Optik - International Journal for Light and Electron Optics 272 (2023) 170341

Contents lists available at ScienceDirect

Optik - International Journal for Light and Electron Optics

journal homepage: www.elsevier.com/locate/ijleo

Original Research Article

Block based visually secure image encryption algorithm using 2D-Compressive Sensing and nonlinearity

Saumya Patel [*,1], Ankita Vaish[2]

Banaras Hindu University, Varanasi, (U.P.), India

ARTICLE INFO

Keywords:
2D-Compressive Sensing
Compression
Encryption
Visual security
Chaotic map

ABSTRACT

In this paper, a block division based visually secure encryption algorithm is proposed for color images. Each block is sparsified through an optimal orthogonal transformation. Block based 2D-Compressive Sensing is applied to collect the compressed samples which best represent the signal, sampling is done through a measurement matrix (MM) which is generated by a 2D-SLIM map. MM is optimized through the proposed optimization algorithm which minimizes the mutual coherence between sparsified basis and MM. These compressed samples are further encrypted through a DNA XOR operation. The compressed-encrypted information is decomposed into the four sub images which are embedded into the host image through integer wavelet transform. SHA-256 is used to generate the seed value of the chaotic map. At the receiver end, the secret information is extracted with the correct knowledge of the keys. The numerical results and robustness of the proposed work is analyzed and the superiority of the developed algorithm is shown by comparing it with some recent published papers.

1. Introduction

In the field of big era and cloud computing, a huge amount of information is transmitted and stored through public networks all over the world. Among all, images are considered as most effective way to represent the information, which contains intuitive and rich information. Especially in the area of medical imaging, satellite imaging, military, etc., most of the information is shared in the form of images, so the security and transmission of the images efficiently is most important. Image encryption techniques plays an important role in the field of data security. Due to the encryption, sensitive information can be transmitted securely without any kind of leakage and the encrypted information cannot be identified by other than the intended receiver. Compression can help in reducing the total number of bits by reducing/removing redundancies. Hence, efficient compression and encryption algorithms are needed. Generally, many image encryption algorithms introduced in the area of data security such as chaotic systems [1,2], DNA [3,4], optical encryption [5], etc. Most encryption algorithms convert the information to noise-like by changing the pixel values or disrupting the pixel values. These encryption algorithms generate encrypted information of the size of the plain image as shown in Fig. 1, due to the demand of the high quality image and access transfer of information in image form leads the high transmission cost and storage space, so compression of the information is necessary while maintaining the security.

In 2006, Donoho [6] has introduced compressive sensing (CS) theory as a new sampling and reconstruction algorithm, which compresses as well as encrypts the signal at lesser than the traditional Nyquist-sampling rate. CS based encryption algorithms are proven to be computationally secure but cannot obtain perfect security therefore, CS based encryption algorithms are combined with

* Corresponding author.
E-mail address: saumyapatel5@gmail.com (S. Patel).
[1] Research Scholar.
[2] Assistant Professor.

https://doi.org/10.1016/j.ijleo.2022.170341
Received 8 October 2022; Received in revised form 21 November 2022; Accepted 2 December 2022
Available online 10 December 2022

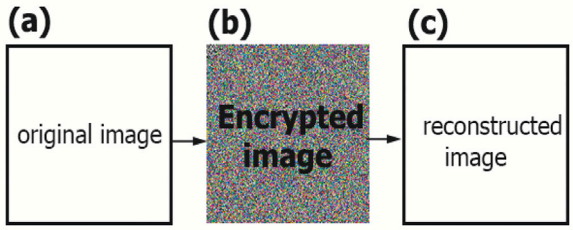

Fig. 1. Encryption.

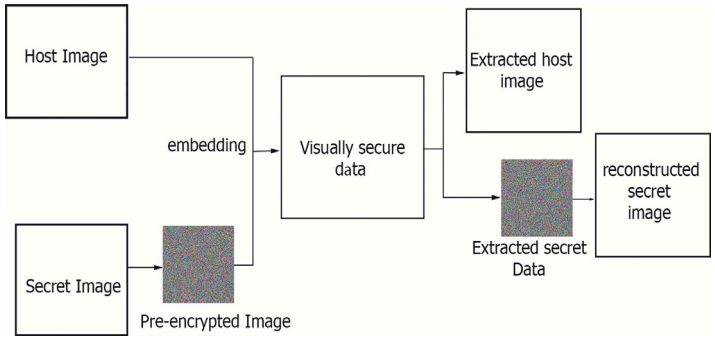

Fig. 2. Visual security.

chaotic systems [1,2], DNA [3,4], optical encryption [5], etc to obtain a more secure cipher image or noise like image. Measurement matrix acts as a key between sender and receiver due to which CS based algorithms comes under symmetric key encryption. This noise-like information is shared between the sender and receiver with a single or multiple secret key which makes information secure on the public network. The secret information is noise-like or texture-like information, which brings attention to the attackers that there is some secret information and thus the risk of information loss, manipulation, or leakage by hackers is increased significantly. To address this problem, the Visual Security (VS) of the information is introduced that produces a visually meaningful encrypted image (VMEI). Fig. 2 depicts the process of VS, from which it can be understood that the encrypted secret information is embedded into a plain image to obtain VMEI, and the information looks like an image on the network which will not bring the attention of the attackers.

2. Related work

Since CS theory was introduced, many image encryption algorithms based on CS have been introduced. For example, in 2011 Huang et al. [7] introduced an encryption algorithm based on CS. Chai et al. [8] have introduced an encryption algorithm that associates CS, chaos, and elementary cellular automata (ECA), in which, Discrete Wavelet Transform (DWT) is applied to transform the image into a sparse representation and then zig-zag scrambling and ECA are executed to permute the information at another level (or to enhance the scrambling degree). Chaotic random values are used to generate the measurement matrix (MM) for sampling and reconstruction. Another algorithm based on CS and chaos is introduced by Luo et al. [9], in which a new chaos-combined asymptotic deterministic random measurement matrices (CADRMM) is introduced for sampling and reconstruction. In [10], Zhou et al. have introduced an encryption algorithm that combines CS and random pixel exchanging, and a key-controlled circulant matrix is utilized as MM for sampling and reconstruction.

1D-CS reduces the dimension of the signal from only one direction whereas the dimensional reduction from both directions is also possible with the help of 2D-CS. In [11], Zhou et al. has introduced an image encryption algorithm based on 2D-CS and fractional Mellin transform (FMT), 2D-CS is applied for sampling which provides compression encryption in two directions and FMT further encrypts the measured values. Zhou et al. [12] have presented an encryption algorithm by combining 2D-CS and hyper-chaos, hyper-chaos is used for MM generation due to good randomness, and further, double encryption has been done to increase the security level. Another algorithm by combining 2D-CS and hyper-chaos is given by Xu et al. [13], in which SHA-512 hash values have been used to obtain the initial value of the chaotic map, and 2D-CS has sampled the plain image through the circulent MM. Further, the encrypted image is re-encrypted.

The above-mentioned algorithms convert the plain image into a noise-like image that attracts the eavesdropper that it contains some important information which is in encrypted form, due to which the information is unprotected visually. To solve this problem, VS of the image is first introduced by Bao et al. [14], in which at first the plain image is pre-encrypted to covert it into noise-like information through permutation and substitution. Then a two-dimensional Discrete wavelet transform (DWT) is applied on the

Table 1
Operational complexity and disk space.

	Operational complexity	Disk space
1D-CS	$O(M^2N^2)$	M^2N^2
Block 1D-CS	$O(mN^2)$	mn
2D-CS	$O(MN^2)$	$2MN$
Block 2D-CS	$O(mn^2)$	mn

host image, which divides the host image into four parts LL, LH, HL, and HH. The pre-encrypted image pixel values is divided into the two parts, *part* 1 keeps 10th and 100th place decimal value, *part* 2 keeps once place decimal value (for example 234 is a pixel value, after division *part* 1 = 23 *and part* 2 = 4) and *part* 1 is embed in the HL part and *part* 2 is embed in the HH part of the host image. At last, the inverse DWT is applied to the host image and gets a visually secure image. This algorithm has given a new direction, a direct replacement of the pixel values, to the VS. Many researchers introduced CS-based visually secure image encryption algorithms [15–17] but the reconstruction algorithm in CS takes a long time to reconstruct the signal due to the multiple iterations. Visual secure algorithms based on Block-CS (BCS) [18,19], parallel CS [20–22], and 2D-CS [23–25] are presented to overcome this problem. In [15], Chai et al. have presented a visually secure image encryption algorithm based on CS, in which CS is used for pre-compression encryption of the signal, and then the DWT-based embedding method is employed to provide the visual security. Ye et al. [16] have introduced a visually secure encryption algorithm, in which simultaneous compression–encryption is achieved through CS, and the embedding process is done by Schur decomposition. Chai et al. [17] have given an algorithm by combining CS and dynamic Least significant bit (LSB) embedding process. Although, CS-based visual secure encryption algorithms' computational complexity is high since 1D CS performs $O(M^2N^2)$ operation and requires M^2N^2 memory units to store the MM, where M, N is the size of the original image. In comparison to 1DCS, BCS performs $O(mN^2)$ operation and needs mn memory units for storing MM, where m, n is size of the sampled image. Pan et al. [19] have presented a visual BCS-based encryption algorithm, in which BCS is used for compression - encryption of the plain image and Discrete Cosine Transform (DCT) is utilized for the embedding process. Another BCS-based visually secure algorithm is given by Zhu et al. [18], in which SVD-based embedding process is employed to provide visual security. Moreover, some researchers have presented visually secure encryption algorithms based on parallel CS (PCS) as well. In [20], Want et al. have given an algorithm for visual security in which PCS has been used for sampling which provides compression, and DWT-based embedding has been utilized as visual security. Jiang et al. [21] have introduced an encryption algorithm based on the integration of PCS and visual security. Slat transform is used for hiding secret information in components of carrier image. Compared to 1D-CS, 2D-CS provides a high compression ratio, and computationally it requires $O(MN^2)$ operations and $2MN$ memory unit to store MM. Huo et al. [23] have presented an encryption algorithm that achieves visual security through 2D-CS and IWT. 2D-CS provides a high compression ratio and IWT provides security without any loss of information. Chai et al. [24,25] have introduced visually meaning full encryption algorithm for color images, in which 2D-CS is utilized as sampling and reconstruction technique through different MM. Thereafter, visual security is employed in [24,25] through IWT and DWT respectively.

In [24], at first the plain color image is decomposed into Red, Green, and Blue planes, and each plane has been compressed and encrypted in noise-like information through 2D-CS. After that, the noise-like information is divided into two sub-images according to the place value of the decimal number. IWT is applied on the color carrier image, the carrier image is further sub-divided into A, H, V, D. The H and V part of the each plane of the carrier image is replaced by the sub-images obtained by CS. Inverse IWT is applied to obtain the cipher image. This algorithm improves the visual effect of the image. However, there are still some issues such as the detailed information is lost due to the replacement of the H and V. In addition, this visual secure algorithm with 2D-CS does not consider the storage space of the MM, it can be seen from the Table 1 that 2D-CS requires $2MN$ storage space to store the MM. To address these problems, block-based 2D-CS is introduced to measure the pixel values which saves storage space to store the MM and makes the algorithm less computational, concurrently the reversibility virtue of the IWT has been used to embed the secret information and information has been hidden in the fractional part of the IWT decomposition.

In the above mentioned papers, 1D-CS, Block based 1D-CS, and 2D-CS have been used for sampling. From the Table 1, it can be understood that among them the 1D-CS is computationally high while the block-CS is computationally low. In contrast, Block-CS is less secure than 1D-CS and 2D-CS due to the block-size trade-off. Small block size facilities low operational complexity and less storage space, in contrast large block size facilitates high security. So, none of these methods can provide low computational complexity and high security at the same time because Block-CS provides ease of computational complexity but is less secure due to block trade-off whereas 1D-CS and 2D-CS are more secure than Block-CS but have higher computational complexity. Although CS can compress and encrypt the signal at the same time through less sampling but CS encrypt the signal via linear operation which does not provide high security against attacks. The motivation of this work is to utilize the virtues of block 2D-CS with non-linear DNA encoding operation. To make the algorithm more secure against attack, nonlinearity can be introduced along with the CS. In the proposed work the virtues of CS and nonlinear DNA are utilized due to the following reasons:

1. We have used the block-wise 2D-CS for sampling and reconstruction of the plain image which reduces the operational complexity of the algorithm. 2D-CS have high compression ratio then the block-CS and 1D-CS. Further, block-wise operation make it computationally low. Hence, in the proposed algorithm the plain image is sub-divided into the 8×8 non-overlapping blocks.
2. Block-based 2D-CS is less secure due to block-size trade-off and 2D-CS provides encryption through linear operation which is also less secure. To address this problem row and column wise DNA coding has been applied which is non-linear operation and improves the security.

3. SHA-256 hash function values of the secret image are used to evaluate the seed value of the chaotic map which will make the algorithm more sensitive and maintain a dependency between the original image and encryption algorithm.
4. MM is generated through the infinite collapse modulation map (2D-SLIM) [26] and an proposed optimization technique will make MM more incoherent and highly satisfy the RIP condition. Incoherence is the necessary condition for the MM. The lower the incoherence of the MM, the better reconstruction is possible. In the proposed algorithm, block-wise 2D-CS is used for sampling which requires less space for MM storage.
5. The block-based 2D-CS algorithm converts the secret information into noise-like information which brings attention to the hackers, thus the possibility of leakage of the information is significantly increased. To overcome this problem, a novel IWT-based embedding technique has been introduced to provide visual security to the information and reversibility of IWT- transformation provides the exact recovery of the cover image and secret information.

The rest of the paper is organized as following: Section 3 discusses the related theory, the proposed algorithm is given in Section 4, simulated results are shown in Section 5, finally conclusion are drawn in Section 6.

3. Preliminary

3.1. Compressive sensing (CS)

CS is a new sampling and reconstruction algorithm introduced by Donoho [6]. CS says that if the signal is sparse and compressible it is possible the signal can be reconstructed at lesser than the Nyquist sampling rate [27]. Sparsity defines that the signal has less number of non-zero values, and these non-zero values contain the primary information of the signal. Compressible means, the transformed values of the signal follow the power law decay. CS sampling and reconstruction depend on the MM and it converts the signal as noise-like structure. MM is shared between the sender and receiver as a key.

A signal S is sparse or compressible if it is transformed through an orthogonal matrix since the orthogonal matrix makes it a reversible process and the transformed information follows the power law decay (such as DWT, DCT, etc.). A sparse signal x is represented through $K-nonzero$ values and represented as:

$$s(N) = \sum_{i=1}^{N} \psi_i x_i \tag{1}$$

where ψ is a sparse basis and x is a sparse representation of x.

The compressed measured values of a sparse or compressible signal $s \epsilon R^N$ is defined as:

$$y = \phi s = \phi\psi x = Ax \tag{2}$$

where ϕ is a MM of size $M \times N$, A is a sensing matrix and $y\ \epsilon\ R^M$ is the measured values where $M \ll N$. To achieve the perfect recovery of the signal, MM should follow restricted isometric property (RIP) which selects those matrix which are nearly orthogonal, is described as follow:

$$(1-\delta)\|x\|_2 \leq \|Ax\|_2 \leq (1+\delta)\|x\|_2 \tag{3}$$

RIP is NP-hard problem therefore another property called mutual coherence is used to select the nearly orthogonal matrix. MM should be incoherent to the sparsify basis and it is defined as:

$$\mu(A) = \max_{i\neq j, 1<i,j<n} \left| \frac{\langle A_i A_j \rangle}{\|A_i\|_2 \|A_j\|_2} \right| \tag{4}$$

where μ is the mutual coherence. When 1D-CS is applied to a 2D image, first the image is converted to a vector, and then further compression is achieved through compressive sensing. In the 1D-CS [28], high dimensionality and the computational limit problem arises. To address this problem, the 2D-CS model is used, which is applied directly to the 2D image and is defined as:

$$Y = \phi_1 x \phi_2^T \tag{5}$$

where ϕ_1, ϕ_2 are two different MM of size $M \times N$ and Y is the measured values. 2D-CS gives high compression ratio since it reduces the dimensional information from both direction with out changing geometrical structure of the original image. For the recovery of the signal many image reconstruction algorithms exist for example matching pursuit (MP), orthogonal matching pursuit (OMP) etc. In the proposed algorithm smoothed-l_0 (Sl_0) reconstruction algorithm is employed to recover the signal.

4. Proposed algorithm

The proposed image compression and encryption algorithm is divided into two parts: (1) The image is compressed and encrypted through 2D-CS. (2) Visual security is provided to the compressed and encrypted information. In the presented paper, the test image size is $N \times N$, after compression and encryption the image size is $M \times M$ ($M \ll N$). The detail steps are discussed below:

4.1. Initial values of the chaotic map

The initial values of the chaotic maps are dependent on the plain image which will maintain the dependency between the plain image and the encryption algorithm. There exist different initial values for the distinct plain images. In the presented paper, SHA-256 hash function is utilized to generate the seed value of the chaotic maps. The process of the seed values generation is discussed below:

First, SHA-256 hash function is employed to the plain image and get 256 bit long hash value that is separated into the $8-bit$ groups to obtain the 32 decimal numbers such as $k_1, k_2, \ldots, k_{32}$. The obtained values have been used to generate the seed values of the chaotic map as discussed below:

$$\begin{aligned} x_0 &= \frac{t_1}{256} \times (k_1 \oplus k_6 \oplus k_{11} \oplus k_{16} \oplus k_{21} \oplus k_{26} \oplus k_{31}) \\ y_0 &= \frac{t_2}{256} \times (k_2 \oplus k_7 \oplus k_{12} \oplus k_{17} \oplus k_{22} \oplus k_{27}) \oplus k_{32} \\ r_0 &= \frac{t_3}{256} \times (k_3 \oplus k_8 \oplus k_{13} \oplus k_{18} \oplus k_{23} \oplus k_{28}) \\ sq1_0 &= \frac{t_4}{256} \times (k_4 \oplus k_9 \oplus k_{14} \oplus k_{19} \oplus k_{24} \oplus k_{29}) \\ sq2_0 &= \frac{t_5}{256} \times (k_5 \oplus k_{10} \oplus k_{15} \oplus k_{20} \oplus k_{25} \oplus k_{30}) \end{aligned} \tag{6}$$

where $(t_1, t_2, t_3, t_4, t_5)\ \epsilon\ (0, 1)$ are the keys, $x \oplus y$ is represented as XOR operation. x_0, y_0 are used as a seed values of the 2D-SLIM map. r_0 is used as a seed value of logistic map [29] and $sq1_0$, $sq2_0$ are used as a seed values of the tent-sine map [30].

4.2. Measurement matrix generation

In the proposed algorithm, 2D-SLIM map is used to obtain the random values and these values are utilized to generate the MM. The procedure of the MM generation is discussed below:

Step 1: The initial values x_0, y_0 are used as the seed values of the 2D-SLIM map to iterate it $T + m \times n \times d$ $(T = 1000)$ times where d is the displacement value and $m = CR \times n$ $(CR = compression\ ratio)$ and n is the block size. And the initial T values are discarded to avoid the adverse effect then two sequences of size $1 \times mdn$ are obtained such as $(x_1, x_2, \ldots, x_{m \times d \times n})$ and $(y_1, y_2, \ldots, y_{m \times d \times n})$.

Step 2: The random sequences x_i and y_i are further processed as follows:

$$\begin{aligned} X_i &= 1 - 2 \times x_(i \times d) \\ Y_i &= 1 - 2 \times y_(i \times d) \end{aligned} \tag{7}$$

Step 3: The obtained sequences X_i and Y_i are used to construct the MM as follows:

$$\phi_1 = \sqrt{\frac{2}{m}} \begin{bmatrix} X_1 & X_{m+1} & \cdots & X_{mn-m+1} \\ X_2 & X_{m+2} & \cdots & X_{mn-m+2} \\ \vdots & \vdots & \ddots & \vdots \\ X_m & X_{2m} & \cdots & X_{mn} \end{bmatrix} \tag{8}$$

$$\phi_2 = \sqrt{\frac{2}{m}} \begin{bmatrix} Y_1 & Y_{m+1} & \cdots & Y_{mn-m+1} \\ Y_2 & Y_{m+2} & \cdots & Y_{mn-m+2} \\ \vdots & \vdots & \ddots & \vdots \\ Y_m & Y_{2m} & \cdots & Y_{mn} \end{bmatrix} \tag{9}$$

where $\sqrt{\frac{2}{m}}$ is used for normalization.

4.2.1. Proposed optimization algorithm

The problem of sampling and reconstruction with fewer samples is solved through CS by estimating a proper MM. The objective of optimization is to reduce the mutual coherence between the MM and sparsify basis which will increase the reconstruction performance of the algorithm. To achieve this objective, an optimization algorithm has been proposed that minimizes the mutual coherence between MM and any sparsifying basis. The procedure of the optimization is discussed below:

Step 1: At first, the initial W columns of the MM is multiplied by the weighting factor t and obtain weighted MM $\phi_i \quad i = 1, 2$.

Step 2: Singular value decomposition (SVD) [31] is applied on the weighted MM to obtain the eigen values of the MM.

$$[U, S, V] = svd(\phi_i); i = 1, 2 \tag{10}$$

where U and V are the orthogonal matrix and S keeps all the eigen values of the MM such as $\delta_1 < \delta_2 < \cdots < \delta_n$.

Step 3: All the diagonal values of the matrix S are replaced by 1 such as $\delta_1 = \delta_2 = \cdots = \delta_N = 1$ and get an updated matrix S'.

Step 4: The orthogonal matrix U, V and updated matrix S' is multiplied to obtain the optimized MM ϕ_1, ϕ_2.

$$\phi_i = U \times S' \times V^T; i = 1, 2 \tag{11}$$

Table 2 depicts the result before optimization and after optimization in term of mutual coherence. From Table 2 it is clear that after optimization mutual coherence is very low which is a necessary condition for MM for better reconstruction. The results exhibit that the mutual coherence is minimum at the highest sampling ratio.

Table 2
Mutual coherence.

Compression ratio (CR)	Before optimization	After optimization
0.5	0.0916	$3.2613 \times e^{-16}$
0.6	0.0607	$2.7756 \times e^{-16}$
0.7	0.0510	$1.9429 \times e^{-16}$
0.8	0.0397	$1.3878 \times e^{-16}$
0.9	0.0195	$1.3480 \times e^{-16}$
1	0.0149	$1.1511 \times e^{-16}$

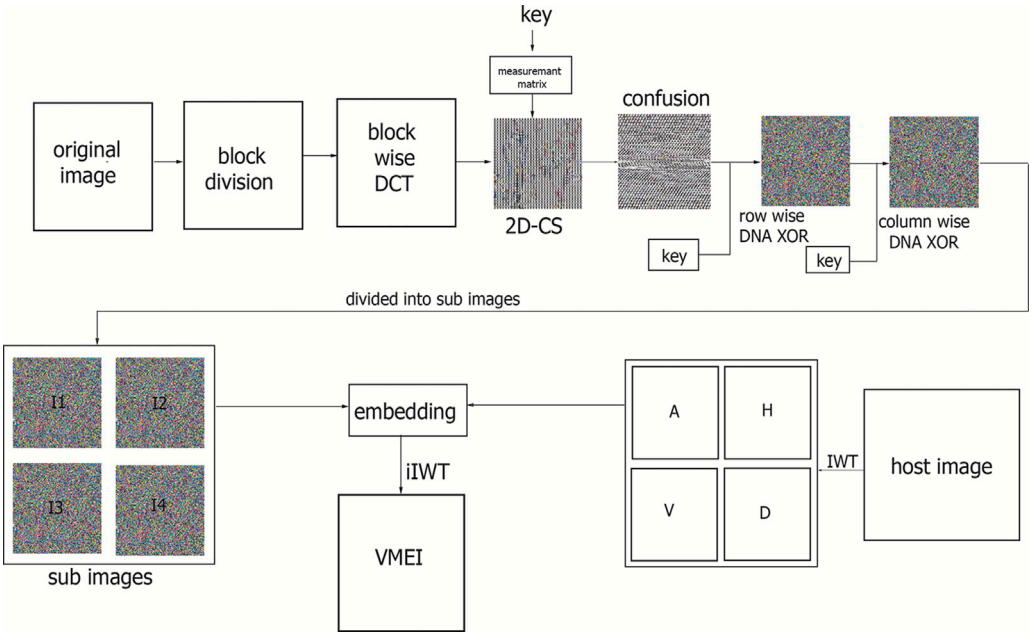

Fig. 3. Proposed algorithm.

4.3. Compression–encryption process

The flowchart of the introduced technique is illustrated in Fig. 3. As shown in Fig. 3 the introduced algorithm incorporates three steps: compression, encryption, and visual security. In the compression phase, the plain color image is split into the R, G, and B planes and sparsified through a DCT basis, followed by sampling through CS. In the encryption phase DNA encoding-decoding and XOR operation is employed to encrypt the sampled values. Finally, IWT based embedding technique is used to provide visual security.

4.3.1. Compression

In the presented paper, CS is employed to obtain the less samples. The detailed steps are as follows:
Step 1: At first, the color image I of size $N \times N$ is splitted into the three color planes R, G and B.
Step 2: Each plane is sub-divided into the non-overlapping sub-blocks and the size of each block is 8×8.
Step 3: DCT is applied on each sub-block of the image which sparsifies the information.
Step 4: MM ϕ_1 and ϕ_2 is generated as discussed in Section 4.2.
Step 5: Each block of the planes is sampled through 2D-CS as discussed in Section 3.1.
Step 6: The sampled values are normalized in the range [0–255] as follows:

$$C(i,j) = round\left(\frac{255 \times (S(i,j) - S_{min})}{S_{max} - S_{min}}\right) \tag{12}$$

where S_{max} and S_{min} are the maximum and minimum values of each block.
Finally, compressed samples of size $M \times M$ are obtained by combining all the blocks.

4.3.2. Confusion–diffusion

Confusion is created through zig-zag scrambling and diffusion is applied through DNA [32] on the compressed samples as discussed below:

Step 1: The initial value r_0 is used as the seed value to iterate the logistic map $M \times M$ times, where M is the size of the compressed image.
Step 2: The generated random sequence is normalized in the range $[1-8]$ as follows:

$$r_i = mod(floor(r_i \times 10^8), 8) + 1 \tag{13}$$

Step 3: Compressed samples are converted to the DNA sequences as discussed in [3], and sequence r is used to select the DNA rule out of eight rules.
Step 4: The initial values $sq1_0$ and $sq2_0$ are used as a seed value to iterate the tent-sine map $1 \times M$ times and obtained the sequences $SQ1$ and $SQ2$, where M is the size of the compressed image.
Step 5: Sequences $SQ1$ and $SQ2$ are normalized in the range [0–255] as follows:

$$SQ(i) = mod(floor(SQ(i) \times 10^8), 256); i = 1, 2 \tag{14}$$

Step 6: Sequences $SQ1$ and $SQ2$ are converted to the DNA sequence, where r (discussed in Step 2) is used to select the DNA rule.
Step 7: DNA based encryption process is done in two steps: (i) Row wise DNA XOR (ii) Column wise DNA XOR
(i) $SQ1$ is used as a key to diffuse the first row of the signal and after diffusion first row is used as key for the 2nd row and so on.
(ii) $SQ2$ is used as a key to diffuse the first column of the signal and after diffusion first column is used as key for the 2nd column and so on.

The detailed steps are discussed in Algorithms 1 and 2 respectively.

Algorithm 1: ROW wise DNA XOR

```
procedure ROW (Im, sq1)
Input: Image Im of size (m,n), chaotic sequence sq1
output: ImR of size (m,n)
key = sq1
for i = 1:m
   R1 = Im(i,:)
   R2 = bitxor(R1, key)
   key = R2
  ImR(i,:) = R2
end
```

Algorithm 2: COLUMN wise DNA XOR

```
procedure COLUMN (ImR, sq2)
Input: Image ImR of size (m,n), chaotic sequence sq2
output: ImC of size (m,n)
key = sq2
for i = 1:n
   R1 = ImR(:,i)
   R2 = bitxor(R1, key)
   key = R2
  ImC(i,:) = R2
end
```

Finally, the encrypted image is obtained.

4.4. Visual security

Integer wavelet transform (IWT) is used to provide the visual security to the algorithm and detail steps are discussed below:
Step 1: At first, the host image of size $N \times N$ is transformed through IWT which decomposes the image into four parts such as LL, LH, HL, HH.
Step 2: Secret image is divide into four part as discussed in algorithm 3.
Step 3: The obtained four parts has been embedded in the LL, LH, HL, HH part of the carrier image by using the following equation:

$$LL(i,j) = LL(i,j) + 0.1 \times A(i,j)$$
$$LH(i,j) = LH(i,j) + 0.1 \times B(i,j)$$
$$HL(i,j) = HL(i,j) + 0.1 \times C(i,j)$$
$$HH(i,j) = HH(i,j) + 0.1 \times D(i,j)$$

Step 4: At last, Inverse IWT is applied to recombine the LL, LH, HL, HH part of the image and got a visually meaningful encrypted image (VMEI).

Algorithm 3: Secret image partition

```
procedure Divide_secret_image (Im)
Input: Image Im of size (m,n)
output: four parts of the image A, B, C, D of size (m,n)
bini,j = dec2bin(Im,8); where i = 1, 2,...,m ; j = 1, 2,...,n
for i = 1:m
  for j = 1 : n
    H = bini,j
    B1 = H(1); B2 = H(2); B3 = H(3);...; B8 = H(8)
    A = bin2dec([B1 B2]);
    B = bin2dec([B3 B4]);
    C = bin2dec([B5 B6]);
    D = bin2dec([B7 B8]);
  end
end
```

Step 5: All the necessary information which are required to recover the secret information for example $SHA-256$ hash values can be embedded in the VMEI through any of the existing reversible data hiding technique such as [33].

5. Experimental analysis

The performance of proposed work is analyzed in this section on various test images of different dimensions such as 256×256 and 512×512, different dimension images are chosen because detail per unit area varies in images with size. In first column of Fig. 4, first three images are of size 512×512 while the last two are of size 256×256. The results are simulated on MATLAB R2018 in the PC with 1.70 GHz CPU and 8 GB RAM with operating system windows 10. The parameter of the chaotic map are: controlling parameter of tent-sine map $\mu = 3.999$, controlling parameter of logistic map $\mu = 4$, and controlling parameters of the 2D-SLIM map a, b are 0.1, 2π respectively, these values are chosen randomly. The simultaneous compression–encryption performance of the various test images before visual security at $CR = 0.25$ are shown in Fig. 4. For an instance, when Lena image of size 512×512 (shown in Fig. 4(a)) is compressed and encrypted through proposed algorithm, the encrypted Lena is shown in Fig. 4(b) which is of size 256×256. It is clear from Fig. 4(a) and (b) that after simultaneous compression–encryption the resultant information is one-fourth of the original information which saves the storage space and transmission time. The third column of Fig. 4 shows the reconstructed images obtained from the one fourth information (shown in Fig. 4(b)). The proposed algorithm uses SL_0 as reconstruction algorithm. It can be clearly observed from first and third column of Fig. 4 that the reconstructed image is visually same as the original and shows that the proposed algorithm has good reconstruction ability. Further, it can be seen in Fig. 4(b) that the compressed–encrypted information is visually noise-like information which may bring the attention to the eavesdroppers as some secret information is transmitting through the network. To address this problem, visual security came into consideration. The results obtained from visual security are shown in Fig. 5. The first column of Fig. 5 depicts the secret information which has to be embedded in the host image and second column shows the host image. The visually secure image is shown in the third column of Fig. 5, it can be observed from the third column of Fig. 5 that the no one can even guess the glimpse of secret image in the VMEI which makes it visually secure against any kind of attack. This is possible due to the proposed block based 2D-CS crypto-system.

5.1. Peak signal noise ratio (PSNR)

PSNR is a mathematical metric used to calculate the quality of the reconstructed image. It is calculated between the reconstructed image and corresponding original image using the equation given below:

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (I(i,j) - I'(i,j))^2$$

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{255 \times 255}{\mathrm{MSE}}\right) \tag{15}$$

where I and I' represent the original and reconstructed signal respectively. The larger the value, the lesser the distortion. It was mentioned in the literature that if the value is greater than 30 dB then no one can perceive any significant difference between the original and reconstructed image [34]. At first, the PSNR values between original and CS reconstructed image is computed at different CR like 0.25, 0.50 and 1 and listed in Table 3. As the PSNR value of the CS reconstructed image is greater than 30 dB in all the cases at CR 0.25, 0.50 and 1, hence the proposed CS based reconstruction algorithm works well on few samples. It can be observed from Table 3 that recovery capability of the proposed algorithm is good enough as the PSNR value increases significantly when CR increases.

Further, to evaluate the visual security of the proposed work, the PSNR between the host and VMEI is calculated and shown in Table 9. It can be clearly seen from Table 9 that the PSNR values of the proposed scheme is more than 55 dB in most of the cases hence no one can even guess the presence of secret image in the VMEI. Hence the proposed work is visually secure over the public networks.

Fig. 4. Compression Performance (a), (d), (g), (j), (m) original image (b), (e), (h), (k), (n) compressed–encrypted information of respective images (c), (f), (i), (l), (o) reconstructed image.

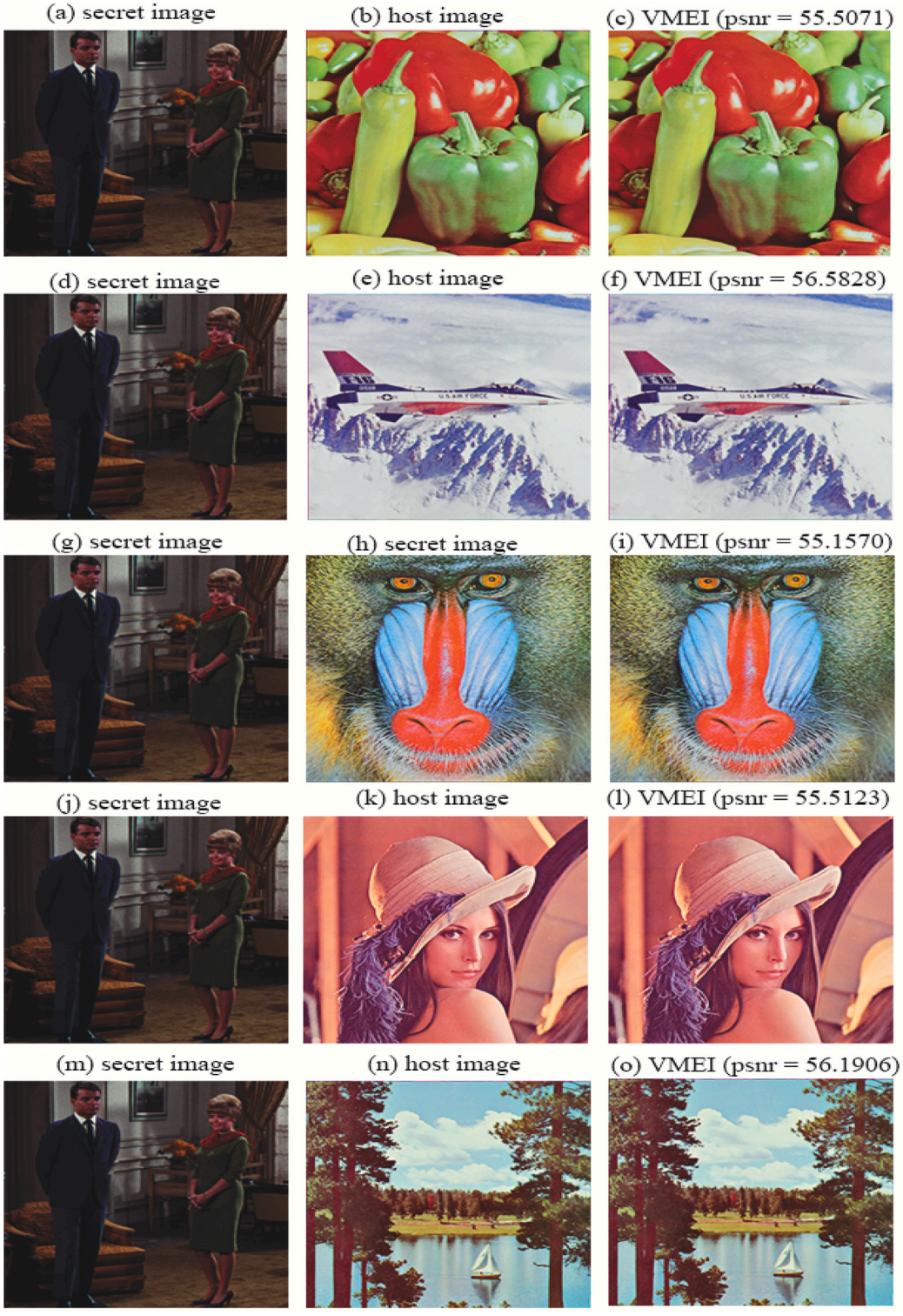

Fig. 5. Visual security Performance (a), (d), (g), (j), (m), secret image (b), (e), (h), (k), (n) host image (c), (f), (i), (l), (o) VMEI.

Table 3
PSNR value of various test images.

Image	CR		
	0.25	0.5	1
Lena	36.2548	39.2123	48.5474
Baboon	31.2934	39.4007	49.5619
Plane	31.4037	37.8536	46.8698
Pepper	32.3283	39.1888	54.2696
Girl	33.8628	38.9335	48.1706
Couple	36.3411	41.9959	50.2688
Sailboat	31.5555	37.8770	49.6343

Table 4
SSIM of the proposed algorithm.

Image	Reconstructed image at $CR = 0.25$	Carrier image after embedding
Lena	0.9842	0.9999
Baboon	0.8539	0.9998
Plane	0.8847	0.9985
Pepper	0.9860	0.9999
Girl	0.9800	0.9999
Couple	0.8902	0.9969
Sailboat	0.8847	0.9985

5.2. Structural similarity index metric (SSIM)

Several measures are available to examine the quality of the reconstructed images such as: PSNR and MSE. Wang et al. [35] has introduced another method called SSIM to evaluate the structural similarity between the original and reconstructed images. Its value lies between −1 and 1. If the SSIM value is 1, it means the reconstructed images are identical to the original. SSIM of two images can be calculated as follows:

$$\mathrm{SSIM} = \frac{(2\mu_I\mu_{I'} + C_1)(2\sigma_{II'} + C_2)}{(\mu_I^2 + \mu_{I'}^2 + C_1)(\sigma_I^2 + \sigma_{I'}^2 + C_2)} \tag{16}$$

where, μ_I and $\mu_{I'}$ are the averages corresponding to images I and I' respectively. σ_I^2 and $\sigma_{I'}^2$ represent the variances of images I and I' respectively. $\sigma_{II'}$ is the covariance between I and I' images, C_1 and C_2 are the predefined constants. At first, the SSIM between the original and reconstructed image at CR 0.25 is computed and shown in the second column of Table 4. It can be noted down that the proposed CS based reconstruction algorithm is capable of giving very good SSIM at CR 0.25, hence it is obvious if CR value is increased from 0.25 to more then the SSIM will approach to 1, showing more similarity. Next, the SSIM value between host and VMEI is calculated and shown in the third column of Table 4 and results are found promising as the SSIM value is very close to 1. For an instance, it can be observed from second column of Table 4 that the SSIM value for Lena image is "0.9842" at $CR = 0.25$ which shows that the reconstructed image is almost similar to the original image. The third column of Table 4 shows the result for SSIM value between the carrier image and the visually secure Lena image is 0.9999 which is almost equal to 1. Hence the host image is structurally identical to the original image.

5.3. Key space analysis

Key space analysis is a way to check the capability of proposed work against the brute-force attacks. Longer the key space better the capability against the brute-force attacks. In [36], Alvarez et al. have stated that if the key space of an algorithm is greater than 2^{100} then the algorithm can resist bruit-force attacks. For any algorithm, key space depends upon the number of keys used to develop an algorithm. In the proposed algorithm SHA-256 hash values of the plain image is used as a key and some other keys x_0, y_0, r_0, $sq1_0$, $sq2_0$, S_{max}, S_{min} and initial value of the zig-zag scrambling. We have considered the precision of these keys as 10^{-14} except SHA-256 hash value, therefore the total key space of the introduced algorithm is $(10^{14})^7 = 10^{98} > 2^{300}$ plus $256 - bit$ hash value. Therefore, the overall key space of the proposed algorithm is 2^{556} which is large enough to resist any brute-force attack.

5.4. Histogram analysis

Histogram of an image depicts the intensity distribution of the pixel values. An encryption scheme is designed in such a way that it modifies the histogram of the image. The histogram of an encrypted image should be as uniform as possible. Fig. 6 shows the result of the histogram before the visual protection. As we can see, the histogram of the encrypted images follows a uniform distribution which is different from the histogram of the original images. The uniform distribution hides the statistical information of the image appropriately. Figs. 6(b) and (e) show the result of the intensity distribution of the plain image and the difference between them is observable whereas the histograms of the encrypted images shown in Figs. 6(c) and (f) is uniformly distributed

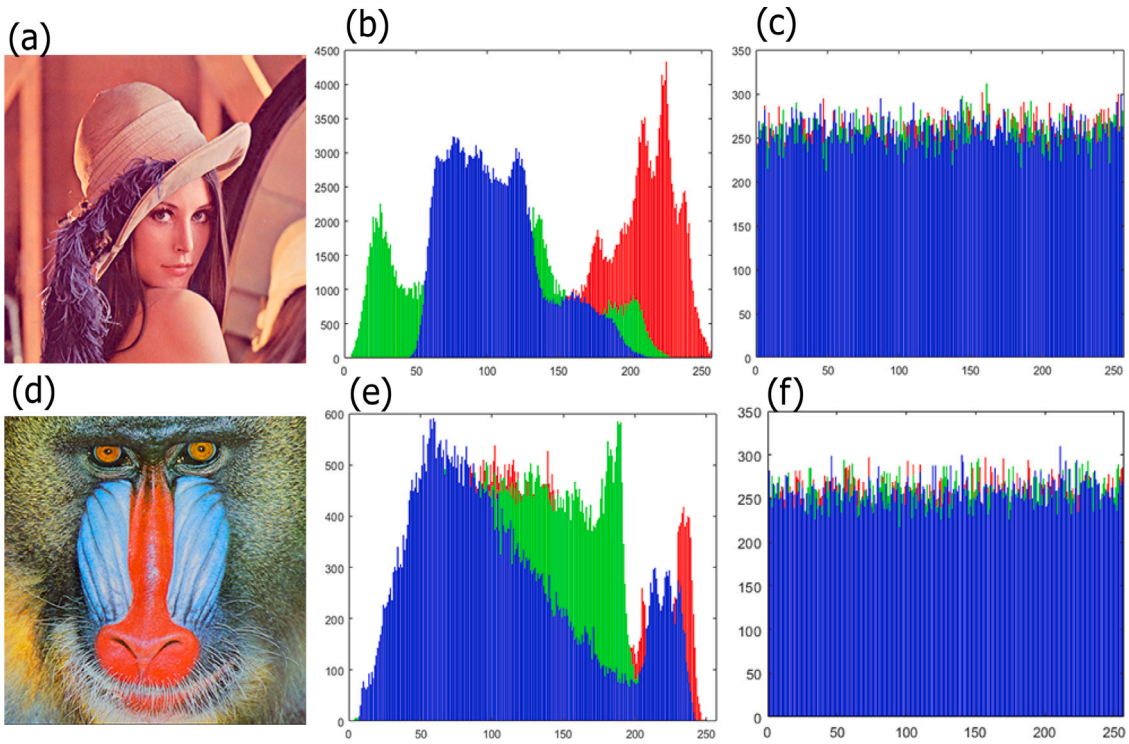

Fig. 6. (a) Lena image (b) histogram of original image (c) histogram of encrypted image (d) Baboon image (e) histogram of original image (f) histogram of encrypted image.

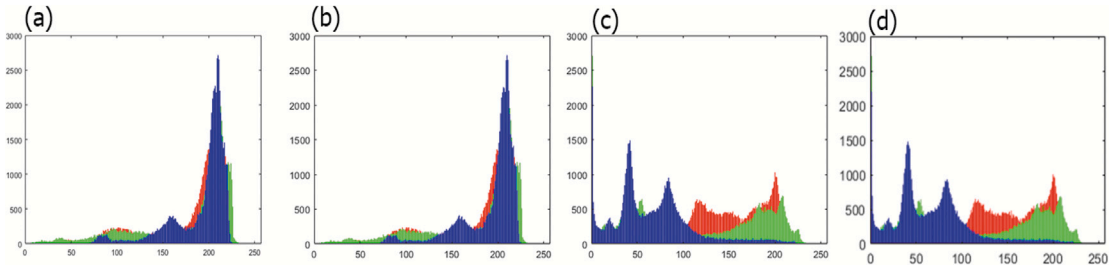

Fig. 7. Histogram (a) airplane image before keeping secret data (b) airplane image after keeping secret data (d) pepper image before keeping secret data (e) pepper image after keeping secret data.

and shows no correlation from the original image. so it is not possible for attackers to identify the original information from the histogram. The above analysis proves that the proposed encryption algorithm is secure against statistical attacks.

Further, in the proposed algorithm, visual protection is implemented to convert noise-like information into a visually meaningful image. With the reference to Fig. 5, the histogram of Fig. 5(b), (c), (e) and (f) is shown in Fig. 7(a), (b), (c) and (d) respectively. The statistical distribution of the two host images before embedding is shown in the 7(a), (c) and 7(b), (d) depicts the statistical distribution of the corresponding image after embedding. It can seen that the histogram 7(a) and (b) i.e. before and after embedding are almost same. Therefore, it is hard to identify the embedded secret information from the histogram.

5.5. Correlation coefficient (CC) analysis

The neighboring pixel values of an image use to be highly correlated, and a good image encryption algorithm should be able to break the relation between neighboring pixels. CC is a metric to measure the correlation of a series of the pixel values, and is calculated as follows:

$$R_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{17}$$

Table 5
Cross Correlation of the proposed algorithm.

Image	Plane	Horizontal	Vertical	Diagonal
Lena encrypted	R	0.0032	0.0170	−0.0063
	G	0.0121	−0.0132	0.0151
	B	0.0200	−0.0055	−0.0010
Lena original	R	0.9562	0.9779	0.9381
	G	0.9442	0.9704	0.9150
	B	0.9211	0.9416	0.8971
Baboon encrypted	R	0.0068	−0.0027	0.0015
	G	0.0089	0.0052	−0.0036
	B	0.0117	0.0021	0.0009
Baboon original	R	0.9428	0.9171	0.9008
	G	0.8718	0.8519	0.8086
	B	0.9135	0.9143	0.8718

Table 6
Information entropy of the plain image and encrypted image.

Image	Plain image	Encrypted image	VMEI
Lena	7.7502	7.9990	7.7347
Baboon	7.7624	7.9991	7.6796
Plane	6.6639	7.9991	6.6819
Pepper	7.6698	7.9990	7.7042
Girl	6.4165	7.9991	6.5262
Couple	6.2945	7.9967	6.4060
Sailboat	7.7622	7.9989	7.7406

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \qquad E(x) = \frac{1}{N}\sum_{i}^{N} x_i$$
$$D(x) = \frac{1}{N}\sum_{i}^{N}(x_i - E(x))^2$$

R_{xy} is the CC of an image, N is the total number of pixels. For illustration purpose, 5000 neighboring pixels are selected from the horizontal, vertical and diagonal direction and CC is calculated. Table 5 shows CC among the adjacent pixels in each direction for plain and encrypted image. Apparently Fig. 8 shows the distribution of the pixel values of each plane of the lena image and encrypted lena image in horizontal, vertical and diagonal direction. Fig. 8(a)–(i) depicts that the pixel values of the input image is highly correlated in horizontal, vertical and diagonal direction, whereas, Fig. 8(j)–(r) shows that the pixel values of the corresponding encrypted image are not correlated. Table 5 illustrated that the CC value of the encrypted image is near to 0 that shows the correlation between the adjacent pixel is minimized and the CC values of the original image is near to 1 that means the adjacent pixels are highly correlated.

5.6. Information entropy (IE)

IE is a measure of randomness in an image, and it is calculated from the following formula:

$$H(m) = -\sum_{i=1}^{N} p(m_i)\log p(m_i) \tag{18}$$

where $p(m_i)$ is the probability of occurrence of the pixel value. If a 256 gray scale image is highly random then IE is 8. Table 6 shows the IE result for the plain image, encrypted image, and VMEI. IE values of the plain image and VMEI are significantly different from the ideal value whereas for encrypted the values are near to 8, which indicates the introduced algorithm makes the information highly random. For example, IE value of the Lena encrypted image is 7.9990 which is near to 8 that shows the encrypted image is safe and reliable against statistical attacks. IE values of the original Lena image and VMEI are 7.7502 and 7.7347 which shows that after embedding the lena image is same as the original image.

5.7. Noise attack analysis

Visually secure information is transmitted through the public network, as the public network is not safe for transmission so the information is contaminated through the different noise such as salt–pepper noise (SPN), which degrade the reconstruction quality. This section is all about the ability of the proposed algorithm against noise attacks. Fig. 9 shows the results for the VMEI that are corrupted through the SPN at different intensities. In the simulation 0.1%, 0.01% density noise has been added to the cipher image.

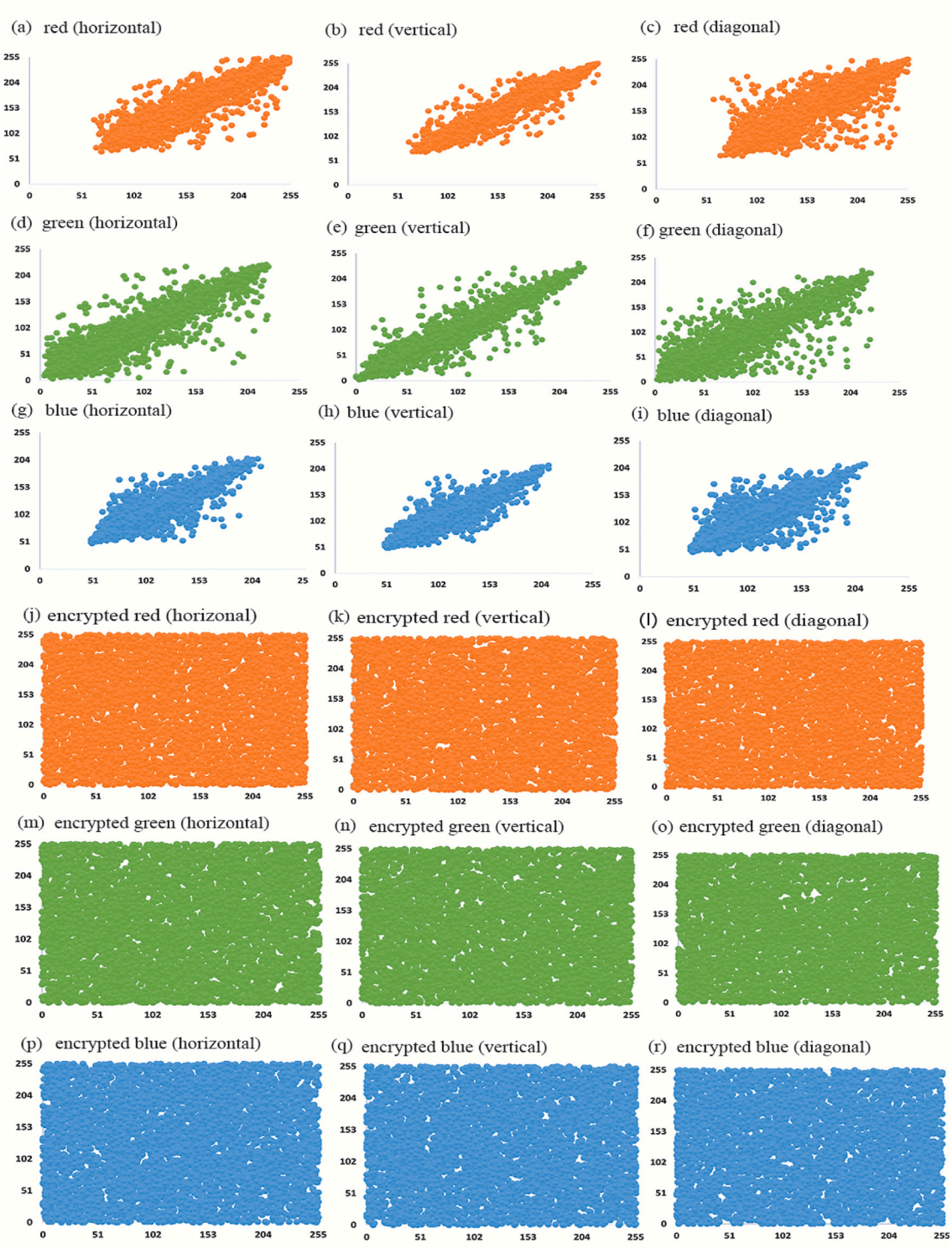

Fig. 8. Distribution of pixel values.

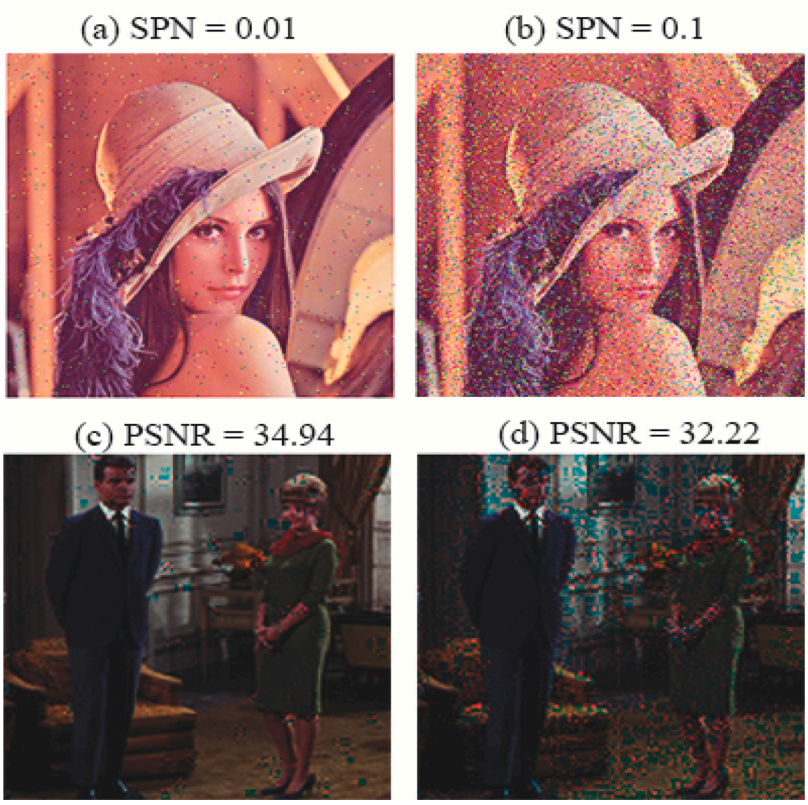

Fig. 9. Noise attack.

Table 7
PSNR value of reconstructed image after noise attack.

Intensity of noise	Before attack	After attack
SPN 0.01	36.3411	34.9466
SPN 0.1	36.3411	32.2186

In Fig. 9, first row shows the results for the noisy protected image, and the second row shows the results for the recovered secret image.

As we can see that the retrieved information is thoroughly recognizable, which proves the feasibility of the algorithm against noise attacks. To quantify feasibility, the PSNR value of the reconstructed images have been calculated and depicted the result in Table 7. It can be seen that with increasing density of the noise, the PSNR values of the reconstructed image have been degraded but still, the information is recognizable which demonstrates the robustness of the proposed algorithm against noise attacks.

5.8. Cropping attack

When the information is shared through the public network, may be the information is lost due to hackers' attacks or network faults which will affect the reconstruction quality of the image. This section covers the consequences of different data loss sizes at different places and shows the result in Fig. 10. The decrypted images have almost the same visual appearance even when the data from the visual cipher image is lost as shown in Fig. 10. As depicted in Fig. 10(a), (c), (e) and (g), (i), (k), the 32×32 and 64×64 square-shaped data from various locations is lost, even though, the secret image is completely extracted and reconstructed, and is perceptually same as the original as shown in Fig. 10(b), (d), (f), (h), (j), (l). Table 8 shows the result for the PSNR value before and after the cropping attack to quantify the feasibility of the proposed algorithm against cropping attack. From Table 8 we can understand that the PSNR values before and after cropping attack are not much different, therefore the proposed algorithm resists the cropping attack.

5.9. Comparison with the existing algorithm

The superiority of the proposed algorithm is quantified by comparing the proposed work with some existing algorithms [23–25] by using mathematical metric such as PSNR as shown in the Table 9. From Table 9 it is clear that the calculated PSNR values for

Fig. 10. Cropping attack.

Table 8
PSNR value of reconstructed image after cropping attack.

Size of cropping attack	Color plane	Before attack	After attack
32 × 32 left-corner	R	36.4177	35.7194
	G	37.0548	36.2203
	B	36.4889	35.9108
32 × 32 middle	R	36.4177	36.0346
	G	37.0548	36.5234
	B	36.4889	36.2726
32 × 32 right-corner	R	36.4177	35.8388
	G	37.0548	36.3412
	B	36.4889	36.1408
64 × 64 left-corner	R	36.4177	34.8594
	G	37.0548	35.4547
	B	36.4889	35.3839
64 × 64 middle	R	36.4177	35.0746
	G	37.0548	35.6125
	B	36.4889	35.4313
64 × 64 right-corner	R	36.4177	34.9468
	G	37.0548	35.4431
	B	36.4889	35.3066

Table 9
PSNR value of the proposed scheme and some existing techniques.

Image	CR	[23]	[24]	[25]	Proposed
Lena	0.25	28.82	33.96	34.71	**36.2548**
	0.50	32.63	35.5389	37.60	**39.2123**
	0.80	35.86	39.9687	40.66	**43.5801**
Baboon	0.25	26.74	28.26	29.75	**31.2934**
	0.50	28.44	30.12	30.65	**39.4007**
	0.80	29.57	31.57	32.82	**49.5619**
Pepper	0.25	28.54	29.97	31.25	**32.3283**
	0.50	30.15	31.27	33.87	**39.1888**
	0.80	34.47	35.78	38.24	**54.2696**

Lena's image at different CR are higher than the existing techniques. For an instance, PSNR values of the reconstructed Lena image at CR 0.25 using the scheme [23–25] are "28.82", "33.96", "34.71" respectively. However, the PSNR value for Lena image through proposed scheme is "35.2548" which is larger than the existing algorithms. CS is a sampling and reconstruction algorithm so PSNR is an important metric to identify the superiority of the algorithm. An effective VMEI algorithm requires high similarity between the host image and visually secure cipher image. Table 10 shows the result for visual security, PSNR value between the host image and VMEI is calculated and compared with existing schemes [23–25]. From Table 10 we can understand that the PSNR value for lena

Table 10
PSNR value between the carrier image and VMEI.

Image	Lena	Baboon	Plane	Pepper	Girl	Couple	Sailboat
Proposed scheme	**55.5123**	**55.1570**	**56.5828**	**55.5071**	**57.3175**	**56.0598**	**56.1906**
Existing scheme [23]	36.58	35.48	37.25	36.84	36.64	35.47	34.87
Existing scheme [24]	38.59	36.74	39.56	37.92	38.59	36.54	35.26
Existing scheme [25]	36.78	34.82	38.13	36.21	37.25	35.56	33.35

Table 11
Key space analysis of the proposed scheme and some existing techniques.

Algorithm	[2]	[24]	[25]	Proposed
Key space	2^{207}	2^{215}	2^{294}	2^{556}

Table 12
Time analysis of the proposed and existing algorithms.

Algorithm	Encryption		Decryption	
[24]	compression	2.56 s	reconstruction	6.26 s
	confusion–diffusion	3.59 s	inverse confusion–diffusion	3.36 s
	embedding	0.56 s	extraction	0.59 s
[25]	compression	0.59 s	reconstruction	4.56 s
	confusion	0.12 s	inverse confusion	0.08 s
	embedding	0.17 s	extraction	0.2 s
Proposed	compression	**0.35 s**	reconstruction	**2.26 s**
	confusion–diffusion	3.46 s	inverse confusion–diffusion	3.28 s
	embedding	**0.12 s**	extraction	**0.10 s**

image after embedding in [23–25] is 35.15, 38.59, 36.78 whereas from proposed algorithm the PSNR value is 55.5123 which is larger than the existing schemes [23–25], so we can understand that the proposed embedding algorithm does not affect the carrier image much, the carrier image after embedding appears the same as the carrier image before embedding.

The key space of the proposed scheme is also calculated and compared with the existing works [2,24,25] and depicted in the Table 11. The work reported in [2] is an encryption algorithm that is based on chaos without using CS hence it is considered a secure algorithm but not efficient as it takes more storage and transmission cost. However, the work reported in [24,25] is using the concept of CS along with stream cipher to make it secure while saving transmission time and storage cost. The proposed block 2D-CS based scheme is compared with [2,24,25] in term of key space and results are summarized in Table 11. It can be observed from Table 11 that the key space of the existing schemes [2,24,25], is 2^{207}, 2^{215}, 2^{294} respectively, whereas the key space of the proposed scheme is 2^{556} that is large enough from the existing schemes, hence the proposed algorithm is more efficient and secure against brute-force in comparison to the existing schemes.

The performance analysis of proposed work for computational cost is also evaluated by calculating the time required for execution of the code in seconds. In the proposed algorithm, encryption phase considered three steps: compression, confusion–diffusion, embedding, whereas decryption phase consists: extraction of the secret data, inverse confusion–diffusion, and then reconstruction of the original data through SL_0 reconstruction algorithm. The Time analysis of the proposed algorithm is tested and listed in Table 12. It can be observed from the Table 12 that due to the block-wise computation, compression and reconstruction phase takes less time in comparison to the existing algorithms [24,25]. DNA encoding-decoding used in the proposed work takes more time when compared to permutation which is used in [25] but permutation operation is a linear operation and it is less secure against attacks when compared to DNA. Hence, when confusion and diffusion both are used, then the proposed algorithm is taking less time compared to [25]. The proposed algorithm is also time efficient in compression and reconstruction when compared to the existing algorithms [24,25]. Further, the use of DNA along with block 2D-CS does not increases the overall computational cost of the proposed algorithm.

6. Conclusion

In the proposed algorithm, a color image encryption algorithm is introduced for visual security based on block 2D-CS. The employment of block-based 2D-CS reduces the computational complexity of the proposed algorithm. CS depends on measurement matrix hence the use of 2D-SLIM chaotic map provides better randomness and wider chaotic range in MM. Further, the mutual coherence between the sparsifying basis and MM is optimized using a novel approach that helps in better image reconstruction. CS has built-in ability to compress and encrypt the images simultaneously using optimized measurement matrix but cannot guarantee robustness against brute force attack therefore cyclic row-wise and column-wise DNA diffusion operations have been employed to secure the secret image. Furthermore, Visual security is applied to convert the secret information into the visually secure information. The adoption of embedding in the fractional part of the image has increased the embedding capacity significantly while ensuring the security of secret image. The experimental results have shown the superiority of proposed work over the existing works in many aspects.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

[1] L.H. Gong, H.X. Luo, R.Q. Wu, N.R. Zhou, New 4D chaotic system with hidden attractors and self-excited attractors and its application in image encryption based on RNG, Physica A 591 (2022) 126793.
[2] S. Yan, L. Li, B. Gu, Y. Cui, J. Wang, J. Song, Design of hyperchaotic system based on multi-scroll and its encryption algorithm in color image, Integration (2022).
[3] A. Vaish, S. Patel, Securing color images using DNA coding and cosine stockwell transformation in wavelet domain, Optik 266 (2022) 169606.
[4] C.F. Duan, J. Zhou, L.H. Gong, J.Y. Wu, N.R. Zhou, New color image encryption scheme based on multi-parameter fractional discrete Tchebyshev moments and nonlinear fractal permutation method, Opt. Lasers Eng. 150 (2022) 106881.
[5] M.B. Farah, R. Guesmi, A. Kachouri, M. Samet, A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation, Opt. Laser Technol. 121 (2020) 105777.
[6] D.L. Donoho, Compressed sensing, IEEE Trans. Inform. Theory 52 (4) (2006) 1289–1306.
[7] R. Huang, K. Sakurai, A robust and compression-combined digital image encryption method based on compressive sensing, in: 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, 2011, pp. 105–108.
[8] X. Chai, X. Zheng, Z. Gan, D. Han, Y. Chen, An image encryption algorithm based on chaotic system and compressive sensing, Signal Process. 148 (2018) 124–144.
[9] Y. Luo, J. Lin, J. Liu, D. Wei, L. Cao, R. Zhou, et al., A robust image encryption algorithm based on Chua's circuit and compressive sensing, Signal Process. 161 (2019) 227–247.
[10] N. Zhou, A. Zhang, F. Zheng, L. Gong, Novel image compression encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing, Opt. Laser Technol. 62 (2014) 152–160.
[11] N. Zhou, H. Li, D. Wang, S. Pan, Z. Zhou, Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform, Opt. Commun. 343 (2015) 10–21.
[12] N. Zhou, S. Pan, S. Cheng, Z. Zhou, Image compression encryption scheme based on hyper-chaotic system and 2D compressive sensing, Opt. Laser Technol. 82 (2016) 121–133.
[13] Q. Xu, K. Sun, C. Cao, C. Zhu, A fast image encryption algorithm based on compressive sensing and hyperchaotic map, Opt. Lasers Eng. 121 (2019) 203–214.
[14] L. Bao, Y. Zhou, Image encryption: Generating visually meaningful encrypted images, Inform. Sci. 324 (2015) 197–207.
[15] X. Chai, Z. Gan, Y. Chen, Y. Zhang, A visually secure image encryption scheme based on compressive sensing, Signal Process. 134 (2017) 35–51.
[16] G. Ye, C. Pan, Y. Dong, K. Jiao, X. Huang, A novel multi-image visually meaningful encryption algorithm based on compressive sensing and Schur decomposition, Trans. Emerg. Telecommun. Technol. 32 (2) (2021) e4071.
[17] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, K.W. Nixon, An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding, Opt. Lasers Eng. 124 (2020) 105837.
[18] L. Zhu, H. Song, X. Zhang, M. Yan, T. Zhang, X. Wang, J. Xu, A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding, Signal Process. 175 (2020) 107629.
[19] C. Pan, G. Ye, X. Huang, J. Zhou, Novel meaningful image encryption based on block compressive sensing, Secur. Commun. Netw. 2019 (2019).
[20] H. Wang, D. Xiao, M. Li, Y. Xiang, X. Li, A visually secure image encryption scheme based on parallel compressive sensing, Signal Process. 155 (2019) 218–232.
[21] D. Jiang, L. Liu, L. Zhu, X. Wang, X. Rong, H. Chai, Adaptive embedding: A novel meaningful image encryption scheme based on parallel compressive sensing and slant transform, Signal Process. 188 (2021) 108220.
[22] Z. Hua, K. Zhang, Y. Li, Y. Zhou, Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing, Signal Process. 183 (2021) 107998.
[23] D. Huo, Z. Zhu, L. Wei, C. Han, X. Zhou, A visually secure image encryption scheme based on 2D compressive sensing and integer wavelet transform embedding, Opt. Commun. 492 (2021) 126976.
[24] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy, Signal Process. 171 (2020) 107525.
[25] X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, Y. Chen, An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing, Inform. Sci. 556 (2021) 305–340.
[26] Q. Xu, K. Sun, S. He, C. Zhu, An effective image encryption algorithm based on compressive sensing and 2D-SLIM, Opt. Lasers Eng. 134 (2020) 106178.
[27] S. Patel, A. Vaish, A systematic survey on image encryption using compressive sensing, J. Sci. Res. 64 (1) (2020) 291–296.
[28] S. Patel, A. Vaish, Double image encryption through compressive sensing and discrete cosine stockwell transform, in: Machine Intelligence and Smart Systems, Springer, Singapore, 2022, pp. 199–206.
[29] S.C. Phatak, S.S. Rao, Logistic map: A possible random-number generator, Phys. Rev. E 51 (4) (1995) 3670.
[30] C. Li, G. Luo, K. Qin, C. Li, An image encryption scheme based on chaotic tent map, Nonlinear Dynam. 87 (1) (2017) 127–133.
[31] E.R. Henry, J. Hofrichter, Singular value decomposition: Application to analysis of experimental data, in: Methods in Enzymology, Vol. 210, Academic Press, 1992, pp. 129–192.
[32] D. Chevizovich, D. Michieletto, A. Mvogo, F. Zakiryanov, S. Zdravkovic, A review on nonlinear DNA physics, R. Soc. Open Sci. 7 (11) (2020) 200774.
[33] D.N.V.S.L.S. Indira, Y.K. Viswanadham, J.N.V.R. Swarup Kumar, C. Suresh Babu, V. Rao, Reversible data hiding using LSB scheme and DHE for secured data transfer, in: Intelligent Data Communication Technologies and Internet of Things, Springer, Singapore, 2022, pp. 519–528.
[34] A. Hagag, E.S. Hassan, M. Amin, F.E. Abd El-Samie, X. Fan, Satellite multispectral image compression based on removing sub-bands, Optik 131 (2017) 1023–1035.
[35] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, Image Quality Assessment: From Error Visibility to Structural Similarity, IEEE, 2004.
[36] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, Int. J. Bifurcation Chaos 16 (08) (2006) 2129–2151.