat{c}_i$, is then descrambled using a proposed scrambling algorithm based on the 2D Henon map that is explained in Algorithm 2. The ith descrambled vector, $\hat{z}_i$, is defined as

$\hat{z}\_i = scrambling\_descrambling\ (\hat{c}\_i, 2)$ (11)

Step 3: BCS-FOCUSS Algorithm that is processed in Algorithm 1 is used to reconstruct vector $\hat{s}_i \in \mathbb{R}^{1\times A^2}$.

Step 4: reshaping the reconstructed vector into a block image and reshaping the block matrix to decrypted image $\hat{\mathrm{I}} \in \mathbb{R}^{N_1\times N_2}$

5. Experimental Results and Analysis

As a test platform, we chose the Barbara picture with 256 x 256 pixels as plaintext, and MATLAB (R2020b) was used for the experiment.

The secret key parameters include: the 3D Logistic chaotic map (x_0=0.9455233676, y_0=0.34556674, and z_0= 0.56763883, α=3.6, β=0.0012, and γ=0.0012), 2D Henon chaotic map (x_0=0.977857033414, y_0==0.564792, a = 1.4, and b = 0.3). Using BCS, we sample 32×32 pixels for each block if they are not overlapping and use DCT as the sparsifying transform. Assume CR = 0.25. and number of DWT=5.

Fig. 2 shows the original images. and the color plaintext, its red channel green, and blue channels, respectively R, G, and B.

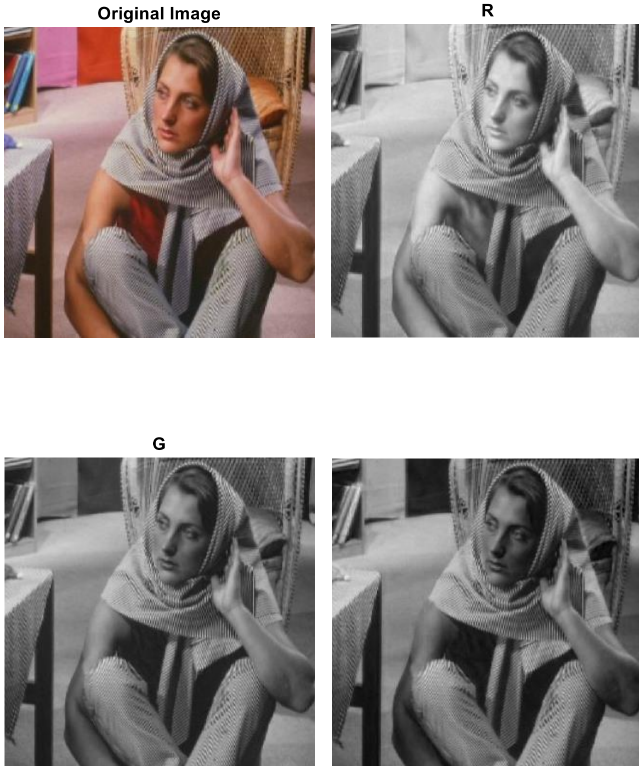

Figure 2. The original image an RGB channels

Fig. 3 shows the decryption results when all the keys are correct.

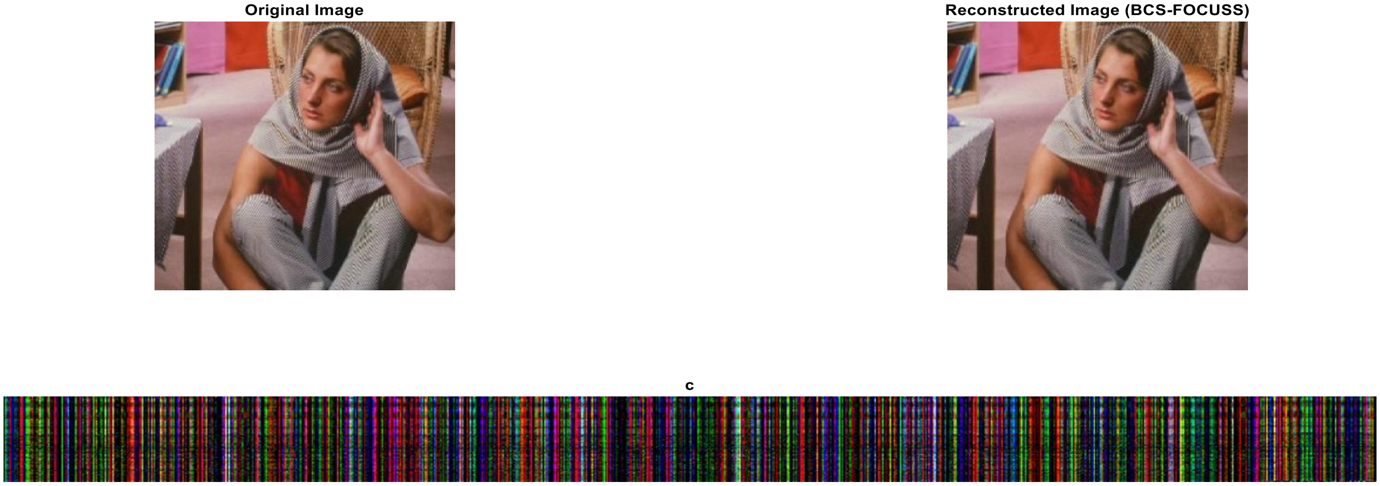

Figure 3. Original and reconstructed image and cipher image

As shown in Fig. 3(a) represents the ciphertext. A decrypted R and G component as well as B and color images can be seen in Fig. 3(b)-(e). We performed grayscale histogram analysis on three original images, including the encrypted image and its three counterparts, to objectively analyze the effects of the decrypted image. R, G, and B channels of the original image were analyzed.

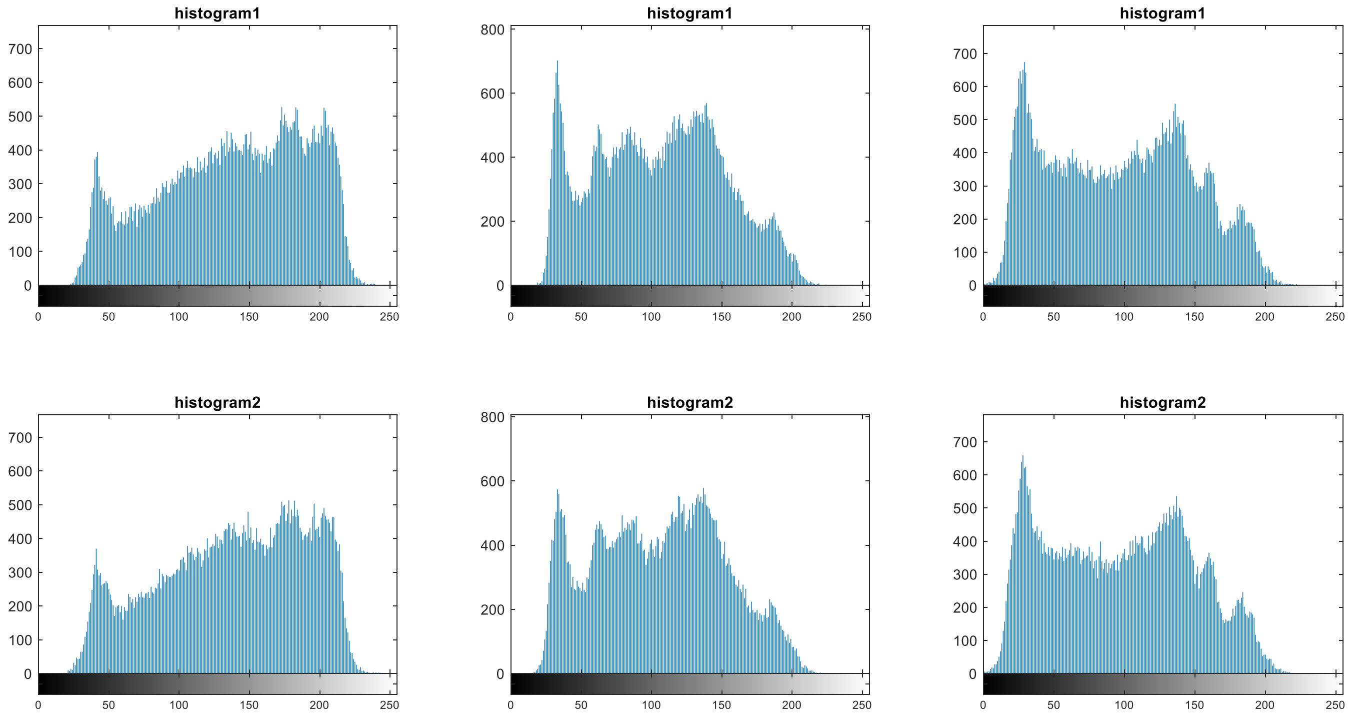

Figure 4. The grayscale histograms of (a) original R, (b) original G, (c) original B, (d) recovered R, (e) recovered G, and (f) recoveredB.

Fig. 4(a)–(c) depicts the grayscale histograms of the original R, G, and B images, represented as the original image histograms. Additionally, Fig. 4(d)–(f) displays the grayscale histograms of the three decrypted images, corresponding to the R, G, and B channels, respectively

A grayscale histogram involves counting pixels in a digital image based on their grayscale values, providing insights into the distribution of grayscale tones. In Fig. 4, it is evident that the grayscale histogram distributions of the three decrypted images closely resemble those of the original images. Furthermore, the peak positions in both sets of histograms are identical.

5.1. Peak signal-to-noise ratio (PSNR) Results

The assessment of the decrypted image quality is frequently conducted through PSNR, which is defined by.

$$PSNR = 10log\frac{255^2}{\frac{1}{N_1N_2}\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}(I(i,j)-\hat{I}(i,j))^2} \qquad (12)$$

The dimensions of the image are N_1 and N_2, and the pixel values of the original image are I(i, j) and Î(i, j). The decrypted image will have lower distortion if the PSNR is higher.

Table 1 shows the PSNRs (dB) of the proposed system for different CRs = 0.4, 0.55, 0.7 with different BARBARA images in comparison with different conventional schemes. From this table, it can be noticed that the suggested algorithm gives a higher value of PSNR (dB).

Table 1. PSNRs (dB) comparisons for different 256×256 images and CR.

Images (256×256)	CR		Ours	MRAMP	SAMP	OMP
BARBARA	0.4	R	26.6	20.1	24.7	25.6
		G	26.9	21.2	25	24.4
		B	26.9	21.8	25.2	24
	0.55	R	28.5	27.2	26.3	29
		G	28.7	27.2	26.8	26.6
		B	28.8	26.8	26.6	26.4
	0.7	R	31.1	29.6	26.4	29
		G	31.4	31.4	27.3	29.1
		B	31.4	30.2	26.9	28.8

In Table 2, the correlation coefficients for R, G, and B channels increase as compression ratios increase and the correlation coefficient is shown in the equation below.

$$r_1 = \frac{\sum_i(x_i-x_m)(y_i-y_m)}{\sqrt{\sum_i(x_i-x_m)^2}\sqrt{\sum_i(y_i-y_m)^2}} \qquad (13)$$

Images 1 and 2 are referred to by their intensity values as x_i, y_i, x_m, and y_m, respectively, where x_i is the intensity of the i^{th} pixel in image 1, and y_i is the intensity of the i^{th}pixel in image 2.

As a result, higher compression ratios are associated with better image recovery. The higher the compression ratio, the more image information is retained, resulting in better recovery results.

Table 2. Coefficients of correlation between recovered images and original images using different reconstruction methods.

Images (256×256)	**CR**		**Ours**	**MRAMP**	**SAMP**	**OMP**
BARBARA	0.4	R	0.9640	0.9590	0.9637	0.9559
		G	0.9601	0.9506	0.9627	0.9549
		B	0.9605	0.9502	0.9655	0.9608
	0.55	R	0.9862	0.9860	0.9749	0.9800
		G	0.9853	0.9842	0.9727	0.9765
		B	0.9846	0.9831	0.9742	0.9782
	0.7	R	0.9904	0.9903	0.9768	0.9851
		G	0.9902	0.9897	0.9742	0.9843
		B	0.9892	0.9888	0.9762	0.9834

5.2 NPCR and UACI

In NPCR, which stands for Number of Pixels Change Rate, it indicates that a given pixel in a plain image has changed a certain number of times. A cryptosystem can resist plain-text attacks if NPCR converges, which shows more sensitivity to plain-text changes. These two metrics are calculated by dividing the difference in intensity between the plain and cipher images by the UACI value.

$$UAC = \frac{1}{\text{Width} \times \text{Height}} \sum_{i,j} \left(\frac{c_1(i,j) - c_2(i,j)}{255} \right) \times 100\% \quad (14)$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{\text{Width} \times \text{Height}} \times 100\% \quad (15)$$

$\mathrm{c1(i,j)}$ and $\mathrm{c2(i,j)}$ An encrypted image before and after changing one pixel of a plain image. A pixel's value after changing is shown in Table 3.

Table 3. UACI and NPCR values of test images

Test images	**NPCR (%)**	**UACI (%)**
Barbara	99.6	33.48
Peppers	99.62	33.46

5.3. Time of encryption algorithm

Time encryption algorithms are among the most interesting and challenging algorithms to develop in different fields. Based on different images, Table 4 shows the encryption time of the proposed algorithm with CR = 0.25.

Table 4. Encryption time with different images (unit: s).

Images	**Time**
Barbara	0.046443
Peppers	0.020311

5.4. Key Space Analysis

The key space (KS) is the size of the total of all parameters utilized in the encryption system. The KS should be greater than 200^{100} to robust against brute-force attacks [20], [33]. In our system, the secret key consists of the 3D Logistic chaotic map parameter $(\alpha, \mu, \gamma,\ x_0, y_0, z_0)$ and 2D henon chaotic map (a, b, x_0, y_0). Using the IEEE-754 standard with double precision, each parameters take 10^{-15}, therefore, $(10^{15})^{10} \approx 2^{489}$. Therefore, the suggested algorithm can resist brute-force attacks.

6. Conclusion

This paper introduced a new image encryption algorithm based on CS and scrambling techniques. Using a 3D Logistic chaotic map system to generate the measurement matrix. Block compressive sensing (BCS) algorithm is proposed in this work in which an individual image reconstruction algorithm that leverages l_1 norm minimization to promote signal sparsity, and a smoothing operator to enhance image quality. The compressed image was scrambled using the 2D Henon map for better security. A fast image encryption algorithm was developed using this method and a 3D logical chaotic map system. Using simulation results, the proposed algorithms have a high probability of resisting a brute-force attack and of recovering good images with minimal measurement requirements. In addition, this algorithm has a faster encryption time than most others. Due to its good encryption effect, the proposed encryption algorithm is suitable for real-time applications. In the field of cryptography, index modulation coupled with a 5D chaotic map presents an intriguing avenue for future research.

Acknowledgment

The authors would like to thank the Electrical Engineering Department in the College of Engineering at Mustansiriyah University, and the Department of Electronics and Communication Engineering, in the University of Baghdad for help and support to achieve this article.

Author Contribution Statement

Asaad H. Sahar: proposed the research problem and supervised the findings of this work. Authors Hussein A. Hussein Al-Delfi, and Ali F. Hassoon: participated in implementing calculations and algorithms. Results and contributions to the final manuscript were discussed by both authors.

Conflict of interest

The authors confirm that the publication of this article causes no conflict of interest.

References

[1] A. Mohammad A. AL-Hussain and M. K. Mahmood, "Spectrum Sensing of Wide Band Signals Based on Energy Detection with Compressive Sensing," *Journal of Engineering and Sustainable Development*, vol. 24, no. 6, pp. 83–90, Feb. 2022, https://doi.org/10.31272/jeasd.24.6.7.

[2] K. M. AlAzawi and J. Q. Kadhim, "Speech Scrambling Employing Lorenz Fractional Order Chaotic System," *DOAJ (DOAJ: Directory of Open Access Journals)*, vol. 17, no. 4, Oct. 2013.

[3] H. R. Hatem, “Color Image Compression and Encryption Based on Compressive Sensing,” *Journal of Engineering and Sustainable Development*, vol. 22, no. 1, 2018, Available: https://jeasd.uomustansiriyah.edu.iq/index.php/jeasd/article/view/337/267

[4] P. Refregier and B. Javidi, “Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding,” *Optics Letters*, vol. 20, no. 7, pp. 767–769, Apr. 1995, https://doi.org/10.1364/OL.20.000767.

[5] B. Hennelly and J. T. Sheridan, “Optical Image Encryption by Random Shifting in Fractional Fourier Domains,” *Optics Letters*, vol. 28, no. 4, p. 269, Feb. 2003, https://doi.org/10.1364/ol.28.000269.

[6] N. Singh and A. Sinha, “Gyrator transform-based Optical Image encryption, Using Chaos,” *Optics and Lasers in Engineering*, vol. 47, no. 5, pp. 539–546, May 2009, https://doi.org/10.1016/j.optlaseng.2008.10.013.

[7] A. Dawood, Q. Thabit, and T. Fahad, “A Comprehensive Review of Color Image Encryption Technology,” *Basrah Journal for Engineering Science*, vol. 23, no. 1, pp. 56–63, Jul. 2023, https://doi.org/10.33971/bjes.23.1.8.

[8] Q. Thabit, Alaa Al-saffar, and I. Abed, “A New DNA strand-based Encryption Algorithm Using Symmetric Key Generation Table,” *Al-Qadisiyah Journal for Engineering Sciences*, vol. 15, no. 1, pp. 032–037, Jan. 2022, https://doi.org/10.30772/qjes.v14i4.803.

[9] A. A. Abdul-Kareem and W. Ameen, "Hybrid Image Encryption Algorithm Based on Compressive Sensing, Gray Wolf Optimization, and Chaos," *Journal of Electronic Imaging*, vol. 32, no. 04, Aug. 2023, https://doi.org/10.1117/1.jei.32.4.043038.

[10] Y. Frauel, A. Castro, T. J. Naughton, and Bahram Javidi, “Resistance of the Double Random Phase Encryption against Various Attacks,” *Optics Express*, vol. 15, no. 16, pp. 10253–10253, Jan. 2007, https://doi.org/10.1364/oe.15.010253.

[11] E. G. Abdulkadhim, S. H. Dhahi, and M. S. Al-Shemarry, “Review on Various Image Protection Methods,” *Journal of Al-Qadisiyah for Computer Science and Mathematics*, vol. 15, no. 4, Dec. 2023, https://doi.org/10.29304/jqcsm.2023.15.41364.

[12] A. F. Mohamed, F. Wanis, and Mohamed Mahmoud Ashour, “Enhance Watershed Algorithms Using Principal Component Analysis Capabilities,” *Al-Qadisiyah Journal for Engineering Sciences*, vol. 17, no. 1, pp. 5–15, Mar. 2024, https://doi.org/10.30772/qjes.2024.145116.1055.

[13] Y. Xiong, J. Gu, and R. Kumar, “Collision in a phase-only Asymmetric Cryptosystem Based on Interference and phase-truncated Fourier Transforms,” *Optical and Quantum Electronics*, vol. 55, no. 8, Jun. 2023, https://doi.org/10.1007/s11082-023-04943-1.

[14] A. Pedram, V. R. Besaga, F. Setzpfandt, and Ö. E. Müstecaplıoğlu, “Nonlocality Enhanced Precision in Quantum Polarimetry via Entangled Photons,” *Advanced Quantum Technologies*, Aug. 2024, https://doi.org/10.1002/qute.202400059.

[15] W. Zhang, X. Qiu, D. Zhang, and L. Chen, “Visualizing the Hardy’s Paradox Using Hyper-Entanglement-Assisted Ghost Imaging,” *Laser & Photonics Review*, vol. 17, no. 11, Sep. 2023, https://doi.org/10.1002/lpor.202200865.

[16] X. Huang, Y. Xu, Y. Bai, and X. Fu, “Fast Focusing Method in Ghost Imaging with a Tracking Trajectory,” *Optics Letters*, vol. 48, no. 21, pp. 5543–5543, Oct. 2023, https://doi.org/10.1364/ol.503027.

[17] A. Sdobnov *et al.*, “Polarization-based Optical Interference Approach For Differential Diagnosis Of Benign And Malignant Tumours” *Optics and Lasers in Engineering*, vol. 171, pp. 107806–107806, Dec. 2023, https://doi.org/10.1016/j.optlaseng.2023.107806.

[18] M. H. Alhayani, “Real-Time Objects Detection, Tracking, and Counting Using Image Processing Techniques,” *Al-Nahrain Journal for Engineering Sciences*, vol. 26, no. 1, pp. 24–30, Feb. 2023, https://doi.org/10.29194/njes.26010024.

[19] A. A. Almindelawy and M. H. Ali, “Improvement of Eye Tracking Based on Deep Learning Model for General Purpose Applications,” *Al-Nahrain Journal for Engineering Sciences*, vol. 25, no. 1, pp. 13–19, Apr. 2022, https://doi.org/10.29194/njes.25010012.

[20] Q. Xu, K. Sun, S. He, and C. Zhu, “An Effective Image Encryption Algorithm Based on Compressive Sensing and 2D-SLIM,” *Opt. Lasers Eng.*, vol. 134, pp. 106178–106178, Nov. 2020, https://doi.org/10.1016/j.optlaseng.2020.106178.

[21] W. Chen, Q. Li, X. Tang, and Q. Pan, “A Digital Watermarking Method for Medical Images Resistant to print-scan Based on QR Code,” *Multimedia Tools and Applications*, vol. 83, pp. 52197–52218, Nov. 2023, https://doi.org/10.1007/s11042-023-17155-2.

[22] T. Li, Q. Zhao, Y. Wang, H. Zhang, S. Liu, and Y. Su, “Image Sequence Encryption Based on Chaotic Fingerprint Phase Mask and single-shot Digital Holography,” *Journal of Optics*, vol. 52, no. 3, pp. 1608–1619, Dec. 2022, https://doi.org/10.1007/s12596-022-01064-y.

[23] I. Muniraj *et al.*, “Low Photon Count Based Digital Holography for Quadratic Phase Cryptography,” *Optics letters/Optics index*, vol. 42, no. 14, pp. 2774–2774, Jul. 2017, https://doi.org/10.1364/ol.42.002774.

[24] A. S. Unde and P. P. Deepthi, “Block Compressive sensing: Individual and Joint Reconstruction of Correlated Images,” *Journal of Visual Communication and Image Representation*, vol. 44, pp. 187–197, Apr. 2017, https://doi.org/10.1016/j.jvcir.2017.01.028.

[25] Y. Luo *et al.*, “A Robust Image Encryption Algorithm Based on Chua’s Circuit and Compressive Sensing,” *Signal Processing*, vol. 161, pp. 227–247, Aug. 2019, doi: https://doi.org/10.1016/j.sigpro.2019.03.022.

[26] X. Zhang *et al.*, “Two-level image authentication by two-step phase-shifting interferometry and compressive sensing,” *Optics and Lasers in Engineering*, vol. 100, pp. 118–123, Jan. 2018, https://doi.org/10.1016/j.optlaseng.2017.08.002.

[27] D. L. Donoho, “Compressed Sensing,” *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006, https://doi.org/10.1109/tit.2006.871582.

[28] D. Needell and J. A. Tropp, “CoSaMP: Iterative Signal Recovery from Incomplete and Inaccurate Samples,” *Applied and Computational Harmonic Analysis*, vol. 26, no. 3, pp. 301–321, May 2009, https://doi.org/10.1016/j.acha.2008.07.002.

[29] N. Rawat, B.-H. Kim, Inbarasan Muniraj, G. Situ, and B.-G. Lee, “Compressive Sensing Based Robust Multispectral double-image Encryption,” *Appl. Opt.*, vol. 54, no. 7, pp. 1782–1782, Mar. 2015, https://doi.org/10.1364/ao.54.001782.

[30] T. Chen, M. Zhang, J. Wu, C. Yuen, and Y. Tong, “Image Encryption and Compression Based on Kronecker Compressed Sensing and Elementary Cellular Automata Scrambling,” *Optics & Laser Technology*, vol. 84, pp. 118–133, Oct. 2016, https://doi.org/10.1016/j.optlastec.2016.05.012.

[31] D. Maluenda, Artur Carnicer, R. Martínez-Herrero, Ignasi Juvells, and Bahram Javidi, “Optical Encryption Using photon-counting Polarimetric Imaging,” *Optics Express*, vol. 23, no. 2, pp. 655–655, Jan. 2015, https://doi.org/10.1364/oe.23.000655.

[32] W. Chen and X. Chen, “Marked Ghost Imaging,” Applied *Physics Letters*, vol. 104, no. 25, p. 251109, Jun. 2014, https://doi.org/10.1063/1.4879843.

[33] J. Wu, X. Liao, and B. Yang, “Image Encryption Using 2D Hénon-Sine Map and DNA Approach,” *Signal Processing*, vol. 153, pp. 11–23, Dec. 2018, https://doi.org/10.1016/j.sigpro.2018.06.008.