applied sciences

MDPI

Article

Quad Key-Secured 3D Gauss Encryption Compression System with Lyapunov Exponent Validation for Digital Images

Sharad Salunke [1], Ashok Kumar Shrivastava [2], Mohammad Farukh Hashmi [3], Bharti Ahuja [4] and Neeraj Dhanraj Bokde [5,*]

[1] Department of Electronics and Communication Engineering, Amity University MP, Gwalior 474005, India
[2] Department of Computer Science and Engineering, Amity University MP, Gwalior 474005, India
[3] Department of Electronics and Communication Engineering, National Institute of Technology, Warangal 506004, India
[4] Department of Information Technology, National Institute of Technology, Raipur 492010, India
[5] Center for Quantitative Genetics and Genomics, Aarhus University, 8000 Aarhus, Denmark
* Correspondence: neerajdhanraj@qgg.au.dk

Abstract: High-dimensional systems are more secure than their lower-order counterparts. However, high security with these complex sets of equations and parameters reduces the transmission system's processing speed, necessitating the development of an algorithm that secures and makes the system lightweight, ensuring that the processing speed is not compromised. This study provides a digital image compression–encryption technique based on the idea of a novel quad key-secured 3D Gauss chaotic map with singular value decomposition (SVD) and hybrid chaos, which employs SVD to compress the digital image and a four-key-protected encryption via a novel 3D Gauss map, logistic map, Arnold map, or sine map. The algorithm has three benefits: First, the compression method enables the user to select the appropriate compression level based on the application using a unique number. Second, it features a confusion method in which the image's pixel coordinates are jumbled using four chaotic maps. The pixel position is randomized, resulting in a communication-safe cipher text image. Third, the four keys are produced using a novel 3D Gauss map, logistic map, Arnold map, or sine map, which are nonlinear and chaotic and, hence, very secure with greater key spaces (2^{498}). Moreover, the novel 3D Gauss map satisfies the Lyapunov exponent distribution, which characterizes any chaotic system. As a result, the technique is extremely safe while simultaneously conserving storage space. The experimental findings demonstrate that the method provides reliable reconstruction with a good PSNR on various singular values. Moreover, the applied attacks demonstrated in the result section prove that the proposed method can firmly withstand the urge of attacks.

Keywords: 3D Gauss map; Arnold map; compression; encryption; logistic map; singular value decomposition; sine map

check for updates

Citation: Salunke, S.; Shrivastava, A.K.; Hashmi, M.F.; Ahuja, B.; Bokde, N.D. Quad Key-Secured 3D Gauss Encryption Compression System with Lyapunov Exponent Validation for Digital Images. *Appl. Sci.* **2023**, *13*, 1616. https://doi.org/10.3390/app13031616

Academic Editor: Luis Javier Garcia Villalba

Received: 17 December 2022
Revised: 16 January 2023
Accepted: 23 January 2023
Published: 27 January 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the phenomenal expansion of social networks and the remarkable progress of communication networks, image transfer has become an established standard since images are highly expressive and informative forms of communication. As a result, there is a necessity for cryptographic techniques to maintain image security. It is critical to consider the unique properties of image data while constructing an encryption method, such as substantial redundancy and significant correlation among neighboring pixels. Because of the uniqueness of image properties, traditional cryptographic algorithms are not suited for visual cryptography. Many methods, including chaotic systems [1,2], DNA encoding [3], cellular automata [4], quantum image encryption [5], and transforms, such as FRFT [6,7], Affine [5], etc., have been proposed to solve the obstacles provided by the distinctive visual features. On the contrary, encryption alone is insufficient to meet today's demands

for rapid transmission and reduced storage space. As a result, numerous scientists have made significant contributions in this area and have successfully presented compression encryption techniques. Some very promising and related works are discussed further.

Compression and encryption are performed concurrently, fastening calculations and bringing more security. Using the spark concept, Ghaffari [8] established the uniqueness criteria of 2D sparse recovery. The uniqueness criteria are improved by the regularity of sparse parameters in columns and rows, resulting in better compression and sparse rebuilding. The sparse depiction is disrupted by chaotic confusion. This phase aids in fulfilling the said criteria and increases the cryptographic safety index. The chaos pattern is then applied to form two orthogonal measuring matrices. The sparse encrypted form is compressed in two dimensions using the singular value decomposition. Further, a compressed–encrypted matrix built on chaos-based uncertainty is utilized to diminish the correlation across neighboring pixels in the compressed matrices, creating a homogenous allocation in the ciphered image. Finally, the XOR procedure is used to encrypt the data. Depending on the smoothing standard in the decryption procedure, researchers have incorporated the variation restriction to the 2D sparse recovery problem in order to improve compression performance.

In another work, Chaudhary et al. [9] presented a technique based on compression encryption. Here, the column-wise scan–optimization compression approach is employed instead of zigzag scanning. The Huffman encoding of JPEG compression is then replaced with arithmetic coding in entropy stage encoding. As with the one-time pad, an image is encrypted with XOR encryption, which is unbreakable in security. Moreover, the compressed information is XORed with a random integer.

In a DCT-based compression encryption technique, Wen et al. suggest employing DCT and chaos to provide high-quality image encryption. In this work, the image hash value is first utilized to create a plaintext-correlated encryption key, and then lightweight chaos is created to build a pseudo-random sequence. Second, to construct the DCT coefficient matrix, DCT and quantize 8×8 subblocks are created. Then, using the DCT matrix, extraction of the DC and AC coefficients for compression coding are achieved. Reconstruction of the ciphertext takes place after permuting the DC coefficient bitstream with the chaotic sequence. By diffusing the ciphertext and hiding the hash value, the final ciphertext is acquired. The algorithm features a good compression rate, and a vast key space [10]. Yet another approach by Li et al. [11] proposed quantum cosine transform-based image compression–encryption. Here, the quantum discrete cosine transform and 5D hyperchaotic system are used for compression and encryption with the zigzag technique.

It is important to compress and encrypt multimedia information, particularly digital images, simultaneously. This challenge has been solved through the development of compressive sensing. Tang et al. proposed a method based on compressive sensing (CS) for compression encryption [12]. Compressive sensing compresses and encrypts data simultaneously; this not only reduces network communication bandwidth but also enhances system security. However, while using compressed sensing cryptography, the entire assessment matrix must be saved; moreover, once compressive sensing is merged with a chaotic map, only the matrix's generation variables must be saved. The system's confidentiality could be further enhanced by using the chaos system's sensitivity. In this method, the innovative and universal chaotic structure generates the chaotic map employed in the strategy, which widens the chaotic area of the chaos structure and enhances its effectiveness.

CS using the chaos measurement matrices provides a high data sensitivity, according to Zhu et al. [13]. Nevertheless, the plaintext sensitivity provided by CS may be significantly diminished due to the quantification performed following CS. Authors in this method developed a novel CS-compression–encryption architecture that makes use of the CS's intrinsic characteristic of providing robust plaintext sensitivity for the proposed technique with minimal additional processing. Meanwhile, a chaos-based substitution box (S-box) building algorithm is being developed.

In one more method of CS, Zhu et al. [14] proposed a CS and cyclic shift hypothesis-based digital image compression–encryption framework. First, the digital image is compressed using a random Gauss sequence and sparse transform. Moreover, after compressive sensing, cyclic shift and diffusion processes are established.

The image encryption method relies on the 2D logistic sine map is also presented by Ye et al. [15]. In the chaotic area, permutation, modulation, and diffusion are all part of the encryption process. The permutation operation is performed cyclically in both the column and row orientations simultaneously. In this work, next, a permuted image modulation function generates the encrypted image, followed by column-wise diffusion. It solves the problem of typical encryption algorithms that need a lot of pixel shuffle before the diffusion phase. In another work presented by Wen et al., color image encryption is done using DNA computing and non-degenerate discrete hyperchaos. Here simulation results and positive Lyapunov exponent indicates, a fast, more secure, and robust image encryption scheme [16].

To accomplish image encryption and compression with reconstructing reliability and strong security, Zhang et al. [7] presented a visual compression and encryption system built on CS and the Fourier transform. Encryption and compression are integrated by utilizing the CS characteristic. To circumvent the security restrictions of releasing the energy content of the plaintext from ciphertext and reprocessing the assessment matrices, a chaos procedure and 2D-FRFT are used to perform encryption. Additionally, diffusion encryption based on double random phase cryptography in 2D may avoid reconstruction resilience loss.

In a study proposed by Vaish et al. [17], singular value decomposition (SVD) in the discrete cosine Stockwell transform (DCST) is used to encrypt color images. SVD's DCST properties and permutation method give more secure data. Decrypting encrypted images requires knowing all the keys and their contents. The work's robustness study shows that if one parameter is wrong and the others are right, it is practically difficult to estimate the original image information.

Kumar et al. [18] offer another encryption compression approach based on SVD. Here, the sender used DWT to reconstruct the image. A pseudo-random integer sequence and a pseudo-random permutation are used to encrypt the approximation and detail sub-bands. The channel provider 'losslessly' compresses the encrypted approximation sub-band, reducing image size without compromising quality. Using SVD and Huffman to compress encrypted detail sub-bands. Choosing important information from detail subbands results in effective compression while maintaining image quality. To reconstitute the image, the receiver decompresses, decrypts, and inverts DWT-encrypted and compressed bit streams.

Memory use and the suitable architecture of the intended result from the compression method impact the entire usefulness of the generated work. Therefore, effectiveness is crucial in the development of the compression strategy. SVD is a common factorization process for collecting precise information on a matrix since it is a technologically costly method. Data compression is one of its many applications since it may minimize the volume of data needed to encode an image while keeping the image quality intact; therefore, it is a suitable choice among various compression techniques.

Among all of the discussed methods above, high-dimensional and multidimensional systems [19–21] are proven to be more secure as compared to their lower-order counterparts, but high security with these complex sets of equations and parameters decreases the processing speed of the transmission system adversely; therefore, there is a requirement of an algorithm, which not only secures the system with higher dimensional orders but also makes the system lightweight so the processing speed cannot be compromised. Keep in mind that the quad key-secured 3D Gauss chaotic map is proposed here in this work.

The main highlights of the proposed scheme are as follows:

1. The suggested quad key-secured system is based on the novel 3D Gauss map.
2. To assure dependability and unpredictability, the pixels of the quad key-secured encryption system are permuted with four recommended chaotic sequences.

3. The integrated image's pixels are changed with the proposed four types of chaos after being randomly shuffled in rows and columns in order to withstand the attack and obtain better results.
4. The proposed 3D Gauss map boosts the key's sensitivity while also creating significant variances in the image pixels.
5. An increased set of parameters might boost resistance to an attack while boosting unpredictability and reducing security breaches.
6. The SVD compression strategy provides the user with a degree of compression flexibility, allowing the user to compress the image proportional to the demand for space and storage while still providing good privacy.
7. The simulation and comparison results are used to examine the superiority and efficiency of the proposed strategy with several attacks and tests.

The rest of the contents are split into the following sections: The essential concepts are discussed in Section 2. Then, the recommended algorithm is illustrated in Section 3, and the simulation results are presented in Section 4 by the simulation experiments. Further, Section 5 is dedicated to the security analysis and comparison. Finally, Section 6 presents our conclusion.

2. Important Terms

2.1. Singular Value Decomposition (SVD)

It is the most often used technique for dividing matrices into component matrices and showing the main attributes of the source matrices. The source may be rebuilt using the matrices that make up the input. The compression method relies on altering the decomposition to produce low-rank approximation matrices. The approach achieves lossy compression as the recovered matrices vary slightly from the source matrix. SVD has a wide range of applications, including rank, numerical error, and low-rank approximation [22,23]. One such use that will be covered in this study is data compression.

One of the benefits of SVD is its capability to work with both kinds of matrices (viz. square and rectangular). An image is just a 2D matrix of numbers that represent the image's pixels. Figure 1 and Equation (1) depict the three matrices U, d, and V that result from the matrix M being split in half. U and V are perpendicular to each other, and d is diagonal; their single values are arranged in ascending order along U, V, and d.

$$M_{m\times n} = U_{m\times r} d_{r\times r} (V_{n\times r})^T \tag{1}$$

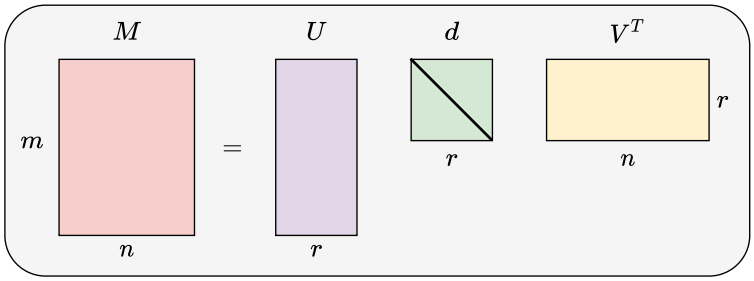


Figure 1. Matrix representation of SVD.

2.2. Chaotic Maps

2.2.1. Logistic Map

The logistic map is a chaotic system with a simple notion but complicated behavior. Because a logistic map is a one-dimensional map, each iteration of the map yields a single value, which is referred to as an iterate. A single parameter (a) is used in logistic map computations. Because of its basic though nonlinear architecture, it is probably the most often utilized chaotic maps in image encryption [24]. Mathematically, it is written as:

$$z_{n+1} = a \times z_n \times (1 - z_n) \tag{2}$$

In the equation, $n \in \{1, 2, 3, 4 \cdots N\}$ and N is the total number of iterates. In the map, $a \in 0, 4$ is called the control parameter also. The first bifurcation in the logistic map behavior comes at $a \sim 3$; hence, its behavior is deterministic up to that point. It becomes difficult to predict where the next iterate value will lay after many bifurcations have occurred since the number of alternative iterate value paths grows exponentially. The region about $a = 4$ exhibits the most chaotic behavior, yet there are still regions with suppressed chaos, such as at $a = 3.85$.

2.2.2. Sine Map

With an output range of $[0, 1]$, the sine map is a chaotic one-dimensional map. As can be seen in Figure 2, the sine map's graph is geometrically comparable to the logistic map's plot.

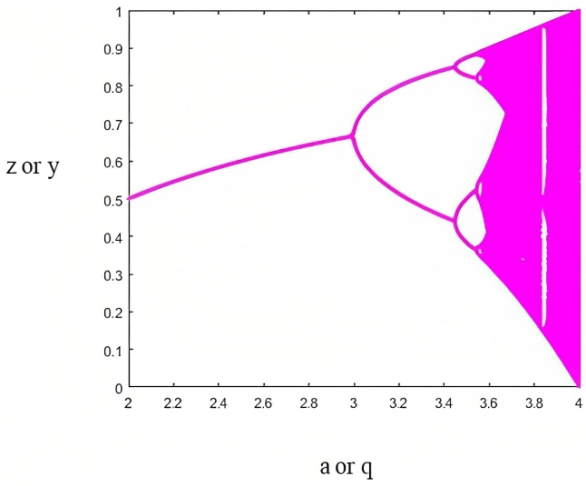


Figure 2. Characteristic representation of the logistic and sine maps.

Unimodal maps are those that have only one axis. Similar to the polynomial that represents the logistic map, sine is a fundamental function rather than an arithmetic function. It is mathematically given by Equation (3), wherein q is the control variable [25].

$$y_{i+1} = q \times sin(\pi y_i) \tag{3}$$

2.2.3. Arnold Cat Map

Firstly, Arnold demonstrated this map's chaotic qualities with a painting of a cat, hence, named the Arnold cat map. Figure 3 shows a recurrent bending and twisting of a chaos pattern in a small region. It is also widely used in image cryptography [26].

If recurrent bending and twisting are repeated multiple times, the original image will almost certainly emerge. The length of Arnold will be proportional to the volume of simulations to be analyzed. The duration of time varies depending on the source images since it is related to the image dimension. Equation (4) is used to adjust the image compositions for each pixel.

$$\begin{bmatrix} \frac{u_{n+1}}{v_{n+1}} \end{bmatrix} = A \begin{bmatrix} \frac{u_n}{v_n} \end{bmatrix} (\text{mod } N) = \begin{bmatrix} 1 & \frac{p}{q} \\ q & pq + 1 \end{bmatrix} \begin{bmatrix} \frac{u_n}{v_n} \end{bmatrix} (\text{mod } N) \tag{4}$$

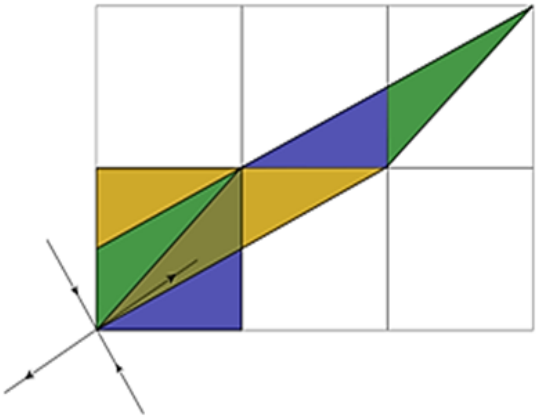


Figure 3. Axis representation of the Arnold map.

The transition, which follows Arnold's transformation, strikes an image and shuffles about the image's constituent parts from their original placement. If the algorithm is run enough times, the identical image will show each time. Arnold's period will be utilized to calculate the number of computations. The Arnold approach for image encryption is described in Algorithm 1.

Algorithm 1: Image encryption with Arnold map.

Input: I (original image), p, q;
Output: E (encrypted image)

Step 1: Read image I and obtain its $N \times N$ size;
Step 2: Let $im = I$ and E be a zero image with the same size as I;
Step 3: For each row u and column v, do:
$U = (u + vy) mod N + 1$;
$V = (pu + (pq + 1)v) mod N + 1$;
$E(U, V) = im(u, v)$;
Return

2.2.4. Gauss Map

A chaotic map generates pseudorandom numbers employed in the encryption process [9]. The Gauss map, often known as the Gaussian map, is a non-linear iterative function with precise intervals that was developed by Carl F. Gauss. For example, Equation (5) may produce pseudorandom numbers from a Gaussian map. α and β are the controlling parameters that exhibit chaotic behaviors.

$$x_{n+1} = e^{-\alpha \times x_n \times x_n} + \beta \tag{5}$$

where α and β are input parameters that substantially impact the Gaussian map outcomes, a Gaussian map will create a succession of random values. This sequence will be employed to generate random sequences of the same length. The bifurcation diagram of the Gauss map is shown in Figure 4.

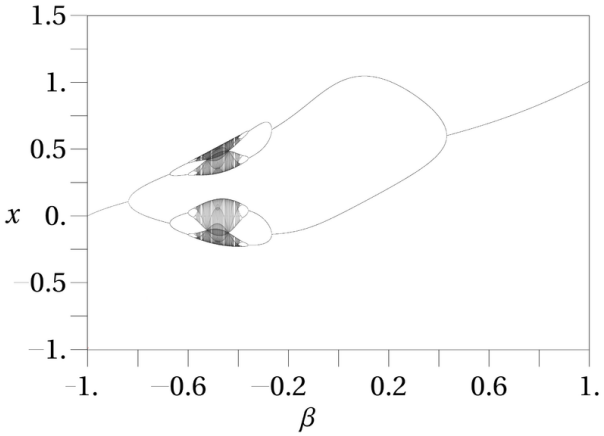


Figure 4. Representation of a Gauss map bifurcation.

2.3. Lyapunov Exponent (LE) and Lyapunov Exponent Chart (LEC) for Chaos

Lyapunov exponents indicate a system's predictability and sensitivity to modifications in its starting states [27]. They may be regarded as the average logarithmic rate of convergence of two neighboring points of two-time series X_t and Y_t separated by an initial distance $\triangle R_0 = ||X_0 - Y_0||^2$. The expression for LE is expressed as;

$$\lambda = \lim_{x \to \infty} \frac{1}{n} \sum_{i=1}^{n} ln \left| \frac{\triangle R_i}{\triangle R_0} \right| \tag{6}$$

The LE is an eigenvalue that may be used to characterize a chaotic system. Correlated Lyapunov exponents are integrated with multidimensional systems to form a LEC for further analysis. For a viscous dissipation system, the LEC represents the character of distinct orbits and describes the character stability of all orbits that leave from an attractor basin of attraction. The attractor is a fixed point in a one-dimensional system. The LE is a negative number. The attractor is either a stationary point or a limit cycle in a two-dimensional system. If it is a fixed point, the distance in phase space between two closed-up points of random direction will shorten. As a result, the two LEs must be negative this time. Here, LE is used to analyze the proposed 3D Gauss map's chaotic behavior toward initial values. The LE distribution for the 1D Gauss map is shown in Figure 5.

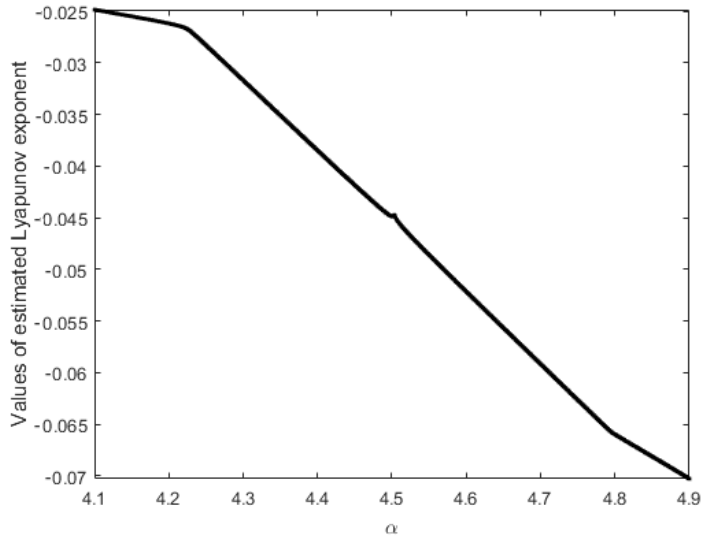


Figure 5. Lyapunov exponent distribution for the 1D Gauss map.

3. Implementation

3.1. 3D Gauss Map

The 3D Gauss map is a 3D variant of the current 1D Gauss form developed and used for the first time for cryptography applications. The 3D Gauss map equations are originally derived from (5) and expressed as:

$$x_{i+1} = e^{(-cx_i^2)} + d + by_i^2 x_i + az_i^3 \tag{7}$$

$$y_{i+1} = e^{(-cy_i^2)} + d + bz_i^2 y_i + ax_i^3 \tag{8}$$

$$z_{i+1} = e^{(-cz_i^2)} + d + bx_i^2 z_i + ay_i^3 \tag{9}$$

Here, x, y, and z are used as intervals, whereas the real numbers a, b, c, and d are employed as inputs. It is a very secure system using quadric, cubic, and quadratic coupling in the equations, as well as four constant components. During this process, the 3D Gauss developer generates a 3D Gauss map. Using the initial conditions of $x_1 = 0.4250$, $y_1 = 0.5250$, $z_1 = 0.6250$, $a = 0.0235$, $b = 0.0377$, $c = 4.9$, and $d = -0.68$, the resulting sequences are chaotic.

Several processes are done on the image in this technique for encryption. Row permutation operations are conducted in the first phase, followed by row rotation operations. When a random sequence is sorted by the key x, the pixel order in each row is permuted. The intermediate phase rotates pixels in rows based on whether the random sequence is odd or even. The operations of column permutation and column rotation are accomplished in the following phases. A pixel column permutation in which pixels are shifted about in accordance with a random sequence y. At this stage, the pixels in the column are rotated dependent on whether the random sequence is odd or even. In the last phase, the key sequence created by the key z is applied column by column to the whole image's bits, which have been partitioned into 8-bit blocks or shuffled images. Figure 6 explains the process of the 3D Gauss system that includes key generation and permutation combination.

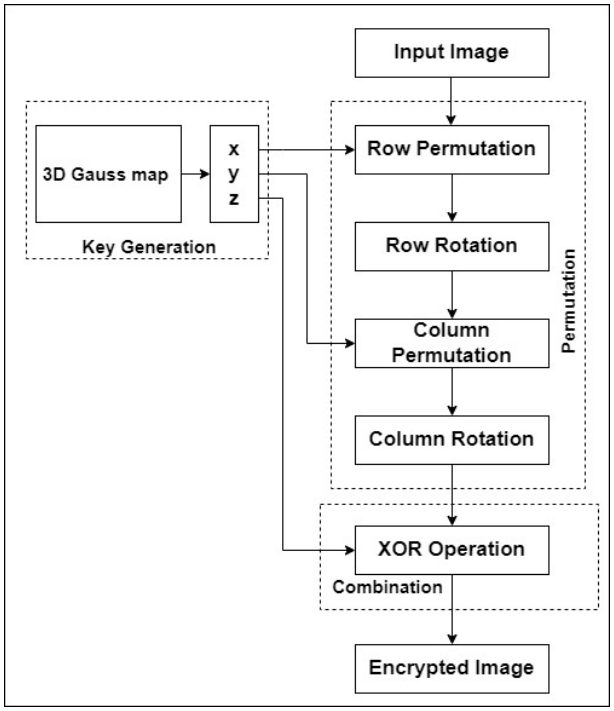


Figure 6. 3D Gauss map system.

3.2. Proposed Method

In this part, we offer a novel quad key-secured image encryption technique based on the three-dimensional Gauss map and the extended sine, logistic, and Arnold chaotic systems. The proposed method is separated into two stages: compression with SVD and scrambling with the pixel shuffle and the XOR operator. After illustrating two units of confusion constructed on a 3D Gauss chaotic map and establishing a measuring matrix, the remainder of this section covers the encryption process.

3.2.1. Quad Key Chaotic System (QKCS)

The encryption coefficient matrix is shuffled using the four chaotic subsystems to attain these circumstances in QKCS. This confusion also reduces the connection between encryption matrix components, which increases the confidentiality degree for the image of interest. The QKCS involves the following steps:

1. Using the 3D Gauss system approach with the logistic, Arnold, and sine maps generates the QKCS sequence $Z = \{zi\}$, given an initial condition with an acceptable step size.
2. Converting the sequence $Z = \{zi\}$ into the integer sequence $Z^* = \{zi^*\}$.

3.2.2. Chaotic Random and Singular Value Matrix Formation

The suggested technique begins by transforming the original image by using SVD. The encryption matrix is then calculated and compressed. We employed four types of chaos based on the QKCS to construct the chaotic random matrix here (to create the chaotic random matrix, the state variables of generalized logistics, Arnold, sine, and novel 3D Gauss models are employed). The following is the four-step process of the chaotic random and singular value matrix formation:

1. SVD computation:
$$X_M = USV^T \tag{10}$$
In (10), $S \in \mathbb{R}^{n1 \times n2}$ is a diagonal matrix containing singular values. The matrices $U \in \mathbb{R}^{n1 \times n2}$ and $V \in \mathbb{R}^{n1 \times n2}$ are unitary in which their columns are singular vectors.
2. Given a starting condition and an appropriate step size, we construct the sequence $Q = \{q_i\}$ of the QKCS using the 3D Gauss system, logistic, Arnold, and sine maps.
3. We convert the sequence $Q = \{q_i\}$ into the integer sequence $Q* = \{q_i*\}$.
4. We reconfigure the pattern $Q*$ to build the matrix Q_M, which is a random matrix created through the QKCS system.

3.2.3. Step-by-Step Image Encryption and Compression Process Based on the Quad Key System (Sender's Side)

Figure 7 depicts the recommended image compression and encryption technique procedure at the sender and receiver sides. The basic method consists of SVD and the combination of four chaotic maps, including a 3D Gauss map, an Arnold map, a logistic map, and a sine map. Figure 8 is a gallery of test images originally retrieved from the SIPI dataset. Furthermore, Figure 9 demonstrates the proposed algorithm for the Lena, Cameraman, Baboon, and Pepper images. Below is a detailed step-by-step description of the compression and encryption technique.

Step 1: Read an image A of size $M \times N$. Initially, the image is divided into three parts or matrices, i.e., U, S, and V, by using SVD, where S is a diagonal matrix containing the sorted singular values of the input matrix in descending order. The matrices U and V are orthogonal matrices in which their columns are singular vectors. For a given $M \times N$ input matrix, (11) below displays the sizes of the corresponding U, S, and V matrices.

$$A_{M \times N} = U_{M \times M} \cdot S_{M \times N} \cdot (V_{N \times N})^T \tag{11}$$

Step 2: The rank of the input matrix is determined by the number of non-zero elements on the diagonal of the matrix S. By approximating the original matrix with a matrix of the lower rank S, which is constructed by deleting tiny singular values, a compressed matrix is achieved.

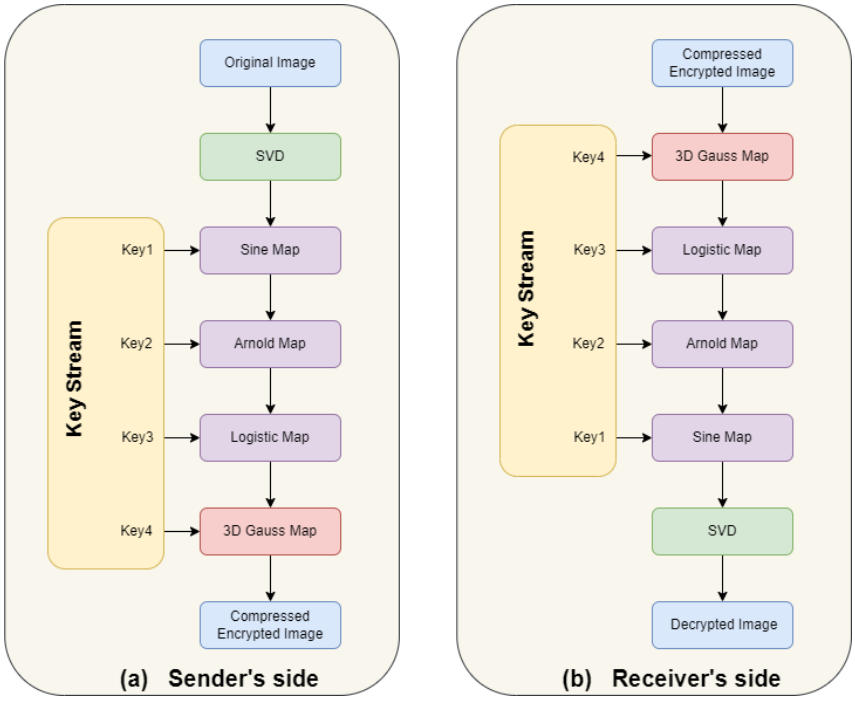


Figure 7. Proposed quad key-secured algorithm for the sender and receiver sides.

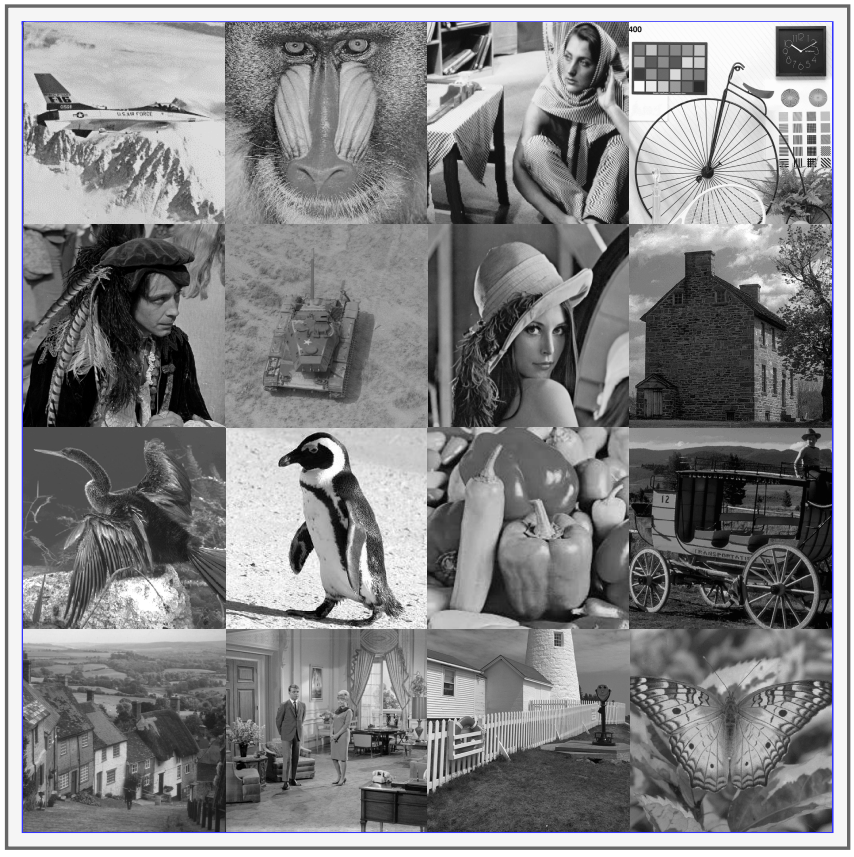


Figure 8. Test images (retrieved from the SIPI dataset).

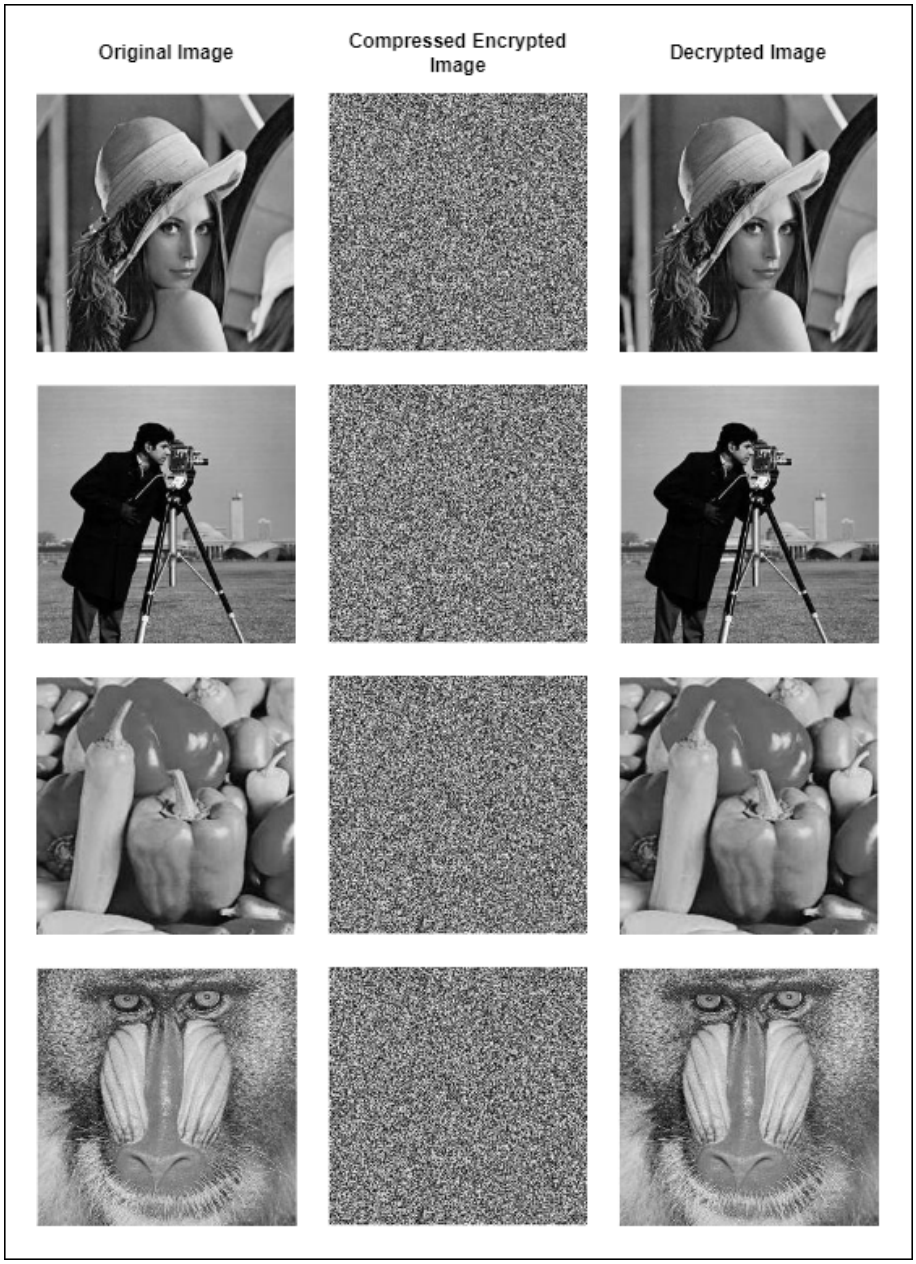


Figure 9. Results for the proposed quad key-secured algorithm.

Step 3: Using Equation (3) (sine map), the chaotic sequence x_i is created, and x_i is used to generate the diffusion sequence by (12).

$$X_i = mod(floor(x_i \times 10^5), 256) \tag{12}$$

Then, as shown in (13), perform a bitwise XOR operation on the compressed image A'.

$$A1 = A' \oplus X_i \tag{13}$$

Step 4: Apply Equation (4), to obtain the scrambled image ($A2$) by using the Arnold transformation (see Algorithm 1 in Section 2.2.3).
Step 5: Using Equation (2) (logistic map), the chaotic sequence y_i is created and y_i is used to generate the diffusion sequence by (14).

$$Y_i = mod(floor(y_i * 10^5), 256) \tag{14}$$

Then, as shown in (15), perform a bitwise XOR operation on the $A2$ image.

$$A3 = A2 \oplus X_i \tag{15}$$

Step 6: A 3D Gauss map is used to generate the final key. In this key, we employed Equations (7)–(9), to produce the pseudo-random sequences x, y, and z as seen in Figure 6.
Step 7: Image $A3$ is first read, and then row and column permutations using x and y sequences are used to produce a shuffled image. Then, using the XOR operation with the shuffled image and the z sequence, one may obtain the compressed–encrypted image $A4$.

3.2.4. Step-by-Step Image Decryption Based on Quad Key System (Receiver's Side)

The image decryption process is illustrated in Figure 7b. This is the reverse process of the encryption algorithm, and image reconstruction or detailed decryption steps are as follows.
Step 1: The encrypted image $A4$ is input, and then row and column permutations using x and y sequences are used to produce a shuffled image. Then, using the XOR operation with the shuffled image and the z sequence, one may obtain the compressed decrypted image $B4$. (Pseudo-random sequences x, y, and z are obtained by a 3D Gauss map, as explained above).
Step 2: Using Equation (2) (logistic map), the chaotic sequence y_i is created and y_i is used to generate the diffusion sequence by (14).

Perform a bitwise XOR operation on the $B4$ image, The inverse diffusion operation can be expressed as follows:

$$B3 = B4 \oplus Y_i \tag{16}$$

Step 3: To obtain the unscrambled image ($B2$), apply the inverse Arnold transformation. (See Algorithm 1 in Section 2.2.3).
Step 4: Using Equation (3) (sine map), the chaotic sequence x_i is created and x_i is used to generate the diffusion sequence by (12).

Perform the bitwise XOR operation on image $B2$. The inverse diffusion operation can be expressed as follows:

$$B1 = B2 \oplus X_i \tag{17}$$

Step 5: Finally, we combine all of the subcomponents of SVD to obtain the decrypted image B, as described by (18).

$$B_{M\times N} = U_{M\times M} \cdot (B1_{M\times N})^{-1} \cdot (V_{N\times N})^{T} \tag{18}$$

4. Results and Analysis

4.1. PSNR and MSE

The quality check of the decrypted image is initially analyzed by the two primary metrics, i.e., $PSNR$ (peak signal-to-noise ratio) and MSE (mean square error) [8]. Mathematically, they are expressed as:

$$PSNR = 10 \log_{10}\left[\frac{256 \times 256}{MSE}\right] \tag{19}$$

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[f'(i,j) - f(i,j)\right]^2 \tag{20}$$

Results of $PSNR$ and MSE of the proposed method for different test images are shown in Table 1.

Table 1. Different measurement metric results for the proposed method.

Image	PSNR	SSIM	MSE	Entropy	Horizontal	Vertical	Diagonal
Cameraman	46.5790	0.9872	1.4295	7.9971	0.0022	0.0007	−0.0020
Barbara	32.1581	0.8954	39.5617	7.9994	0.0001	−0.0053	−0.0007
Pepper	51.6533	0.9967	0.4444	7.9993	−0.0021	0.0002	0.0001
Lena	45.8460	0.9905	1.6923	7.9974	−0.0013	0.0020	0.0023
Baboon	34.0663	0.9519	25.4946	7.9969	−0.0025	0.0004	0.0004
Boat	36.7878	0.9327	13.6239	7.9993	−0.0047	0.0001	−0.0005

4.2. Structural Similarity Index Measure (SSIM)

The $SSIM$ evaluates the connection between a reconstructed image and a reference image [28]. It is used to calculate consistency by multiplying three factors: structure, brightness, and contrast. Therefore, the $SSIM$ should be characterized as follows:

$$SSIM(p,q) = l(p,q)c(p,q)s(p,q)\begin{cases} l(p,q) = \frac{2\mu_p\mu_q+C_1}{\mu_p^2+\mu_q^2+C_1} \\ c(p,q) = \frac{2\sigma_{fp}\sigma_q+C_2}{\sigma_p^2+\sigma_q^2+C_2} \\ s(p,q) = \frac{\sigma_{fg}+C_3}{\sigma_p\sigma_q+C_3} \end{cases} \tag{21}$$

Table 1 shows the SSIM of the suggested approach for several test images.

4.3. Information Entropy (IE)

The uncertainty of a visual system is measured using a metric called IE [28]. When entropy is high, the distribution of grayscale values is stable. In addition, an ideal arbitrary image has an entropy of 8. Here is a formula for calculating the entropy of information:

$$E(m) = \sum_{i=0}^{L-1} p(m_i)\log_2\frac{1}{p(m_i)} \tag{22}$$

Here, $L = 256$ denotes the number of gray values and $p(m_i)$ is the likelihood of a gray value appearing. The entropy of several test images is illustrated in Table 1. The 256×256 and 512×512 images are utilized for execution, as illustrated in Figure 8. The simulation is carried out using MATLAB 2016a.

4.4. Correlation Coefficient (CC)

The strength of a link between two data points may be quantified statistically by calculating the correlation coefficient. In a visual world, there is a lot of coherence between neighboring pixels in every direction. Safe image encryption relies on the fewest possible shared features among pixels, as demonstrated by [8]. The joint distribution of horizontally adjacent pixels in the original and encrypted images is shown in Figure 10.

After analyzing the important protection criteria in the preceding section, the suggested approach is compared to other ways to establish its efficiency level. Lena is a typical example image in most image protection systems. As seen in Table 1, the suggested method outperforms existing strategies in terms of the correlation coefficient and entropy. Furthermore, it has the strongest security level because it has the highest entropy value and the lowest correlation coefficient compared to the other compared references. As a result, the suggested technique has a greater security level. Therefore, it may be employed in a variety of real-time applications.

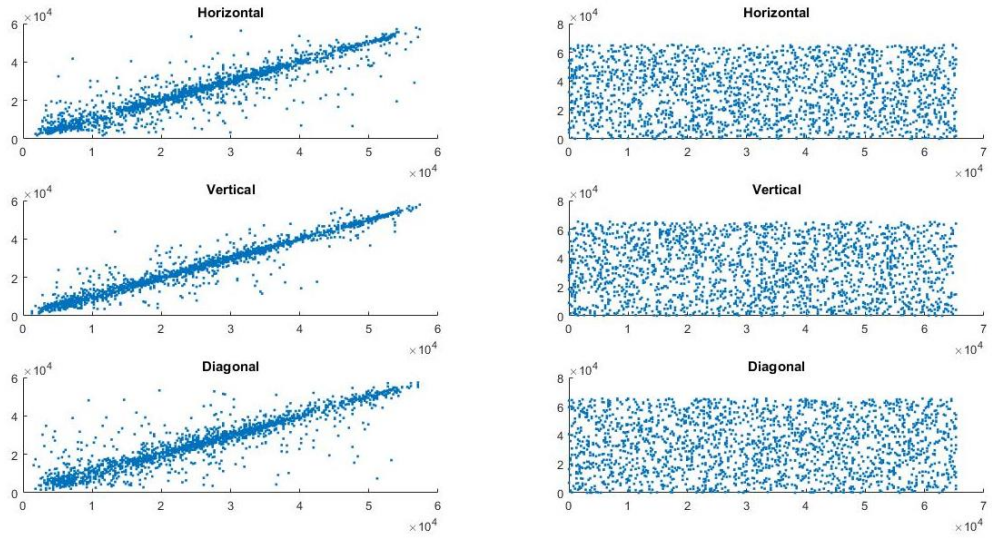


Figure 10. Horizontal, vertical, and diagonal correlation coefficients of the original (**left**) and encrypted (**right**) Lena image.

4.5. Lyapunov Exponent Analysis

Lyapunov exponents are used to describe the typical chaotic system because they measure a system's predictability and sensitivity to changes in its starting conditions [27]. The proposed 3D Gauss map's Lyapunov exponent graph is shown in Figure 11. The pattern similarity of the 3D Gauss map in Figure 11 with the 1D Gauss map (from Figure 5) proves the successful generation of a 3D Gauss chaotic map.

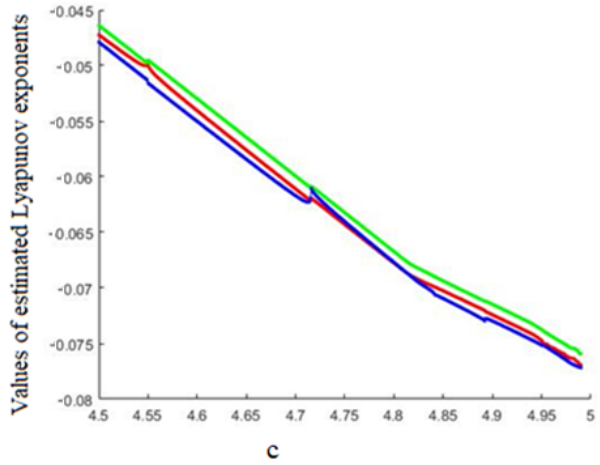


Figure 11. Lyapunov exponent distribution for 3D Gauss map.

4.6. Time Execution Analysis

The time spent running an algorithm is a crucial metric for gauging a cryptographic technique's effectiveness. The proposed procedure is put through its paces on the following hardware: The PC has a 1.60 GHz Intel(R) Core(TM) i5-8265U processor, 8 GB of RAM, and Windows 10. Computer simulations in MATLAB R2016a are used to carry out the encrypting and decrypting processes. It took 1.320452 s to encrypt the test image.

5. Security Analysis and Comparison

An important part of an image encryption algorithm is security analysis. This section assesses its effectiveness from four angles in order to define the level of security: histogram analysis, key sensitivity, robustness, and as well as correlation.

5.1. Histogram Analysis

A histogram is a measure that is used to evaluate the efficacy of an encryption scheme. A good histogram for a secure cryptosystem is a homogenous distribution that makes the process of encryption immune to statistical attacks [29]. The chi-square analysis is used to measure the uniform distribution of the histogram for more evaluation. Figure 12 shows the histograms of the original, compressed–encrypted, and decrypted images; Table 2 illustrates the χ^2 test results for the proposed method.

Table 2. χ^2 test results for the proposed method for different test images.

Images	Cameraman	Pepper	Baboon	Lena
Encrypted image	254.29	252.93	249. 38	258.44

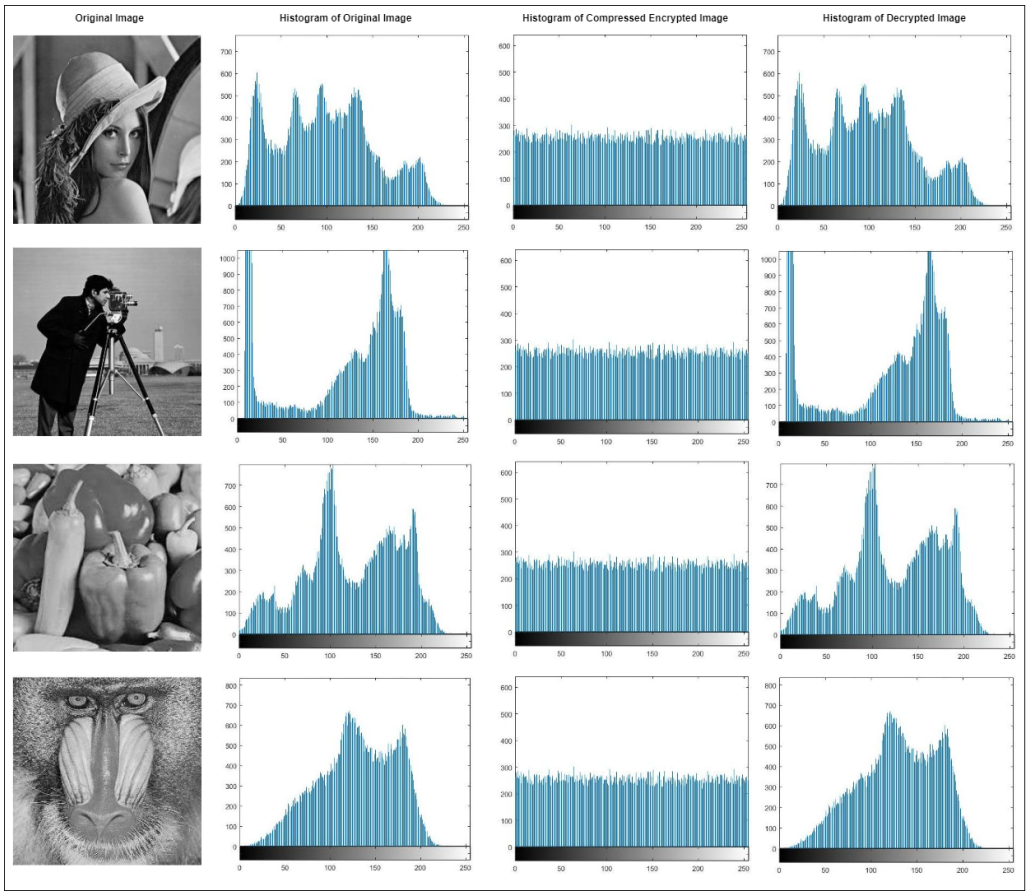


Figure 12. Histogram representation of selected test images.

The results in Table 2 and Figure 12 indicate that the histograms of the encrypted images are evenly distributed. The results of the above analysis show that the suggested method can effectively conceal the information on the image's pixel value distribution.

5.2. Key Sensitivity Analysis

In a safe cryptosystem, even a slight change to the secret key results in a decoded image that is significantly different from the original. To ensure the safety of the keys, the suggested method relies on the chaotic system's sensitivity to the starting conditions [29]. Several incorrect keys are represented in Figure 13 as decrypted Lena images. Each pair of keys has one incorrect key while all the others are correct. However, the deciphered image is notably deformed. In Figure 13, the decoded or decrypted Lena image with incorrect keys: (a) decoded image using $a + 10^{-15}$; (b) decoded image using $b + 10^{-15}$;

(c) decoded image using $c + 10^{-15}$; (d) decoded image using $d + 10^{-15}$; (e) decoded image using $x^1 + 10^{-15}$; (f) decoded image using $y^1 + 10^{-15}$; (g) decoded image using $z^1 + 10^{-15}$, (h) decoded image using $p + 10^{-15}$, (i) decoded image using $q + 10^{-15}$, and (j) decoded image using $r + 10^{-15}$.

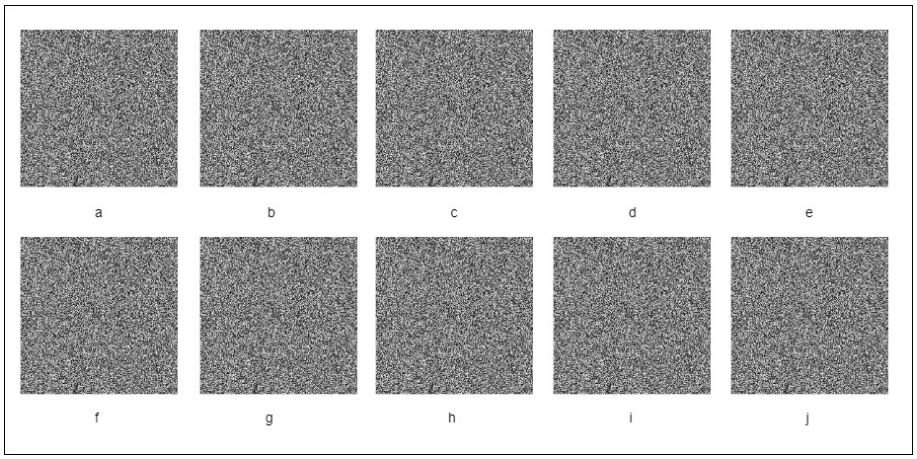


Figure 13. Key sensitivity analysis on the application of wrong keys.

5.3. Noise Attack

Images usually suffer some degradation during transmission. We evaluate the suggested method's resistance to noise threats, such as salt and pepper noise in this section (SPN) [8]. The Lena image is utilized as a test image in this simulation. Figure 14 shows the encrypted images with varying levels of noise attack (noise density 0.005). As a consequence, we can infer that the suggested method has the highest level of resistance to SPN attacks. Furthermore, these results demonstrate that the suggested encryption approach is capable of recovering the original image in the midst of a noise attack.

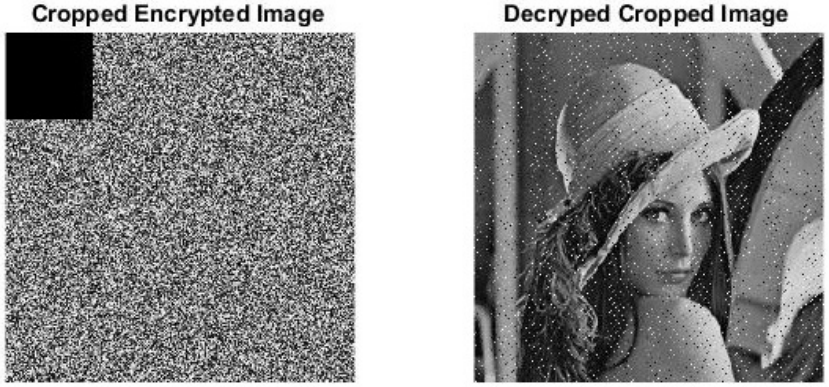


Figure 14. Noise attack.

5.4. Cropping Attack

The cropping attack is a key difficulty in image transmission [8]. The encrypted image has some pixels missing. Moreover, because the suggested image encryption is based on chaotic hybrid maps, it is resistant to data loss (6.25%) and can successfully retrieve the original image. The suggested approach's performance for cropping masks is examined, and the results are displayed in Figure 15. The encrypted images and their PSNR indicate the suggested method's resilience in the face of a cropping attack. The PSNR values of the cropped encrypted image vs. the noisy encrypted Lena image are shown in Table 3.

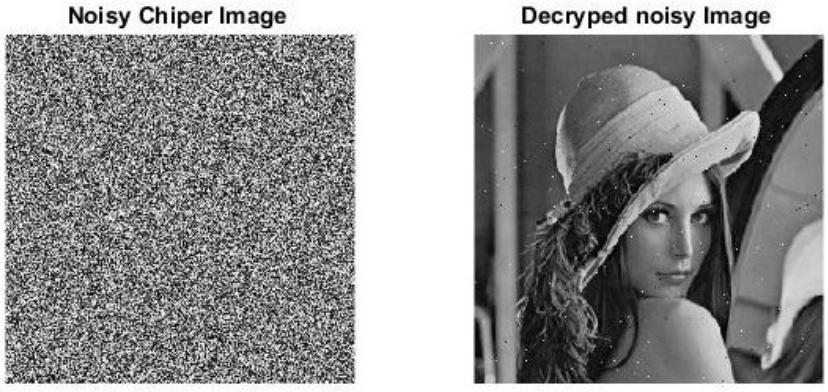


Figure 15. Cropping attack.

Table 3. Cropped encrypted image PSNR vs. the noisy encrypted image for the Lena image.

Image	Cropped Encrypted Image PSNR	Noisy Encrypted Image PSNR
Lena	20.675432	31.912601

5.5. Differential Attack

A differential attack is an attack on an encryption system that involves comparing and analyzing individual differences in plaintext concerning changes sent during encryption. The capacity to survive differential attacks is closely related to the sensitivity of the plaintext image. The number of changing pixel rates ($NPCR$) and unified average change intensity ($UACI$) of the encoded image can also measure the method's ability to survive differential assaults. The most common approaches for determining plaintext sensitivity are $NPCR$ and $UACI$ analyses [30]. Table 4 displays the simulation results for the $NPCR$ and $UACI$ mathematical structures. Mathematically, $NPCR$ and $UACI$ are expressed as:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} K(i,j) \times 100\% \tag{23}$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|a_1(i,j) - a_2(i,j)|}{255} \times 100\% \tag{24}$$

Table 4. $NPCR$ and $UACI$ results of various test images.

Images	$NPCR$ (%)	$UACI$ (%)
Peppers	99.58	33.34
Man	99.59	33.35
Baboon	99.61	33.41
Barbara	99.57	33.33
Boat	99.64	33.43
Lena	99.62	33.42

5.6. Randomness Test

The NIST test [31] is the global standard for testing the randomness of a time series. We investigate the randomness of the chaotic sequences produced by the suggested approach in the NIST test using 12 different random testing methodologies. Table 5 displays the results of NIST tests conducted on the proposed method.

Table 5. The outcomes of NIST tests on the suggested approach.

Test	Values	Results
Frequency	0.0359	Success
Block Frequency	0.2714	Success
Cumulative Sums Forward	0.0120	Success
Cumulative Sums Reverse	0.5171	Success
Runs	0.8475	Success
Longest Run	0.4237	Success
Rank	0.2785	Success
FFT	0.5650	Success
Overlapping Template	0.3225	Success
Approximate Entropy	0.2464	Success
Linear Complexity	0.1145	Success
Serial	0.1454	Success

5.7. Keyspace

To make the brute-force search difficult, the keyspace of an image encryption technique should normally be rather wide. Equation (25) is the formula used for calculating an approximate keyspace size. It is of the utmost importance to determine which parameters are the original secrets. In principle, the keyspace for this approach can be as large as necessary or infinitely theoretically. The suggested method employs several different cryptographic keys, including a, b, c, d, x^1, y^1, and z^1 for the 3D Gauss map (key 4), and p (key 1), q (key 2), and r (key 3) for the logistic, Arnold, and sine maps, respectively. Quantifying the complete keyspace makes use of the IEEE floating-point standard [32]. The comparison of keyspace among various recent literature is tabulated in Table 6.

$$\text{Keyspace} = 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} = 10^{150} \approx 2^{498} \quad (25)$$

Table 6. Keyspace comparison of the proposed scheme with different literature studies.

Methodologies	Proposed	[8,33]	[34]	[35]	[36]	[37]	[38]	[39]	[29]
Keyspace	2^{498}	2^{300}	2^{276}	2^{232}	2^{398}	2^{363}	2^{397}	2^{426}	2^{478}

5.8. Compression According to Different Singular Values

The main advantage of using SVD for compression gives freedom to a user. Users may choose the appropriate compression level with encryption according to the different singular values, as displayed in Table 7. Figure 16 illustrates the PSNR of the cameraman image at various singular values. Figure 17 shows the SSIM of the cameraman image on various singular values, and Figure 18 shows the PSNR and SSIM of the various test images on 150 singular values.

Table 7. PSNR and SSIM on varied singular values for different test images.

Images	Singular Values	PSNR	SSIM
LENA	75	22.7925	0.9247
	100	38.2170	0.9599
	125	41.9426	0.9799
	150	45.8460	0.9905
	175	50.1768	0.9961
	200	55.9573	0.9989
	225	68.0090	0.9999

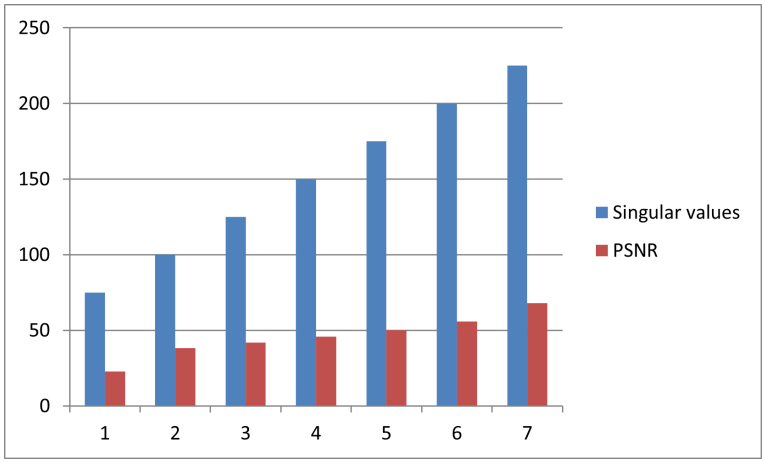


Figure 16. PSNR of the cameraman image on different singular values.

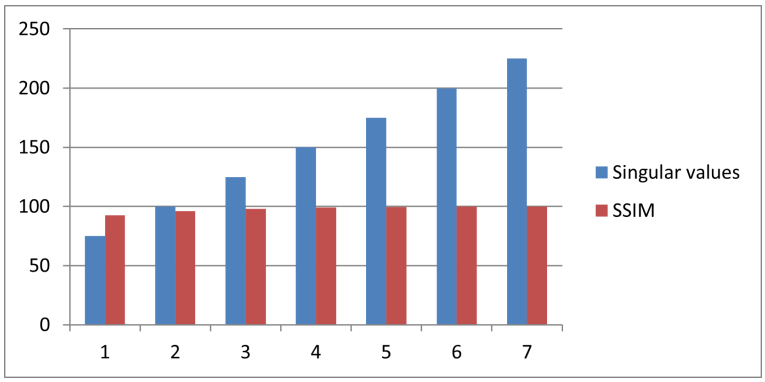


Figure 17. SSIM of the cameraman image on different singular values.

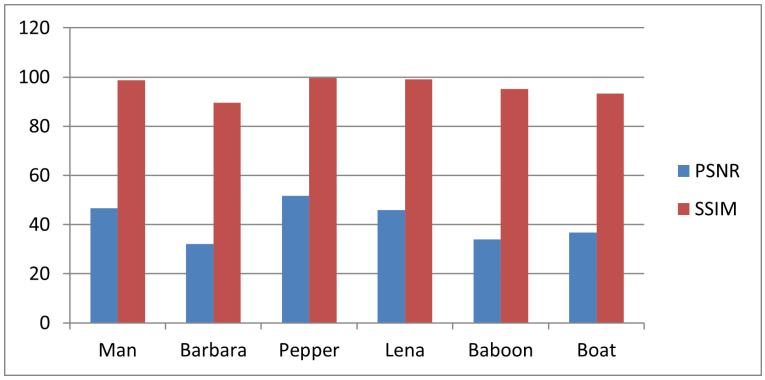


Figure 18. PSNR and SSIM of the different test images on 150 singular values.

5.9. Comparison Analysis

In the comparison analysis, PSNR with various compression ratios, entropies, and correlation coefficients are performed. Table 8 compares the proposed method's PSNR with other literature studies for the Lena image on 0.25 and 0.5 compression ratios. Tables 9 and 10 compare the proposed method's information entropy and correlation coefficient, respectively, with other literature studies for different test images.

Table 8. PSNR value comparisons with different literature studies for the Lena image on 0.25 and 0.5 compression ratios.

Algorithms	PSNR in dB (CR = 0.25)	Algorithms	PSNR in dB (CR = 0.5)
[34]	17.41	[34]	25.99
[35]	26.06	[35]	29.82
[36]	32.77	[36]	32.10
[40]	31.97	[41]	33.25
[42]	26.56	[40]	34.01
[43]	27.95	[42]	29.83
Proposed	51.31	[43]	32.27
		Proposed	55.27

Table 9. Information entropy comparison with different literature studies on different images.

Algorithms	Images			
	Cameraman	**Pepper**	**Baboon**	**Lena**
Proposed	7.9971	7.9993	7.9994	7.9974
[8]	7.9945	7.9949	7.9941	N/A
[36]	7.9965	7.9965	N/A	7.9960
[44]	N/A	7.9993	7.9993	N/A
[13]	N/A	7.998569	N/A	N/A
[25]	N/A	7.9889	7.9974	7.9995

Table 10. Correlation coefficient comparison with different literature studies on different images.

Algorithms	Images			
		H	**V**	**D**
Proposed	Lena	−0.0013	0.0020	0.0023
	Cameraman	0.0022	0.0007	−0.0020
	Pepper	−0.0021	0.0002	0.0001
	Baboon	−0.0025	0.0004	0.0004
[44]	Lena	0.0020	0.0002	0.0007
	Cameraman	0.0005	0.0036	0.0016
	Baboon	0.0027	0.0014	−0.0016
[45]	Lena	0.0069	−0.0028	0.0047
	Cameraman	−0.0044	0.0054	0.0025
	Pepper	0.0074	0.0035	0.0041
[36]	Lena	0.0064	0.0003	0.0026
	Cameraman	0.0040	0.0027	−0.0084
	Pepper	−0.0117	0.0039	0.001
[8]	Cameraman	0.0014	−0.0044	−0.0031
	Pepper	0.0033	−0.0016	−0.000058
[37]	Lena	0.0008	0.0019	0.0004
[25]	Lena	0.0008	0.0004	0.0020

6. Conclusions

We developed a novel method for image encryption, i.e., a 3D Gauss map from the 1D Gauss map. Further, the method is blended with the other three strong chaos maps as the logistic map, Arnold cat map, and sine map, which in integration makes a powerful quad key structure with a very large key and is very difficult to breach. To make the system lightweight (in terms of the processing speed), the SVD compression scheme is also employed. One major benefit of the proposed method is that it gives the user some flexibility in terms of compression, so that the user may tailor the amount of compression applied to the visual data to meet the needs of storage without sacrificing security.

The encryption strength of the suggested strategy was assessed using NPCR, UACI, entropy, and correlation coefficient studies, which were also compared with the state-of-the-art methods. In addition, the suggested approach was evaluated in terms of calculation time. This work can be expanded in the future to include video compression and video security.

According to the experimental results and security analysis, the suggested technique has an excellent encryption effect, high key sensitivity, strong pixel randomization, and poor correlation of neighboring pixels. Additionally, it is opposed to standard statistical and differential attacks. Compared to existing work, the suggested approach is highly secure and suitable for lightweight transmission.

Author Contributions: Conceptualization, S.S. and B.A.; methodology, S.S., A.K.S., M.F.H., B.A. and N.D.B.; software, S.S., M.F.H. and B.A.; validation, S.S., A.K.S., M.F.H., B.A. and N.D.B.; formal analysis, S.S., A.K.S. and B.A.; investigation, S.S.; resources, M.F.H. and N.D.B.; data curation, S.S. and B.A.; writing—original draft preparation, S.S., A.K.S., M.F.H., B.A. and N.D.B.; writing—review and editing, S.S., A.K.S., M.F.H., B.A. and N.D.B.; visualization, B.A. and N.D.B.; supervision, A.K.S., M.F.H. and N.D.B.; project administration, S.S. and M.F.H.; funding acquisition, M.F.H. and N.D.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available upon request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

1D	One-Dimensional
2D	Two-Dimensional
3D	Three-Dimensional
CC	Correlation Coefficient
CS	Compressive Sensing
DCST	Discrete Cosine Stockwell Transform
DNA	Deoxyribonucleic Acid
FFT	Fast Fourier Transform
FRFT	Fractional Fourier Transform
IE	Information Entropy
IEEE	Institute of Electrical and Electronics Engineers
JPEG	Joint Photographic Experts Group
LE	Lyapunov Exponent
LEC	Lyapunov Exponent Chart
MSE	Mean Square Error
NIST	National Institute of Standards and Technology
NPCR	Number of Changing Pixel Rate
PSNR	Peak Signal-to-Noise Ratio
QKCS	Quad Key Chaotic System
S-box	Substitution Box
SPN	Salt and Pepper Noise
SSIM	Structural Similarity Index Measure
SVD	Singular Value Decomposition
UACI	Unified Average Change Intensity

References

1. Mohamed, N.A.; El-Azeim, M.A.; Zaghloul, A.; Abd El-Latif, A.A. Image encryption scheme for secure digital images based on 3D cat map and turing machine. In Proceedings of the IEEE 7th International Conference of Soft Computing and Pattern Recognition (SoCPaR), Fukuoka, Japan, 13–15 November 2015; pp. 230–234.
2. Shao, W.; Cheng, M.; Luo, C.; Deng, L.; Zhang, M.; Fu, S.; Tang, M.; Liu, D. An image encryption scheme based on hybrid electro-optic chaotic sources and compressive sensing. *IEEE Access* **2019**, *7*, 156582–156591. [CrossRef]
3. Patro, K.A.K.; Acharya, B.; Nath, V. Secure, lossless, and noise-resistive image encryption using chaos, hyper-chaos, and DNA sequence operation. *IETE Tech. Rev.* **2020**, *37*, 223–245. [CrossRef]
4. Zhang, H.; Wang, X.q.; Sun, Y.j.; Wang, X.y. A novel method for lossless image compression and encryption based on LWT, SPIHT and cellular automata. *Signal Process. Image Commun.* **2020**, *84*, 115829. [CrossRef]
5. Khan, M.; Rasheed, A. Permutation-based special linear transforms with application in quantum image encryption algorithm. *Quantum Inf. Process.* **2019**, *18*, 298. [CrossRef]
6. Panna, B.; Kumar, S.; Jha, R.K. Image encryption based on block-wise fractional fourier transform with wavelet transform. *IETE Tech. Rev.* **2019**, *36*, 600–613. [CrossRef]
7. Zhang, M.; Tong, X.J.; Liu, J.; Wang, Z.; Liu, J.; Liu, B.; Ma, J. Image compression and encryption scheme based on compressive sensing and Fourier transform. *IEEE Access* **2020**, *8*, 40838–40849. [CrossRef]
8. Ghaffari, A. Image compression-encryption method based on two-dimensional sparse recovery and chaotic system. *Sci. Rep.* **2021**, *11*, 369. [CrossRef]
9. Chaudhary, P.; Gupta, R.; Singh, A.; Majumder, P.; Pandey, A. Joint image compression and encryption using a novel column-wise scanning and optimization algorithm. *Procedia Comput. Sci.* **2020**, *167*, 244–253. [CrossRef]
10. Wen, H.; Ma, L.; Liu, L.; Huang, Y.; Chen, Z.; Li, R.; Liu, Z.; Lin, W.; Wu, J.; Li, Y.; et al. High-quality restoration image encryption using DCT frequency-domain compression coding and chaos. *Sci. Rep.* **2022**, *12*, 16523. [CrossRef]
11. Li, X.Z.; Chen, W.W.; Wang, Y.Q. Quantum image compression-encryption scheme based on quantum discrete cosine transform. *Int. J. Theor. Phys.* **2018**, *57*, 2904–2919. [CrossRef]
12. Tang, Y.; Zhao, M.; Li, L. Secure and efficient image compression-encryption scheme using new chaotic structure and compressive sensing. *Secur. Commun. Netw.* **2020**, *2020*, 6665702. [CrossRef]
13. Zhu, Z.; Song, Y.; Zhang, W.; Yu, H.; Zhao, Y. A novel compressive sensing-based framework for image compression-encryption with S-box. *Multimed. Tools Appl.* **2020**, *79*, 25497–25533. [CrossRef]
14. Zhu, S.; Zhu, C. A new image compression-encryption scheme based on compressive sensing and cyclic shift. *Multimed. Tools Appl.* **2019**, *78*, 20855–20875. [CrossRef]
15. Ye, G.; Pan, C.; Huang, X.; Zhao, Z.; He, J. A chaotic image encryption algorithm based on information entropy. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850010. [CrossRef]
16. Wen, H.; Liu, Z.; Lai, H.; Zhang, C.; Liu, L.; Yang, J.; Lin, Y.; Li, Y.; Liao, Y.; Ma, L.; et al. Secure DNA-coding image optical communication using non-degenerate hyperchaos and dynamic secret-key. *Mathematics* **2022**, *10*, 3180. [CrossRef]
17. Vaish, A.; Kumar, M. Color image encryption using singular value decomposition in discrete cosine Stockwell transform domain. *Opt. Appl.* **2018**, *48*, 25–38.
18. Kumar, M.; Vaish, A. An efficient encryption-then-compression technique for encrypted images using SVD. *Digit. Signal Process.* **2017**, *60*, 81–89. [CrossRef]
19. Zhang, X. Multimedia Image Encryption Analysis Based on High-Dimensional Chaos Algorithm. *Adv. Multimed.* **2021**, *2021*, 7384170. [CrossRef]
20. Patel, S.; Bharath, K.; Kumar, R. Symmetric keys image encryption and decryption using 3D chaotic maps with DNA encoding technique. *Multimed. Tools Appl.* **2020**, *79*, 31739–31757. [CrossRef]
21. Darwish, S.M. A modified image selective encryption-compression technique based on 3D chaotic maps and arithmetic coding. *Multimed. Tools Appl.* **2019**, *78*, 19229–19252. [CrossRef]
22. Yu, C.; Li, H.; Wang, X. SVD-based image compression, encryption, and identity authentication algorithm on cloud. *IET Image Process.* **2019**, *13*, 2224–2232. [CrossRef]
23. Beneš, Š.; Kruis, J. Singular value decomposition used for compression of results from the finite element method. *Adv. Eng. Softw.* **2018**, *117*, 8–17. [CrossRef]
24. Zefreh, E.Z. An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions. *Multimed. Tools Appl.* **2020**, *79*, 24993–25022. [CrossRef]
25. Mondal, B.; Behera, P.K.; Gangopadhyay, S. A secure image encryption scheme based on a novel 2D sine–cosine cross-chaotic (SC3) map. *J. Real-Time Image Process.* **2021**, *18*, 1–18. [CrossRef]
26. Mishra, P.; Bhaya, C.; Pal, A.K.; Singh, A.K. A medical image cryptosystem using bit-level diffusion with DNA coding. *J. Ambient. Intell. Humaniz. Comput.* **2021**, 1–22. . [CrossRef]
27. Liu, L.; Du, C.; Zhang, X.; Li, J.; Shi, S. Dynamics and entropy analysis for a new 4-D hyperchaotic system with coexisting hidden attractors. *Entropy* **2019**, *21*, 287. [CrossRef]
28. Rustad, S.; Setiadi, D.R.I.M.; Syukur, A.; Andono, P.N. Inverted LSB image steganography using adaptive pattern to improve imperceptibility. *J. King Saud Univ.-Comput. Inf. Sci.* **2021**, *34*, 3559–3568. [CrossRef]

29. Gao, X.; Mou, J.; Banerjee, S.; Cao, Y.; Xiong, L.; Chen, X. An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 1535–1551. [CrossRef]
30. Abdullah, H.A.; Abdullah, H.N. FPGA implementation of color image encryption using a new chaotic map. *Indones. J. Electr. Eng. Comput. Sci.* **2019**, *13*, 129–137. [CrossRef]
31. Açikkapi, M.Ş.; Özkaynak, F. A method to determine the most suitable initial conditions of chaotic map in statistical randomness applications. *IEEE Access* **2020**, *9*, 1482–1494. [CrossRef]
32. Ahuja, B.; Doriya, R. A novel hybrid compressive encryption cryptosystem based on block quarter compression via DCT and fractional Fourier transform with chaos. *Int. J. Inf. Technol.* **2021**, *13*, 1837–1846. [CrossRef]
33. Zhu, S.; Zhu, C.; Wang, W. A novel image compression-encryption scheme based on chaos and compression sensing. *IEEE Access* **2018**, *6*, 67095–67107. [CrossRef]
34. Zhou, N.; Pan, S.; Cheng, S.; Zhou, Z. Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing. *Opt. Laser Technol.* **2016**, *82*, 121–133. [CrossRef]
35. Chai, X.; Zheng, X.; Gan, Z.; Han, D.; Chen, Y. An image encryption algorithm based on chaotic system and compressive sensing. *Signal Process.* **2018**, *148*, 124–144. [CrossRef]
36. Xu, Q.; Sun, K.; He, S.; Zhu, C. An effective image encryption algorithm based on compressive sensing and 2D-SLIM. *Opt. Lasers Eng.* **2020**, *134*, 106178. [CrossRef]
37. Huang, W.; Jiang, D.; An, Y.; Liu, L.; Wang, X. A novel double-image encryption algorithm based on Rossler hyperchaotic system and compressive sensing. *IEEE Access* **2021**, *9*, 41704–41716. [CrossRef]
38. Sayed, W.S.; Radwan, A.G.; Fahmy, H.A.; Elsedeek, A. Trajectory control and image encryption using affine transformation of lorenz system. *Egypt. Inform. J.* **2021**, *22*, 155–166. [CrossRef]
39. Asl, A.M.; Broumandnia, A.; Mirabedini, S.J. Scale invariant digital color image encryption using a 3D modular chaotic map. *IEEE Access* **2021**, *9*, 102433–102449.
40. Ren, H.; Niu, S.; Chen, J.; Li, M.; Yue, Z. A Visually Secure Image Encryption Based on the Fractional Lorenz System and Compressive Sensing. *Fractal Fract.* **2022**, *6*, 302. [CrossRef]
41. Xie, Y.; Yu, J.; Guo, S.; Ding, Q.; Wang, E. Image encryption scheme with compressed sensing based on new three-dimensional chaotic system. *Entropy* **2019**, *21*, 819. [CrossRef]
42. Chai, X.; Wu, H.; Gan, Z.; Zhang, Y.; Chen, Y.; Nixon, K.W. An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding. *Opt. Lasers Eng.* **2020**, *124*, 105837. [CrossRef]
43. Zhu, L.; Song, H.; Zhang, X.; Yan, M.; Zhang, T.; Wang, X.; Xu, J. A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding. *Signal Process.* **2020**, *175*, 107629. [CrossRef]
44. Cun, Q.; Tong, X.; Wang, Z.; Zhang, M. Selective image encryption method based on dynamic DNA coding and new chaotic map. *Optik* **2021**, *243*, 167286. [CrossRef]
45. Luo, Y.; Lin, J.; Liu, J.; Wei, D.; Cao, L.; Zhou, R.; Cao, Y.; Ding, X. A robust image encryption algorithm based on Chua's circuit and compressive sensing. *Signal Process.* **2019**, *161*, 227–247. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.