Integrating Quadratic Polynomial and Symbolic Chaotic Map-based Feistel Network to Improve Image Encryption Performance

by Kristiawan Nugroho

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Integrating Quadratic Polynomial and Symbolic Chaotic Map-based Feistel Network to Improve Image Encryption Performance

Edy Winarno*, Wiwien Hadikurniawati, Kristiawan Nugroho, Veronica Lusiana
Faculty of Information Technology and Industry, Universitas Stikubank, Semarang, Central Java, Indonesia

Corresponding author: Edy Winarno (edywin@edu.unisbank.ac.id).

ABSTRACT This research introduces an innovative image encryption method that amalgamates two secure and efficient chaotic maps, namely a 2D Simplified Quadratic Polynomial Map (2D-SQPM) and a 2D Symbolic Chaotic Map (2D-SCM), within an enhanced Feistel network structure. The primary motivation for this research is to address the limitations of current image encryption methods that are vulnerable to statistical and differential attacks. A hash function is also integrated to elevate the key's security and sensitivity. Unlike standard Feistel networks, which split the plaintext into two parts and employ only XOR operations at the bit level, this research's Feistel Network modification involves dividing the plaintext into four sections and introducing a diverse set of operations, including substitution and permutation at both the bit and byte levels across different parts, thereby optimizing confusion and diffusion effects. The empirical evaluation demonstrates that this method significantly reduces pixel correlation and strengthens encryption against statistical and differential attacks. Supported by various analytical tools like entropy analysis, NPCR, UACI, chi-square, key space and sensitivity analysis, robustness testing, and NIST suite evaluations, the proposed method significantly enhances image encryption performance. In conclusion, the proposed method effectively secures image data and sets a new benchmark in image encryption. The significance of this research lies in its integration of complex, chaotic dynamics and advanced encryption mechanisms, providing a substantial contribution to digital information security.

INDEX TERMS Image Encryption, Feistel Network, Chaotic Encryption, Image Cryptosystem, Cryptography

I. INTRODUCTION

Security in transmitting digital data is a crucial aspect in today's era of internet technology. With increasing human work requiring this technology[1], cybercrime rates have also risen [2]–[7]. According to data from CrowdStrike 2024 Global Threat Report, there has been a significant increase in cyber-attacks, with a 75% rise reported[8]. Cryptography has become one of the methods for securing digital transactions, but this method must continuously evolve due to the increasing sophistication of cryptanalysis. The advancement of cryptography is inherently influenced by cryptanalysis research such as [9]–[12], which exposes potential vulnerabilities and drives the development of more secure encryption techniques. This race has spurred the need for more secure and efficient encryption methods[13], [14]. Specifically, this research focuses on image objects. Images require a special cryptographic approach that considers their intrinsic characteristics, such as high redundancy, large file sizes, and a high correlation between pixels[15], [16], making the research on image encryption particularly compelling for further development.

Shannon's theory on communication security emphasizes the importance of diffusion and confusion. In the context of image cryptography, this theory guides our approach, suggesting that permutations and substitutions must be carried out not only at the pixel level but also at the bit level to enhance security[17], [18]. This theory remains valid to this day, with ongoing research efforts to improve it[19]–[22]. Building on this foundation, complex permutation techniques with unpredictable patterns can be implemented to increase diffusion. Moreover, confusion can be enhanced by creating key-sensitive substitution functions, such as dynamic substitutions whose parameterizations change based on several aspects of the image being encrypted or by using more than one substitution function simultaneously. In addition to these techniques, mage encryption can also be substituted at both pixel and bit levels. Thus, a balanced combination of these two techniques at the bit and pixel levels can enhance the security of image cryptography[23], [24].

One crucial factor influencing the quality of diffusion and confusion is the key and the method. With recent advancements, researchers have developed many image encryption methods using various approaches, such as those based on chaos[25]–[31], DNA encoding [32], [33], neural networks [34], [35], etc. Interestingly, combining these methods results in high security but inevitably impacts computational complexity and efficiency. Particularly, most of these methods still combine them with chaotic-based methods. Because of their benefits, chaotic methods are preferred and used in image encryption due to their dynamic nature, sensitivity to parameters and initial conditions, and unpredictable patterns[36]–[40]. Consequently, the output of chaotic methods generally takes the form of a keystream commonly referred to as a chaotic sequence[41]. The chaotic sequence is used to carry out the permutation and substitution processes by leveraging this characteristic. Some simple chaotic methods are Arnold, Logistic, Baker, and Tent maps; these methods are relatively simple and have fast computations to generate chaotic sequences. Further encryption methods are being developed with higher dynamic complexity, such as in research[42]–[44], which is widely used today.

In the context of optimizing chaotic methods, various studies have involved and analyzed various chaotic systems. However, it is uncommon to find chaotic system methods that display simple chaotic behavior with a narrow chaotic range, lack of complex dynamic behavior, and uneven trajectory distribution. This limitation can significantly reduce the security of image encryption applications. On the other hand, it is also not uncommon to find chaotic systems with complex structures unsuitable for image encryption applications [45]–[48]. Furthermore, some image encryption methods are overly complex, which can limit their development to meet the needs of practical applications, or some algorithms may not be relevant to the plaintext or are designed too simplistically[49], [50].

This recognition necessitates an exploration of more sophisticated chaotic properties, such as those found in the 2D symbolic chaotic map (2D-SCM), which exhibits ergodicity, unpredictability, diversity, complexity, aperiodicity, and sensitivity to control factors and initial states. Contrastingly, the 2D simplified quadratic polynomial map (2D-SQPM) is an efficiently and securely designed chaotic algorithm. Integrating these insights, utilizing a hash function and the Feistel network, we combine both chaotic maps and apply the permutation and substitution techniques at the image pixel and bit levels. Furthermore, this study has several contributions and goals, namely:

1. To design an efficient and secure encryption method using a combination of 2D-SQPM and 2D-SCM.
2. To modify and implement the Feistel network, substitution operations, and permutations at the bit and pixel levels to enhance the confusion and diffusion of encryption.
3. A hash function increases resistance to statistical and differential attacks and enlarges the keyspace.

The rest of the manuscript is structured into four parts: Section 2, which includes preliminary discussions of related theoretical reviews and research inspiration to redesign and improve the method. Section 3 elaborates on the step-by-step process and illustrates the proposed method. Section 4 serves the dataset, testing results, comparison, analytical insights, and discussion. Lastly, Section 5 summarizes the objectives, results, and analysis in a titled Conclusion.

II. PRELIMINARIES

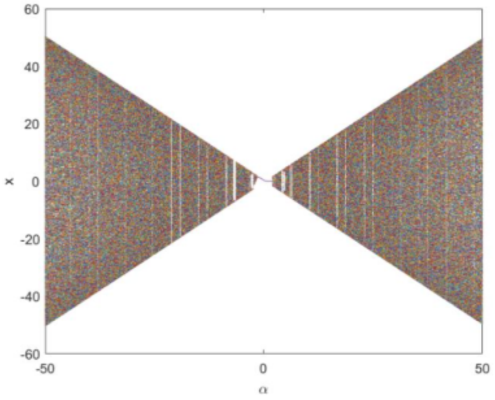
A. TWO-DIMENSIONAL SYMBOLIC CHAOTIC MAP (2D-SCM)

The 2D-SCM method was proposed by [26] as a novel approach to image encryption that leverages hyper-chaotic maps to enhance security and efficiency. Its advantages over previous methods include increased ergodicity, more complex behavior, and a significant chaotic range. The 2D-SCM is built upon a one-dimensional symbolic map, utilized as the seed to produce a two-dimensional chaotic sequence. The one-dimensional symbolic map is defined by Equation (1). However, this map is not optimal because if the control factor α is not appropriate, it will result in a zero value in the iteration, causing subsequent iterations to fail. Therefore, the map is modified from $\frac{x_n}{|x_n|}$ to $\frac{x_n}{e^{|x_n|}}$, and then expanded into two dimensions according to Equation (2).

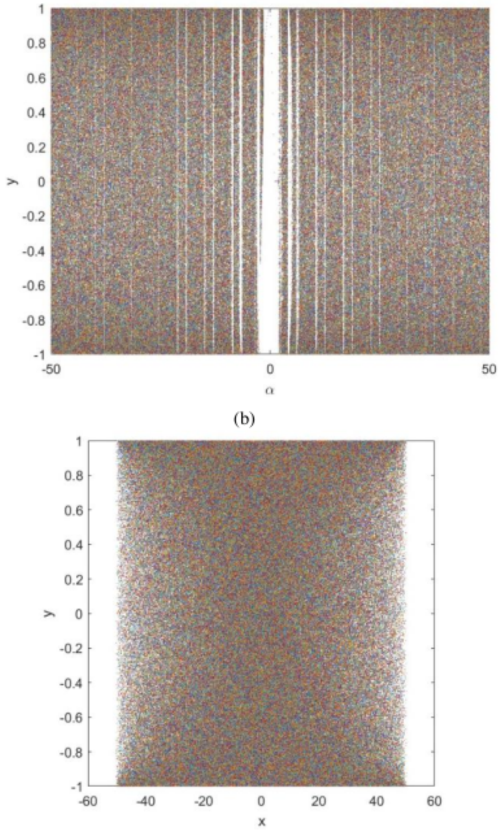
$$x_{n+1} = -\alpha x_n + \frac{x_n}{|x_n|} \quad (1)$$

$$\begin{cases} x_{n+1} = -\alpha y_n + \dfrac{y_n}{e^{|y_n|}} \\ y_{n+1} = \sin(x_n + y_n) \end{cases} \quad (2)$$

where $\alpha \in (1, 2)$ and after being developed into 2D-SCM, the range of α becomes $[-50,50]$. The behavior of the 2D-SCM is depicted in the bifurcation diagram and chaotic attractor in Figure 1.



(a)



(b)

(c)

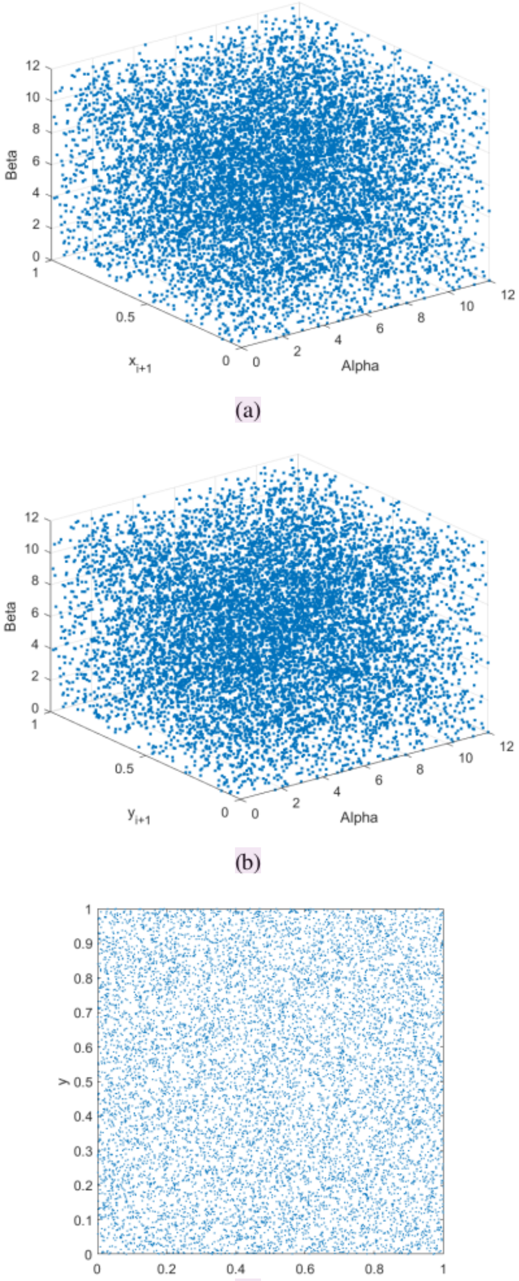
FIGURE 1. **2D-SCM (a) Bifurcation Diagram Plot to x; (b) Bifurcation Diagram Plot to y; (c) Chaotic Attractor**

B. TWO-DIMENSIONAL SIMPLIFIED QUADRATIC POLYNOMIAL MAP (2D-SQPM)

The 2D-SQPM is designed by[27] to overcome shortcomings in practicality, security, and efficiency found in chaotic maps and image encryption algorithms. This method was selected for its straightforward structure, which facilitates its application. The construction of the 2D-SQPM begins with the formation of a simple quadratic polynomial map, drawing inspiration from logistic and tent maps, with the addition of a modulus operation and giving an exponential form to one of the parameters to accelerate the divergence of trajectories, thereby enhancing chaotic performance. Equation (3) presents how to calculate the 2D-SQPM, while the bifurcation plot and its attractor are shown in Figure 2.

$$\begin{cases} x_{n+1} = \left(\alpha x_i^2 + 10^{\beta} y_i\right)\text{mod}1 \\ y_{n+1} = \left(\alpha y_i^2 + 10^{\beta} x_i\right)\text{mod}1 \end{cases} \quad (3)$$

where α and β are control parameters, x and y are seeds, while x_{n+1} and y_{n+1} represent the output values for the next iteration, calculated based on the previous values (x_i and y_i), which act as 'seeds' or initial values. This map is considered 'hyperchaotic', meaning it possesses highly complex dynamics and is sensitive to initial conditions, making it ideal for applications like encryption, where chaos and unpredictability are valuable assets. The 2D-SQPM behavior diagram illustrates the bifurcation behavior, and the chaotic attractor is shown in Figure 2.



(a)

(b)

(c)

FIGURE 2. **2D-SQPM (a) Bifurcation Diagram Plot to x; (b) Bifurcation Diagram Plot to y (c) Chaotic Attractor**

C. FEISTEL NETWORK AND ITS MODIFICATION

Feistel Network, often called Feistel cipher, works by dividing a plaintext block into two equal parts (R_0 and L_0). During encryption, only one part of the data is processed at a time, while the others remain unchanged[51]. This process involves an encryption function and several sub-keys generated from the master key. Each step of this process, known as round $i = 0,1,\ldots,n$, consists of steps illustrated by Equation (4). After several rounds, the two parts are combined again to form an encrypted data block.

$$\begin{aligned} L_{i+1} &= R_i, \\ R_{i+1} &= L_i \oplus F(R_i, K_i) \end{aligned} \tag{4}$$

where $F(R_i, K_i)$ equal $R_i \oplus K_i$

Feistel Network has several advantages and is widely used in symmetric cryptographic algorithms. One of its advantages is its encryption structure that offers strong security through complex nonlinear operations, making it resistant to cryptographic analysis[51], [52]. Advantages include flexibility in using different encryption functions per round for enhanced security, efficiency through similar encryption and decryption processes that facilitate easy implementation, and a modular design that facilitates algorithm analysis and development.

Inspired by research [23] and the Substitution-Permutation Network (SPN) in AES, the Feistel Network is modified by combining cross operations, permutation, and substitution techniques so that encryption operations occur at the bit and pixel level. First, the plaintext is converted into a vector, then divided into four equal parts (A, B, C, D), then the operation is carried out in i rounds with a transformation function that depends on the keystream or chaotic sequence. Equation (5) is used as an illustration of the proposed Feistel Network. After the Feistel Network modification is carried out, all parts are combined again.

$$\begin{aligned} A_{i+1} &= \text{permute}\big(C_i, \text{sort}(x_{\text{seq}})\big), \\ C_{i+1} &= A_i \oplus F\big(C_i, K_{x_i}\big), \\ B_{i+1} &= \text{permute}\left(D_i, \text{sort}\big(y_{\text{seq}}\big)\right), \\ D_{i+1} &= G(B_i, K_{y_i}) \end{aligned} \tag{5}$$

where $F\big(C_i, K_{x_i}\big) = \text{permute}\big(C_i, \text{sort}(x_{\text{seq}})\big) \oplus K_{x_i}$, $G\big(B_i, K_{x_i}\big) = \big(B_i + K_{x_i}\big)\text{mod } K_{x_i}$, $K_{x_i} = \text{mod}(x_{\text{seq}} \times 10^5, 256)$, $K_{y_i} = \text{mod}(y_{\text{seq}} \times 10^5, 256)$, x_{seq} and y_{seq} are a chaotic sequence from a two-dimensional transform.

Next, the decryption stage of the proposed Feistel Network modification is illustrated in Equation (6). These modifications make Feistel operations even more robust and secure.

$$\begin{aligned} B_{i+1} &= \text{mod}\big(D_{i+1} - K_{y_i} + 256{,}256\big), \\ D_i &= \text{depermute}(B_{i+1}, \text{sort}(y_{\text{seq}})), \\ A_{i+1} &= C_i \oplus \big(A_i \oplus K_{x_i}\big), \\ C_i &= \text{depermute}\big(A_{i+1}, \text{sort}(x_{\text{seq}})\big) \end{aligned} \tag{6}$$

III. PROPOSED METHOD

In this section, the proposed encryption method is explained. This method generally consists of two two-dimensional chaotic maps combined with a Feistel Network basis. Substitution and permutation operations are carried out at the pixel and bit level. At the same time, the SHA-512 hash function is also added to increase keyspace and the system's sensitivity to small (1-bit) changes in both key and plaintext. Minor changes will produce different hash values, making the method more resistant to chosen-plaintext, chosen-ciphertext, and differential attacks [53]–[56]. Using a hash function also converts various input keys into fixed lengths, making key processing easier[18], [57]. As an illustration of the proposed method, you can see Figure 3.

While the detailed stages of the proposed method are as follows:

1. Reading the plain text, in this instance, the image (I), as the input for SHA-512, yields a hexadecimal hash value, which serves as $key1$.
2. Convert the image to a one-dimensional array, which is referred to as I'.
3. Gathering the user's password for SHA-512 input produces a hexadecimal hash value denoted as $key2$.
4. Covert 128 hexadecimal format to 64 ASCII numbers, then combine key1 and key2 to form key, using the modulus operation with Equation (7), ensuring the key consists of 64 ASCII numbers.
$$key = \text{mod}((key1 + key2), 256) \tag{7}$$
5. Calculate initial parameters from the 64 ASCII numbers for 2D-SCM, namely $x1_0$ and $y1_0$, and for 2D-SQPM, namely $x2_0$ and $y2_0$, using Equation (8).
$$\begin{aligned} x1_0 &= \sigma(key[1{:}16]), \\ y1_0 &= \sigma(hash[17{:}32]), \\ x2_0 &= \sigma(hash[33{:}48]), \\ y2_0 &= \sigma(hash[49{:}64]) \end{aligned} \tag{8}$$
where σ is the standard deviation.
6. Produce a chaotic sequence by iterating eight times the number of pixels (n) utilizing 2D-SCM in Equation (2), where $x1_0$ and $y1_0$ serves as the initial state, and $\alpha = 1.99$ is a constant control factor.
7. Arrange the initial chaotic sequence $(x1_i[1{:}n])$ in ascending order and store the resulting sorted index $(idx1)$. Afterward, permute pixels of I' according to $idx1$, to obtain the permuted I'.
8. Covert permuted I' to binary form, then reshape to a 1D array. On the other side, sort the second sequence $(y1_i[1{:}8n])$ in ascending order and save the sorted index $(idx2)$, the permute bits of I' based on $idx2$, so get final permuted I'.
9. Covert back the final permuted I' in pixel form.
10. Generate a chaotic sequence with the number of iterations being eight times the number of pixels (n) utilizing 2D-SQPM in Equation (3), where $x2_0$ and $y2_0$ serves as the initial state, and $\alpha = 0.6$ and $\beta = 0.1$ are constant control factors. In this stage, we can get x_{seq} and y_{seq}.

11. Split I' into four equal parts (A, B, C, D) and use x_{seq} and y_{seq} for Feistel network input.
12. Perform Feistel network operation base on Equation (5) in eight rounds $(r = 8)$, where each of round will use 1/8 segment of the keystream $x_{seq}[(i-1)*n+1 : i*n]$
13. After completing all the rounds of the Feistel Network, concatenate all parts (A, B, C, D) to obtain an encrypted 1D array.
14. Reshape the encrypted 1D array according to the dimensions of the plain image to form the encrypted image (E).

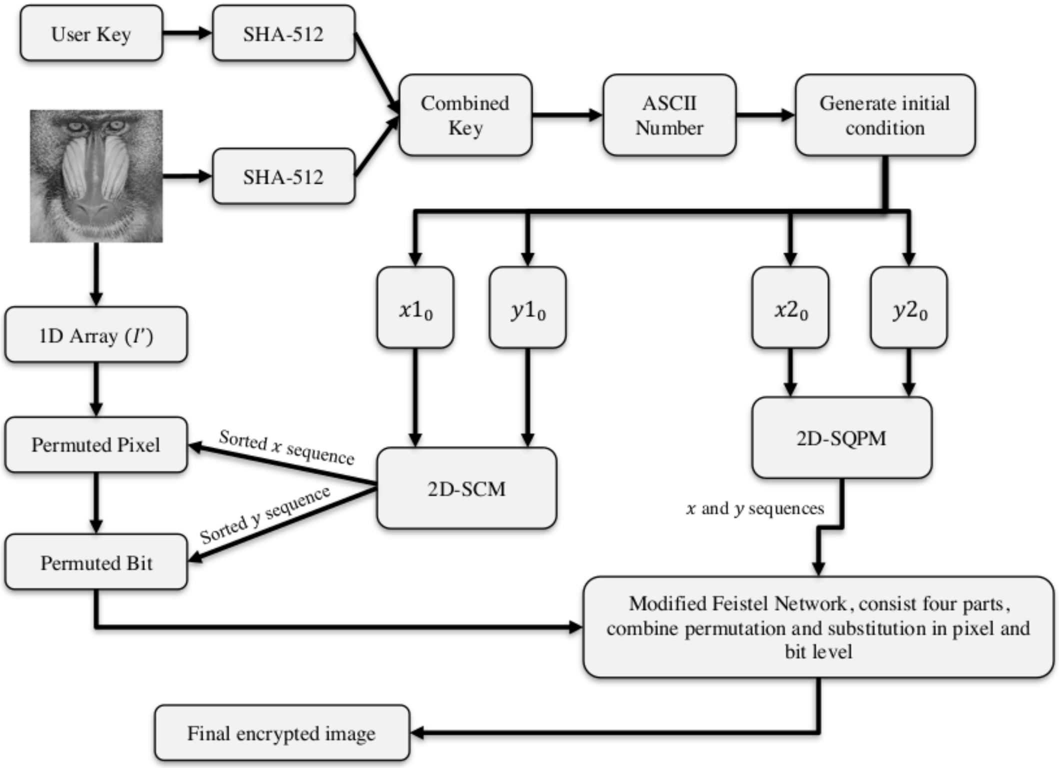


FIGURE 3. **Proposed Encryption Flow**

IV. RESULTS AND ANALYSIS

In this section, we present the results of our research and conduct a comprehensive analysis of the findings. The results highlight the effectiveness and performance of the proposed Modified Feistel Network-based 2D-SCM and 2D-SQPM combination, its impact on encryption quality, and resistance to various cryptographic attacks, and compare it with related research. First, we would like to explain the software and hardware used in the research, namely Matlab 2021a as IDE tools, while the processor is i7-1165G7 @ 2.80GHz with 16GB memory. Standard images are used in this research to make it easy to compare with previous research. All images have dimensions of 512×512. For larger or smaller images, we preprocess them with the imresize function in Matlab; several standard images are presented in Figure 4.

Next, in Figure 5, a sample of the encryption results at each stage of the proposed method is presented, and the respective histograms are presented. An image histogram is a graphical representation that shows the distribution of pixel intensity, this is an indicator of the quality of image encryption[58]. Visually, in Fig. 5(b), the image begins to be scrambled. It has no meaning, but because only the original image histogram pixel permutation process is carried out and the permutation results are still the same, see Fig. 5(e). After the bit permutation is carried out (Fig. 5(c)), the image is more scrambled and indirectly experiences changes in pixel values. It also looks like a change in contrast when compared to Fig. 5(b). This is also proven by the histogram changes in Fig. 5(e). The distribution starts out uniform. In the final stage of encryption, after going through eight rounds of the modified Feistel Network, the histogram changes appear more uniform. At the decryption stage, the proposed method can also work perfectly to carry out decryption, see Figure 6. These results show that the proposed cryptographic method was successfully carried out, but further analysis must be conducted. These measurements are discussed in more detail in Section 4.A to 4.I.

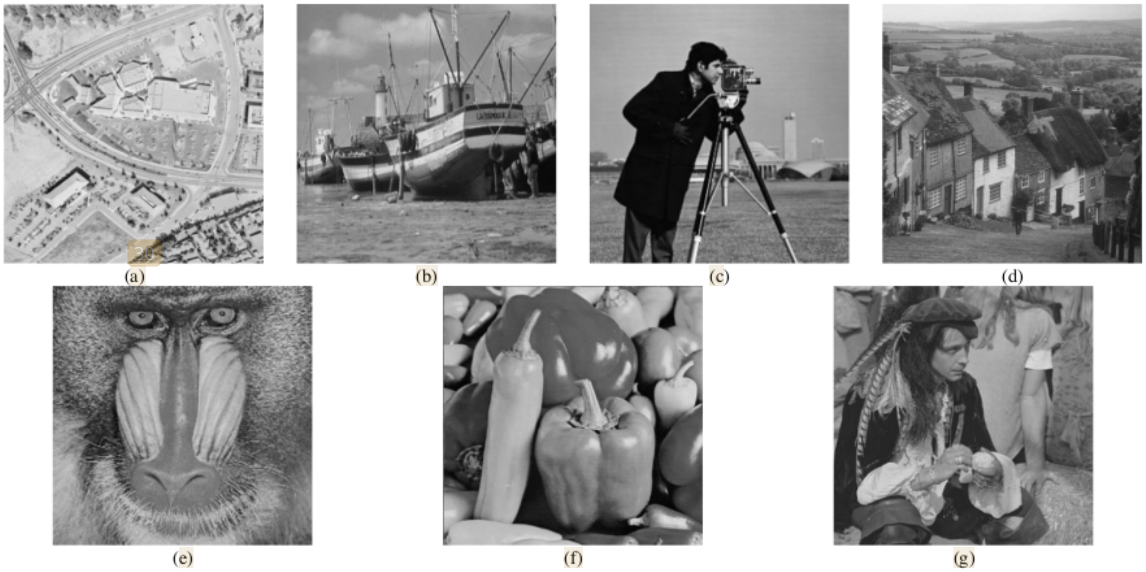


FIGURE 4. Image Dataset {(a)Aerial; (b) Boat; (c) Cameraman; (d) Gold Hill (e) Mandril; (f) Peppers; (g)Pirate}

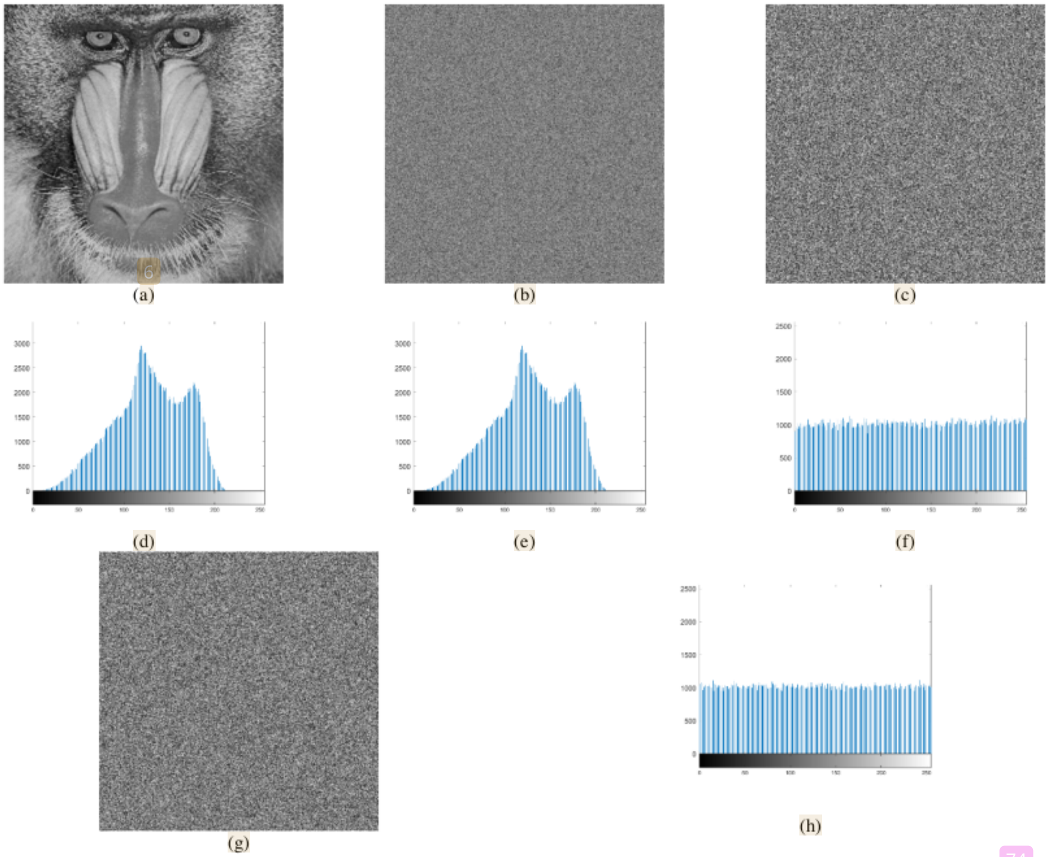


FIGURE 5. Sample Encryption Results {(a) Original image; (b) Encryption after pixel permutation; (c) Encryption after bit permutation (d) Original Image Histogram; (e) Histogram after pixel permutation; (f) Histogram after bit permutation; (g) Final Encrypted Image; (h) Final Encrypted Histogram}

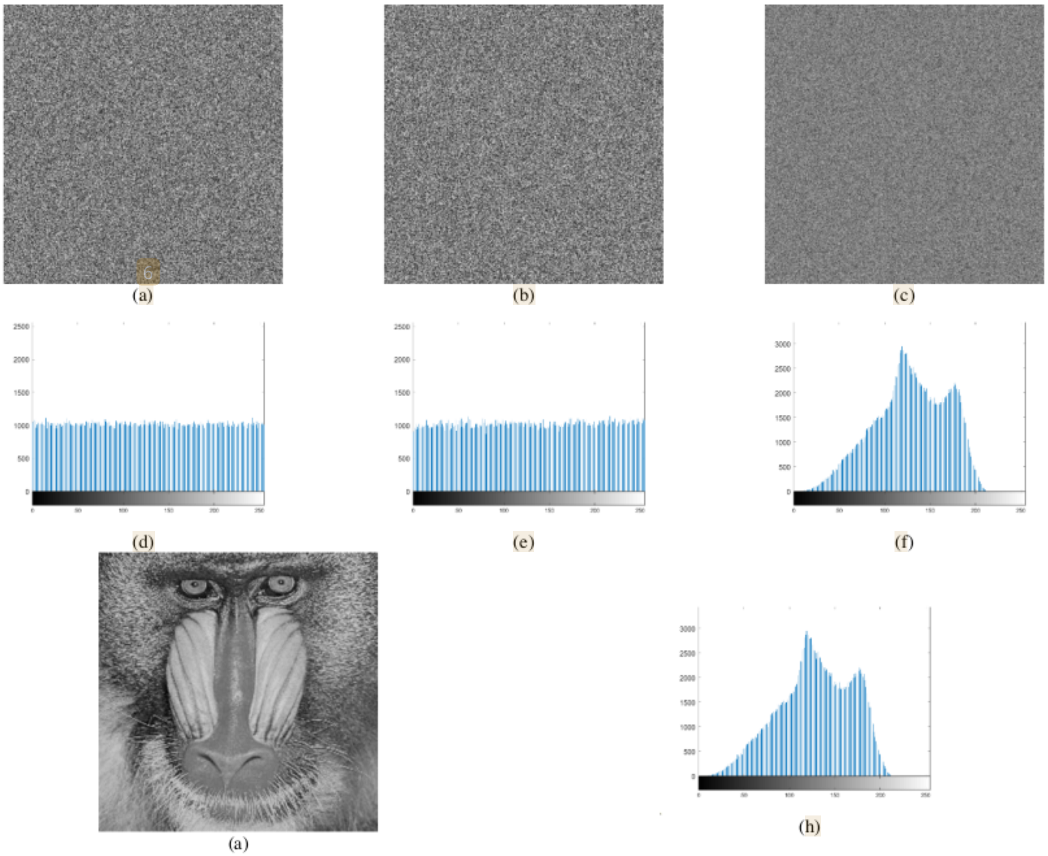


FIGURE 6. Sample Decryption Results {(a) Encrypted image; (b) decryption after inverse proposed Feistel Network; (c) Decryption after bit inverse permutation (d) Encrypted Image Histogram; (e) Histogram after inverse proposed Feistel Network; (f) Histogram after bit inverse permutation; (g) Final Decrypted Image; (h) Final Decrypted Histogram}

A. INFORMATION ENTROPY ANALYSIS

Good encryption aims to render the encrypted image resilient against statistical attacks. This resilience entails ensuring that the distribution of pixel values in the encrypted image is uniform or nearly uniform, thereby complicating attackers' attempts to deduce information about the original image. Entropy serves as a metric for assessing the randomness of pixel value distributions. A high entropy value indicates a uniform and random distribution of pixel values, signifying robust encryption that thwarts statistical analysis. In the 8-bit grayscale images, a higher entropy value approaches the maximum value of eight[59]. The maximum entropy value is derived from the logarithm base 2 of 2^8, which equals eight. Further calculation of the entropy formula can be executed using Equation (9).

$$H = \sum_{i=1}^{n} p(s_i) log_2 \left(\frac{1}{p(s_i)}\right) \tag{9}$$

TABLE I
MEASUREMENTS RESULTS OF INFORMATION ENTROPY AND COMPARISON WITH PRIOR STUDIES

Image	Method[26]	Method[28]	Method[30]	Method[31]	Method [33]	Proposed
Aerial	-	-	-	7.9989	-	7.9993
Boat	-	-	-	7.9971	-	7.9993
Cameraman	-	-	-	7.9972	-	7.9994
Goldhill	-	-	-	-	-	7.9993
Mandril	7.9992	7.9993	7.9977	7.9993		7.9994
Peppers	-	7.9994	-	7.9992	7.9946	7.9994
Pirate	7.9993	-	-	-	-	7.9993
Average	7.99925	7.99935	7.99770	7.99834	7.99460	7.99934

The presented results in Table 4 indicate that the entropy measurements, where n represents the total number of symbols, s_i denotes the information source, and $p(s_i)$ represents the probability of occurrence of the source s, which is consistently close to eight. This proximity suggests that the encryption quality is excellent, as assessed by entropy. Moreover, Table 1 demonstrates that the proposed encryption method outperforms previous approaches. Specifically, the table illustrates that the proposed method achieves a higher entropy value than various prior methods, indicating a notable level of randomness and resilience against statistical attacks.

B. DIFFERENTIAL ANALYSIS

Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are two commonly used metrics to assess the performance of image encryption, particularly against differential attacks [24]. NPCR evaluates the sensitivity of encryption to minor changes by measuring the percentage of pixels that differ between two encrypted images with minimal discrepancies from the original image. The optimal value of NPCR is around 99.6094% for grayscale images [53], [60], [61]. Deviations from this ideal value suggest varying degrees of encryption sensitivity. Conversely, excessively high NPCR values may not significantly enhance security and introduce unnecessary variability.

UACI measures the average intensity change between two encrypted images, reflecting the extent of intensity alteration induced by encryption. The ideal UACI value is approximately 33.4635% for grayscale images[53], [60], [61]. Deviations from this ideal value may indicate weaknesses in the encryption process. Extremely high UACI values may suggest excessive intensity changes, potentially revealing exploitable patterns. The calculation formulas for NPCR and UACI entail pixel-by-pixel comparisons between two encrypted images $(E1, E2)$ to determine the percentage of pixel changes and the disparity in their average intensities. Equations (10) and (11) are employed for computing NPCR and UACI.

$$NPCR = \left[\frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} Diff(i,j)\right] \times 100\%, \qquad (10)$$

$$Diff(i,j)\begin{cases} 0 \ if \ E1(i,j) = E2(i,j) \\ 1 \ if \ E1(i,j) \neq E2(i,j) \end{cases}$$

$$UACI = \left[\frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|E1(i,j) - E2(i,j)|}{255}\right] \times 100\% \qquad (11)$$

where M and N represent image dimension, $E1$ and $E2$ must have the same dimension, i and j denote pixel coordinate. It is important to note that $E2$ has minor differences from $E1$; The difference lies in one bit of plaintext before encryption. That is, to create $E2$, we change one random bit in the light text image corresponding to $E1$, while all other bits remain the same. This process guarantees that the difference between $E1$ and $E2$ is minimal and limited to just one bit, allowing for accurate analysis of the encryption system's resistance to differential attacks. Table 2 shows the NPCR calculation results and comparisons, while Table 3 shows the UACI values.

TABLE II
MEASUREMENTS RESULTS OF NPCR AND COMPARISON WITH PRIOR STUDIES

Image	Method[27]	Method[31]	Method[33]	Proposed
Aerial	99.6151	99.6082	-	99.6132
Boat	99.6189	99.6080	-	99.5989
Cameraman	-	99.6201	-	99.6181
Goldhill	99.6051	-	-	99.5852
Mandril	-	99.5667	-	99.6141
Peppers	-	99.6403	99.6492	99.6160
Pirate	-	-		99.6121

TABLE III
MEASUREMENTS RESULTS OF UACI AND COMPARISON WITH PRIOR STUDIES

Image	Method[27]	Method[31]	Method[33]	Proposed
Aerial	33.4867	33.3858	-	33.4592
Boat	33.4503	33.4643	-	33.4630
Cameraman	-	33.4591	-	33.4738
Goldhill	33.4568	-	-	33.4577
Mandril	-	33.5354	-	33.4835
Peppers	-	33.5468	33.3356	33.4801
Pirate	-	-	-	33.4732

According to Table 2, the proposed method shows NPCR results close to ideal values, indicating high sensitivity to pixel changes, which indicates strong image encryption in terms of security against differential attacks. The UACI for the proposed method is consistently within ideal values (see Table 3), showing good intensity changes without being excessive. Compared with previous work, the proposed method shows slight improvements in most of the results, although it is not entirely superior, and some are not better. But overall, this method is relatively slightly better.

C. CHI-SQUARE ANALYSIS

The chi-square (X^2) measurement function in the context of grayscale image encryption is used to evaluate the uniform distribution of encrypted image pixel values, which is important for assessing security against statistical attacks. Chi-square tests whether there is a significant difference between the observed distribution of pixel values in an encrypted image and the expected distribution if the image were completely uniform or random. The chi-square value calculated from the encrypted image $(X^2_{\alpha,df})$ must be less than or equal to 293.2478, with an alpha level (α) of 0.05 and degrees of freedom (df) of 255, then the distribution of image pixel values can be confirmed as uniform. Equation (12) is used to evaluate this research's chi-square value.

$$X^2 = \sum_{i=1}^{256}\frac{(P_i - E_i)^2}{E_i} \qquad (12)$$

where $E_i = P/256$ is the expected frequency for each pixel value if the distribution is uniform. We use 256 for 8-bit grayscale images because there are 256 possible pixel intensities; P_i is the observed frequency for the i^{th} pixel value; i is an index, which ranges from 1 to 256 because, in Matlab, its indexing starts at 1. Table 4 displays the outcomes of the chi-square evaluations for the suggested approach and contrasts these with earlier studies.

TABLE IV
MEASUREMENTS RESULTS OF CHI-SQUARE AND COMPARISON WITH PRIOR STUDIES

Image	Method[26]	Method[28]	Proposed
Aerial	-	-	257.7322
Boat	-	-	214.8063
Cameraman	-	-	221.3281
Goldhill	-	-	267.8222
Mandril	249.974	284.3348	248.8271
Peppers	237.615	259.1784	229.6903
Pirate	206.254	-	232.5359
Average	231.2810	271.7566	238.9632

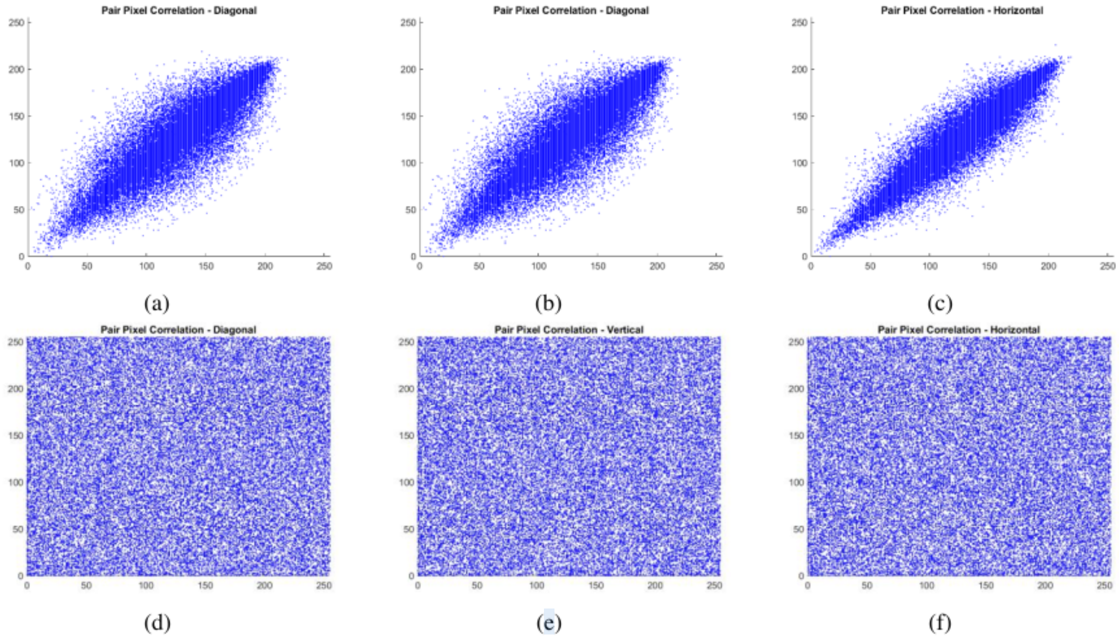
The chi-square values for the proposed method have all passed and been proven uniform. Even though the average value is not the best, this average value is calculated from all images. The images of Mandril and Peppers are especially superior. Overall, these results conclude that the proposed method is proven effective in generating a uniform distribution of post-encryption pixels.

D. CORRELATION COEFFICIENT OF ADJACENT PIXEL ANALYSIS

The correlation coefficient (r) measurement function evaluates the effectiveness of image encryption in reducing the correlation between adjacent pixels. High correlation between adjacent pixels is common in natural images, making it easier for attackers to conduct statistical attacks. Effective encryption aims to diminish this correlation, thereby impeding statistical analysis by attackers [31]. Typically, the correlation coefficient is computed for pixel pairs adjacent horizontally, vertically, and diagonally. The values range from -1 to 1, where 0 signifies no correlation, 1 denotes perfect positive correlation, and -1 indicates perfect negative correlation. In encrypted images, an ideal r value approaches 0, indicating a negligible correlation between pixels and affirming the effectiveness of encryption. Equation (13) is utilized to evaluate the r value.

$$r_{x,y} = \frac{\frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)]}{\sqrt{\frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2}\sqrt{\frac{1}{N}\sum_{i=1}^{N}[y_i - E(y)]^2}} \quad (13)$$

where $E(x)$ and $E(y)$ represent the average pixel intensity value for all pairs of pixels analyzed in each x and y direction; x_i and y_i are the intensity values for the ith pair of adjacent pixels in the image; N denotes the total number of adjacent pixel pairs analyzed.



(a) (b) (c)

(d) (e) (f)

FIGURE 7. Sample Illustration of Mandril Image Pixel Pair Adjacency Correlation {(a) Plain Diagonal Adjacency Correlation; (b) Plain Horizontal Adjacency Correlation; (c) Plain Vertical Adjacency Correlation; (d) Encrypted Diagonal Adjacency Correlation; (e) Encrypted Horizontal Adjacency Correlation; (f) Encrypted Vertical Adjacency Correlation}}

TABLE V
MEASUREMENTS RESULTS OF CORRELATION COEFFICIENT AND WITH PRIOR STUDIES

Image	Direction	Method [28]	Method [30]	Method[31]	Method [33]	Proposed
Aerial	D	-	-	−0.0024	-	0.0012
	H	-	-	−0.0004	-	-0.0015
	V	-	-	0.0026	-	-7.64E-5
Boat	D	-	-	0.0012	-	-0.0011
	H	-	-	0.0003	-	0.0020
	V	-	-	0.0002	-	-0.0011
Cameraman	D	-	-	0.0023	-	-0.0001
	H	-	-	0.0093	-	0.0012
	V	-	-	−0.0021	-	-0.0032
Goldhill	D	-	-	-	-	-0.0011
	H	-	-	-	-	0.0007
	V	-	-	-	-	-0.0008
Mandril	D	0.0017	−0.0007	-	-	-0.0014
	H	0.0016	−0.0029	-	-	-0.0001
	V	0.0019	0.0005	-	-	-0.0006
Peppers	D	-	-	0.0020	0.0044	0.0007
	H	-	-	−0.001	-0.0016	-0.0013
	V	-	-	0.0021	-0.0020	-0.0011
Pirate	D	0.0018	-	-	-	0.0009
	H	0.0017	-	-	-	0.0007
	V	0.0019	-	-	-	0.0001

Figure 7 depicts a correlation coefficient plot for 10,000 pairs of pixels in each direction (horizontal, vertical, and diagonal) for both the original and encrypted images. Figures 7(a-c) illustrate pairwise pixel correlation plots of a plain image of Mandril in three directions: vertical, diagonal, and horizontal. These plots reveal a structured pattern with points clustered along diagonal lines, indicating a high correlation between adjacent pixels. Conversely, in the encrypted plot (Fig. 7(d-f)), the scattered arrangement of dots lacks a discernible structure, suggesting the successful removal of correlation between adjacent pixels through encryption. Further details are presented in Table 5, which showcases the results of measuring the correlation coefficient (r) in horizontal, vertical, and diagonal directions. Additionally, Table 5 offers a comparative analysis with previous studies.

The data provided in Table 5 demonstrates that the r values for the proposed method are predominantly close to zero across three directions: diagonal (D), horizontal (H), and vertical (V). This suggests that the proposed method effectively diminishes the correlation between pixels in encrypted images, which is a desirable characteristic in image encryption algorithms for enhancing security against statistical attacks. Furthermore, the correlation values remain relatively consistent and outperform those of the previous method.

E. PEAK SIGNAL-TO-NOISE RATIO (PSNR) ANALYSIS

PSNR is a statistical metric commonly employed in the assessment of image encryption. It gauges the distortion level or noise within an encrypted image; a high degree of distortion signifies the effectiveness of the encryption process[30], [40], [62], [63]. PSNR can be assessed using Equation (14), which takes the plaintext image (P) and the encrypted image (E) as inputs.

$$PSNR_{PE} = 10\log 10\left(\frac{\max^2}{\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(P_{ij}-E_{ij}\right)^2}\right) \tag{14}$$

where N and M denote the width and height dimensions of the images, respectively, while i and j refer to the specific pixel coordinates. Meanwhile, max represents the maximum pixel value found in both images.

At the decryption stage, the quality can also be assessed by a high PSNR after decryption, indicating that the original image has been reconstructed with minimal or no information loss. An infinite PSNR value indicates no errors in the decrypted image; in other words, the original and decrypted images are identical. Maintaining the integrity and quality of the original image after encryption and decryption is crucial in image encryption applications. Table 6 shows the PSNR calculation results for the encryption and decryption process. Apart from that, it is also compared with previous methods, where the proposed method appears significantly superior.

TABLE VI
MEASUREMENTS RESULTS OF PSNR (DB) IN ENCRYPTION AND DECRYPTION

Image	Encryption		Decryption
	Method[31]	Proposed	
Aerial	8.7651	7.1817	∞
Boat	7.0034	7.5144	∞
Cameraman	8.4045	7.6038	∞
Goldhill	-	7.2369	∞
Mandril	9.7296	8.2315	∞
Peppers	8.8792	7.2191	∞
Pirate	-	7.7168	∞
Average	8.55636	7.52917	∞

F. KEYSPACE AND KEY SENSITIVITY ANALYSIS

Keyspace analysis is critical in evaluating the strength of image encryption methods. A huge key space is essential to withstand brute-force attacks, where an attacker tries every possible key and makes such attacks impractical. A large key space also reduces the chance of key collisions, where different keys produce the same encryption output. This guarantees that the key used for encryption is unpredictable and not easy to guess. Studies [64], [65] have indicated that a key space of at least 2^{100} is required to make it difficult for an attacker to perform a brute-force attack. The proposed method employs various dynamically adjustable initial value parameters and hash functions to expand the key space, with Table 7 providing an in-depth keyspace calculation.

TABLE VII
APPROXIMATION OF KEYSPACE FOR ALL PHASE

Method	Keyspace
SHA-512	2^{512}
2D-SQPM	$\approx 2 \times 2 \times 10^{18}$
2D-SCM	$\approx 2 \times 2 \times 10^{18}$
Total	$\approx 1.34 \times 10^{154}$

In Table 7, it can be seen that using SHA-512 alone produces a key space of 2^{512}. In practice, SHA-512 output is indeed 512 bits[66], which are usually represented as 128 hexadecimal characters because each hexadecimal character (0-9, A-F) represents 4 bits ($2^4 = 16$ possible values). So, 128 hexadecimal characters represent $128 \times 4 = 512$ bits. This provides strong security, adding other initial parameters for a total key space of about $\approx 1.34 \times 10^{154}$. Indicating a robust defense against brute-force attacks as per the data. This substantial key space size effectively ensures the method's resilience to invasive attempts. Key sensitivity in image encryption is a crucial aspect that ensures small changes to the encryption key result in significant alterations to the encrypted image. This is vital as it guarantees that no two nearly identical keys can produce similar encrypted images. If the encryption system is not sensitive to key changes, attackers could potentially guess the original key by observing output patterns and making minor variations to the guessed key. High key sensitivity also ensures that every bit of the key significantly influences the encrypted image, thereby enhancing the complexity and security of the encryption.

In our study, we introduced a 1-bit alteration to the decryption key, and the outcomes, as depicted in Fig. 8, demonstrate a marked difference in the encrypted images. This significant variation is attributed to the high sensitivity of the dynamic key parameters and the chaotic sequence to any alterations. When these elements are integrated with the SHA-512 function, the overall sensitivity of the key is greatly amplified, showcasing the profound impact of even minor changes on the encryption process.

In addition to testing key sensitivity with 1-bit alteration, we were also inspired by the research [53], which utilizes a difference of 10^{-15}. Therefore, one of the initial parameters of the 2D-SCM is tested with constant values, namely 5.6×10^0 and $5.6 \times 10^0 + 1 \times 10^{-15}$, the difference between these two values is 10^{-15}. In this case, it was tested on the Mandrill image, where the resulting NPCR is 0.996192 and UACI is 0.33488. The encrypted image and its difference are presented in Figure 9. These results affirm that the proposed method possesses very high key sensitivity.

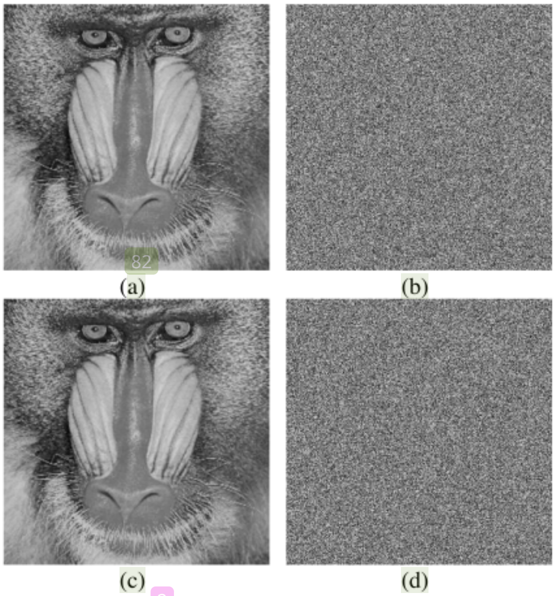


FIGURE 8. Sample of Key Sensitivity Decryption Results{(a) Original Mandril Image; (b) Encrypted Mandril Image; (c) Decrypted Mandril Image with correct key;(d) Decrypted Mandril Image with slight key modification}

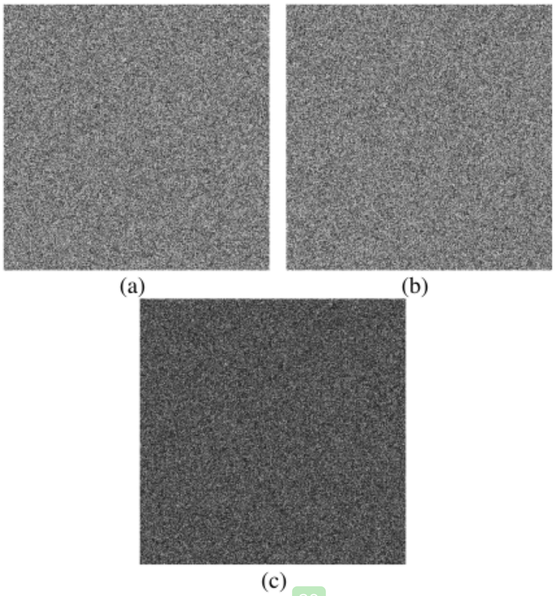


FIGURE 9. Sample of Key Sensitivity Encryption Results with different 10^{-15} {(a) Initial parameter 5.6×10^0; (b) Initial parameter $5.6 \times 10^0 + 1 \times 10^{-15}$; (c) Different Image}

G. NIST STATISTICAL TEST SUITE

The NIST Statistical Test Suite, developed by the National Institute of Standards and Technology (NIST), comprises a set of statistical tests to evaluate the randomness of binary sequences generated by hardware or software random number generators. This evaluation is crucial in the realm of image encryption, where high randomness is essential to ensure security. A well-encrypted image should exhibit a seemingly random distribution of pixels, thwarting attackers' attempts to extract meaningful information or detect patterns[67]. The suite of tests can be downloaded at URL https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software.

The suite encompasses 15 tests, each targeting different aspects of randomness and employing specific methods for analyzing binary sequences. The data under examination is typically converted into a .dat file to facilitate measurement. Each test produces a p-value, which evaluates the null hypothesis that the tested sequence is random. The p-value range is between 0 and 1, where a p-value greater than 0.01 usually indicates that the sequence can be considered random (accepting the hypothesis) [31]. If the p-value is less than 0.01, the sequence is considered non-random (rejects the hypothesis), which could indicate a weakness in the encryption. The results of the NIST statistical test, presented in Table 8, reveal that the proposed encryption method has passed all the tests, confirming its resilience against diverse types of attacks. This is further supported by the average p-value for all encrypted images, indicating the method's efficacy.

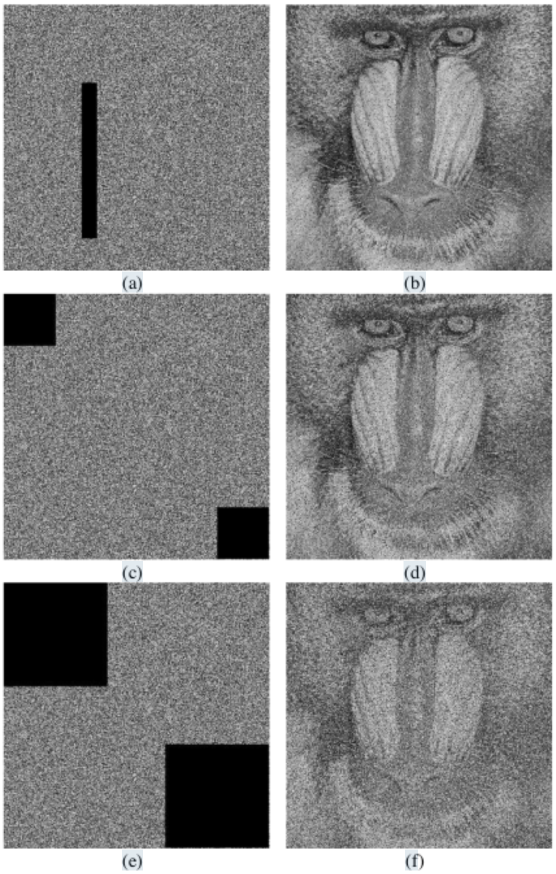
TABLE VIII
MEASUREMENTS RESULTS OF NIST STATISTICAL TEST SUITE RESULTS

No	Test Name	p-Value	Note
1	Frequency	0.59970	succeed
2	Block Frequency	0.75750	succeed
3 a	Cumulative Sums (Forward)	0.77910	succeed
3 b	Cumulative Sums (Reverse)	0.87780	succeed
4	Runs	0.57431	succeed
5	Longest Run of Ones	0.26108	succeed
6	Rank	0.59129	succeed
7	Discrete Fourier Transform	0.70995	succeed
8	Nonperiodic Template Matchings	0.79943	succeed
9	Overlapping Template Matchings	0.85375	succeed
10	Universal Statistical	0.66330	succeed
11	Approximate Entropy	0.89097	succeed
12	Random Excursions	0.48021	succeed
13	Random Excursions Variant	0.78095	succeed
14	Serial	0.91158	succeed
15	Linear Complexity	0.53519	succeed
	Mean	0.69163	succeed

H. DATA LOSS ATTACK

The data loss attack test on image encryption can demonstrate the robustness of the encryption against data loss. In the context of digital information security, it is crucial to ensure that encrypted images can be decrypted as effectively as possible, even if some data is missing, such as due to transmission disruptions or deliberate attacks by third parties[68]–[70]. Figure 10 presents a sample of a data loss attack test, where parts (a), (c), and (e) are samples of attacks on the encrypted image. The black areas indicate parts of the image that no longer contain useful information. In part (a), the data loss dimension is 30×300 pixels, in part (b) the data loss dimension is 2×100×100 pixels, and in part (c) the data loss dimension is 2×200×200 pixels. Parts (b), (d), and (f) show the decryption results. Next, we tested with noise attacks such as salt and paper 0.05 and Gaussian noise 0.01 which were presented respectively in parts (g), (h) and (i), (j).

It is apparent that the larger the area of data loss, the more noise is present in the decrypted image. Nevertheless, visually, the results are still recognizable, as the decrypted images are able to retain the majority of the content and recognizable visual structure, indicating that the encryption method can handle partial data loss without a total loss of information. The results of this data loss attack test show that the proposed image encryption is proven not only to protect against unauthorized access but also to ensure that data can be recovered as much as possible in conditions of data loss.


(a) (b)
(c) (d)
(e) (f)

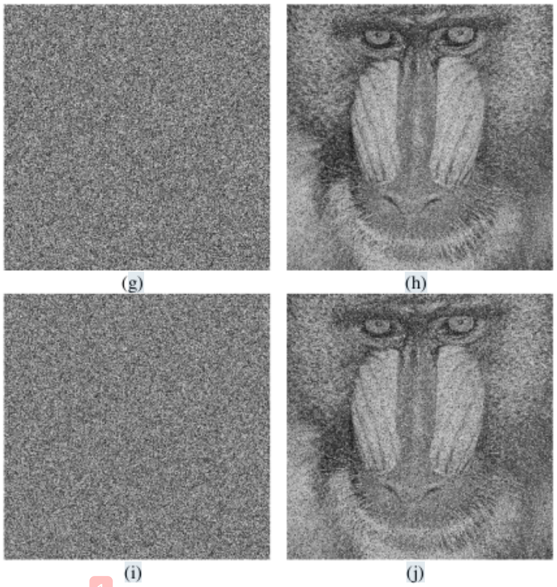


FIGURE 10. Sample of Encrypted and Decrypted Image after Attack {(a, c, e) Encrypted Mandril Image after Data Loss Attack; (b, d, f) Decrypted Mandril Image after Data Loss Attack; (g) Encrypted Mandril Image after Salt and Pepper Attack 0.05; (h) Decrypted Mandril Image after Salt and Pepper Noise 0.05; (i) Encrypted Mandril Image after Gaussian Noise Attack 0.01; (j) Decrypted Mandril Image after Gaussian Noise Attack 0.01}

I. COMPUTATIONAL COMPLEXITY AND TIME ANALYSIS

Computational complexity analysis in Big-O notation is crucial for image encryption as it provides insights into the efficiency and scalability of the algorithm[56], [71]. By understanding Big-O complexity, developers can select or design optimal algorithms, ensuring that the encryption method can efficiently handle large images and remain effective as data scales increase. This also aids in comparing different algorithms, balancing security and efficiency, and optimizing the algorithm for practical application. Here are detailed discussions on the proposed encryption algorithm:

1. The sort operation for permutation on the image array has a complexity of $O(n\ log\ n)$.
2. Binary to decimal conversion, and vice versa, modulus operation and bitxor have a complexity of $O(n)$ because operations are performed individually on each element.
3. The Feistel loop has a constant factor of 8 rounds. Thus, the Feistel loop does not add complexity that depends on the image size but adds a constant factor, making its complexity $O(n)$ instead of $O(rounds \times n)$.
4. The 2D-SCM and 2D-SQPM functions have iterations depending on the number of pixels, meaning they have a complexity of $O(n)$.

The main consideration in complexity analysis is that there are no other operations in the algorithm with a faster growth rate than $O(n\ log\ n)$. Although there are many operations with $O(n)$, complexity, the total algorithm complexity is taken from the fastest-growing facto, in this case $O(n\ log\ n)$.

This study also measures the time required for encryption and decryption. Since the method implementation uses MATLAB, the tic toc function measures the required time. The 100 encryption and decryption process trial test results produced average values of 0.47832 and 0.48232, respectively.

V. CONCLUSION

In this research, we have successfully developed an innovative image encryption method by integrating 2D-SQPM and 2D-SCM chaotic maps, modified Feistel network techniques, and the SHA-512 hash function. The primary motivation for this research is to expand the key space and increase key sensitivity, thereby enhancing the overall security of the encryption process. Our method focuses on achieving a uniform distribution of encryption and increasing encryption complexity while maintaining efficiency. The empirical results emphasize the method's substantial progress in reducing inter-pixel correlation and show strong robustness against various attacks, including statistical, differential, and data loss attacks. This method produces explicitly more prominent NPCR, UACI, and correlation coefficient values; the performance of the encryption method is also relatively stable on various measuring instruments. The proposed method has a relatively fast computational process with encryption and decryption times of less than 0.5 seconds. This demonstrates that the proposed method is overall effective and superior to previous research. The success of this research is seen in its contribution to the field of image encryption, meeting the research objectives by offering a more secure and efficient encryption solution. The significance of this research lies in its integration of complex, chaotic dynamics and advanced encryption mechanisms, providing a substantial contribution to digital information security. However, this research has some limitations, such as the dependence on susceptible initial parameters and the need for relatively high computational resources. Future research should explore further optimization to reduce computational complexity and enhance resistance to more sophisticated types of attacks. This method not only addresses current encryption challenges but also sets a new benchmark for future research in image encryption, paving the way for further innovation in securing digital images against evolving cyber threats.

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.

ACKNOWLEDGEMENT

This research was supported and funded by Universitas Stikubank (UNISBANK) Semarang Indonesia in 2023 (Grant

No. 003/DP PMP/UNISBANK/KONTRAK-PN/IV/2023)

REFERENCES

[1] B. M. P. Waseso and N. A. Setiyanto, "Web Phishing Classification using Combined Machine Learning Methods," *J. Comput. Theor. Appl.*, vol. 1, no. 1, pp. 11–18, Aug. 2023, doi: 10.33633/jcta.v1i1.8898.

[2] P. N. Andono and D. R. I. M. Setiadi, "Improved Pixel and Bit Confusion-Diffusion Based on Mixed Chaos and Hash Operation for Image Encryption," *IEEE Access*, vol. 10, no. November, pp. 115143–115156, 2022, doi: 10.1109/ACCESS.2022.3218886.

[3] J. K. Oladele *et al.*, "BEHeDaS: A Blockchain Electronic Health Data System for Secure Medical Records Exchange," *J. Comput. Theor. Appl.*, vol. 1, no. 3, pp. 231–242, Jan. 2024, doi: 10.62411/jcta.9509.

[4] M. I. Akazue, I. A. Debekeme, A. E. Edje, C. Asuai, and U. J. Osame, "UNMASKING FRAUDSTERS: Ensemble Features Selection to Enhance Random Forest Fraud Detection," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 201–211, Dec. 2023, doi: 10.33633/jcta.v1i2.9462.

[5] F. O. Aghware *et al.*, "Enhancing the Random Forest Model via Synthetic Minority Oversampling Technique for Credit-Card Fraud Detection," *J. Comput. Theor. Appl.*, vol. 1, no. 4, pp. 407–420, Mar. 2024, doi: 10.62411/jcta.10323.

[6] E. U. Omede, A. E. Edje, M. I. Akazue, H. Utomwen, and A. A. Ojugo, "IMANoBAS: An Improved Multi-Mode Alert Notification IoT-based Anti-Burglar Defense System," *J. Comput. Theor. Appl.*, vol. 1, no. 3, pp. 273–283, Feb. 2024, doi: 10.62411/jcta.9541.

[7] D. R. I. M. Setiadi, S. Widiono, A. N. Safriandono, and S. Budi, "Phishing Website Detection Using Bidirectional Gated Recurrent Unit Model and Feature Selection," *J. Futur. Artif. Intell. Technol.*, vol. 2, no. 1, pp. 75–83, 2024, doi: 10.62411/faith.2024-15.

[8] CrowdStrike, "CrowdStrike 2024 Global Threat Report," 2024. Accessed: Jul. 10, 2024. [Online]. Available: https://www.crowdstrike.com/global-threat-report/

[9] H. Wen and Y. Lin, "Cryptanalyzing an image cipher using multiple chaos and DNA operations," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 7, p. 101612, Jul. 2023, doi: 10.1016/j.jksuci.2023.101612.

[10] H. Wen, Y. Lin, and Z. Feng, "Cryptanalyzing a bit-level image encryption algorithm based on chaotic maps," *Eng. Sci. Technol. an Int. J.*, vol. 51, p. 101634, Mar. 2024, doi: 10.1016/j.jestch.2024.101634.

[11] H. Wen and Y. Lin, "Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding," *Expert Syst. Appl.*, vol. 237, p. 121514, Mar. 2024, doi: 10.1016/j.eswa.2023.121514.

[12] H. Wen, Y. Lin, L. Yang, and R. Chen, "Cryptanalysis of an image encryption scheme using variant Hill cipher and chaos," *Expert Syst. Appl.*, vol. 250, p. 123748, Sep. 2024, doi: 10.1016/j.eswa.2024.123748.

[13] A. Singh, K. B. Sivangi, and A. N. Tentu, "Machine Learning and Cryptanalysis: An In-Depth Exploration of Current Practices and Future Potential," *J. Comput. Theor. Appl.*, vol. 1, no. 3, pp. 257–272, Feb. 2024, doi: 10.62411/jcta.9851.

[14] D. R. I. M. Setiadi and M. Akrom, "Hybrid Quantum Key Distribution Protocol with Chaotic System for Securing Data Transmission," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 188–200, Dec. 2023, doi: 10.33633/jcta.v1i2.9547.

[15] D. R. I. M. Setiadi, E. H. Rachmawanto, and R. Zulfiningrum, "Medical Image Cryptosystem using Dynamic Josephus Sequence and Chaotic-hash Scrambling," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6818–6828, Oct. 2022, doi: 10.1016/j.jksuci.2022.04.002.

[16] W. Song, C. Fu, Y. Zheng, M. Tie, J. Liu, and J. Chen, "A parallel image encryption algorithm using intra bitplane scrambling," *Math. Comput. Simul.*, vol. 204, pp. 71–88, 2023, doi: 10.1016/j.matcom.2022.07.029.

[17] C. E. Shannon, "A Mathematical Theory of Cryptography." pp. 1–136, 1945. [Online]. Available: https://www.iacr.org/museum/shannon45.html

[18] N.-R. Zhou, L.-L. Hu, Z.-W. Huang, M.-M. Wang, and G.-S. Luo, "Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm," *Expert Syst. Appl.*, vol. 238, no. PC, p. 122052, Mar. 2024, doi: 10.1016/j.eswa.2023.122052.

[19] W. Alexan, N. Alexan, and M. Gabr, "Multiple-Layer Image Encryption Utilizing Fractional-Order Chen Hyperchaotic Map and Cryptographically Secure PRNGs," *Fractal Fract.*, vol. 7, no. 4, p. 287, Mar. 2023, doi: 10.3390/fractalfract7040287.

[20] M. Ahmad, I. A. Khaja, A. Baz, H. Alhakami, and W. Alhakami, "Particle Swarm Optimization Based Highly Nonlinear Substitution-Boxes Generation for Security Applications," *IEEE Access*, vol. 8, pp. 116132–116147, 2020, doi: 10.1109/ACCESS.2020.3004449.

[21] H. Li *et al.*, "A novel image encryption scheme based on non-adjacent parallelable permutation and dynamic DNA-level two-way diffusion," *J. Inf. Secur. Appl.*, vol. 61, no. June, p. 102844, Sep. 2021, doi: 10.1016/j.jisa.2021.102844.

[22] S. K.U. and A. Mohamed, "Novel hyper chaotic color image encryption based on pixel and bit level scrambling with diffusion," *Signal Process. Image Commun.*, vol. 99, no. May, p. 116495, Nov. 2021, doi: 10.1016/j.image.2021.116495.

[23] D. R. I. M. Setiadi, R. Robet, O. Pribadi, S. Widiono, and M. K. Sarker, "Image Encryption using Half-Inverted Cascading Chaos Cipheration," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 61–77, Oct. 2023, doi: 10.33633/jcta.v1i2.9388.

[24] D. Wei, M. Jiang, and Y. Deng, "A secure image encryption algorithm based on hyper-chaotic and bit-level permutation," *Expert Syst. Appl.*, vol. 213, no. PB, p. 119074, 2023, doi: 10.1016/j.eswa.2022.119074.

[25] J. Sun, "2D-SCMCI Hyperchaotic Map for Image Encryption Algorithm," *IEEE Access*, vol. 9, no. Cmc, pp. 59313–59327, 2021, doi: 10.1109/ACCESS.2021.3070350.

[26] Q. Lai, H. Hua, X.-W. Zhao, U. Erkan, and A. Toktas, "Image encryption using fission diffusion process and a new hyperchaotic map," *Chaos, Solitons & Fractals*, vol. 175, no. September, p. 114022, Oct. 2023, doi: 10.1016/j.chaos.2023.114022.

[27] W. Feng *et al.*, "Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption," *Expert Syst. Appl.*, vol. 246, no. January, p. 123190, Jul. 2024, doi: 10.1016/j.eswa.2024.123190.

[28] D. R. I. M. Setiadi and N. Rijati, "An Image Encryption Scheme Combining 2D Cascaded Logistic Map and Permutation-Substitution Operations," *Computation*, vol. 11, no. 9, p. 178, Sep. 2023, doi: 10.3390/computation11090178.

[29] E. Winarno, K. Nugroho, P. W. Adi, and D. R. I. M. Setiadi, "Integrated dual hyperchaotic and Josephus traversing based 3D confusion-diffusion pattern for image encryption," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 9, p. 101790, Oct. 2023, doi: 10.1016/j.jksuci.2023.101790.

[30] D. Li, J. Li, and X. Di, "A novel exponential one-dimensional chaotic map enhancer and its application in an image encryption scheme using modified ZigZag transform," *J. Inf. Secur. Appl.*, vol. 69, no. August, p. 103304, 2022, doi: 10.1016/j.jisa.2022.103304.

[31] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik (Stuttg).*, vol. 272, no. November 2022, p. 170316, Feb. 2023, doi: 10.1016/j.ijleo.2022.170316.

[32] H. Liu, L. Teng, Y. Zhang, R. Si, and P. Liu, "Mutil-medical image encryption by a new spatiotemporal chaos model and DNA new computing for information security," *Expert Syst. Appl.*, vol. 235, no. March 2023, p. 121090, 2024, doi: 10.1016/j.eswa.2023.121090.

[33] V. R. Folifack Signing *et al.*, "A cryptosystem based on a chameleon chaotic system and dynamic DNA coding," *Chaos, Solitons & Fractals*, vol. 155, p. 111777, Feb. 2022, doi: 10.1016/j.chaos.2021.111777.

[34] S. Xu, X. Wang, and X. Ye, "A new fractional-order chaos system of Hopfield neural network and its application in image encryption," *Chaos, Solitons & Fractals*, vol. 157, p. 111889, Apr. 2022, doi: 10.1016/j.chaos.2022.111889.

[35] S. Wang, L. Hong, and J. Jiang, "An image encryption scheme using a chaotic neural network and a network with multistable hyperchaos," *Optik (Stuttg).*, vol. 268, no. January, p. 169758, Oct. 2022, doi: 10.1016/j.ijleo.2022.169758.

[36] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review,

Application, and Challenges," *Mathematics*, vol. 11, no. 11, 2023, doi: 10.3390/math11112585.

[37] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Appl. Phys. B Lasers Opt.*, vol. 126, no. 9, pp. 1–19, 2020, doi: 10.1007/s00340-020-07480-x.

[38] E. Winarno, K. Nugroho, P. W. Adi, and D. R. I. M. Setiadi, "Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption Based on Hyperchaotic System," *IEEE Access*, vol. 11, pp. 69005–69021, 2023, doi: 10.1109/ACCESS.2023.3285481.

[39] X. Wang and H. Liu, "Cross-plane multi-image encryption using chaos and blurred pixels," *Chaos, Solitons & Fractals*, vol. 164, no. August, p. 112586, Nov. 2022, doi: 10.1016/j.chaos.2022.112586.

[40] N. R. Zhou, L. J. Tong, and W. P. Zou, "Multi-image encryption scheme with quaternion discrete fractional Tchebyshev moment transform and cross-coupling operation," *Signal Processing*, vol. 211, p. 109107, 2023, doi: 10.1016/j.sigpro.2023.109107.

[41] X. Wang and Y. Chen, "A New Chaotic Image Encryption Algorithm Based on L-Shaped Method of Dynamic Block," *Sens. Imaging*, vol. 22, no. 1, 2021, doi: 10.1007/s11220-021-00357-z.

[42] W. Feng *et al.*, "Exploiting Newly Designed Fractional-Order 3D Lorenz Chaotic System and 2D Discrete Polynomial Hyper-Chaotic Map for High-Performance Multi-Image Encryption," *Fractal Fract.*, vol. 7, no. 12, pp. 1–30, 2023, doi: 10.3390/fractalfract7120887.

[43] O. Kocak, U. Erkan, A. Toktas, and S. Gao, "PSO-based image encryption scheme using modular integrated logistic exponential map," *Expert Syst. Appl.*, vol. 237, no. September 2023, 2024, doi: 10.1016/j.eswa.2023.121452.

[44] H. Li *et al.*, "Exploiting Dynamic Vector-Level Operations and a 2D-Enhanced Logistic Modular Map for Efficient Chaotic Image Encryption," *Entropy*, vol. 25, no. 8, 2023, doi: 10.3390/e25081147.

[45] U. Erkan, A. Toktas, and Q. Lai, "2D hyperchaotic system based on Schaffer function for image encryption," *Expert Syst. Appl.*, vol. 213, no. October 2022, p. 119076, Mar. 2023, doi: 10.1016/j.eswa.2022.119076.

[46] U. Erkan, A. Toktas, and Q. Lai, "Design of two dimensional hyperchaotic system through optimization benchmark function," *Chaos, Solitons & Fractals*, vol. 167, p. 113032, Feb. 2023, doi: 10.1016/j.chaos.2022.113032.

[47] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "A novel pixel-split image encryption scheme based on 2D Salomon map," *Expert Syst. Appl.*, vol. 213, no. PA, p. 118845, Mar. 2023, doi: 10.1016/j.eswa.2022.118845.

[48] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, Aug. 2018, doi: 10.1016/j.sigpro.2018.03.010.

[49] L. Chen, C. Li, and C. Li, "Security measurement of a medical communication scheme based on chaos and DNA coding," *J. Vis. Commun. Image Represent.*, vol. 83, p. 103424, Feb. 2022, doi: 10.1016/j.jvcir.2021.103424.

[50] S. Liu, C. Li, and Q. Hu, "Cryptanalyzing Two Image Encryption Algorithms Based on a First-Order Time-Delay System," *IEEE Multimed.*, vol. 29, no. 1, pp. 74–84, Jan. 2022, doi: 10.1109/MMUL.2021.3114589.

[51] A. JarJar, "Improvement of Feistel method and the new encryption scheme," *Optik (Stuttg).*, vol. 157, pp. 1319–1324, Mar. 2018, doi: 10.1016/j.ijleo.2017.12.065.

[52] B. Schneier, *Applied cryptography*, 20th ed. Standards Information Network, 2017.

[53] A. Raghuvanshi, M. Budhia, K. A. K. Patro, and B. Acharya, "FSR-SPD: an efficient chaotic multi-image encryption system based on flip-shift-rotate synchronous-permutation-diffusion operation," *Multimed. Tools Appl.*, no. 0123456789, Dec. 2023, doi: 10.1007/s11042-023-17700-z.

[54] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019, doi: 10.1109/ACCESS.2019.2906052.

[55] Z. Gan, X. Chai, D. Han, and Y. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation," *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7111–7130, Nov. 2019, doi: 10.1007/s00521-018-3541-y.

[56] K. A. K. Patro and B. Acharya, *An efficient dual-layer cross-coupled chaotic map security-based multi-image encryption system*, vol. 104, no. 3. Springer Netherlands, 2021. doi: 10.1007/s11071-021-06409-z.

[57] M. SaberiKamarposhti, A. Ghorbani, and M. Yadollahi, "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," *Chaos, Solitons & Fractals*, vol. 178, no. November 2023, p. 114361, Jan. 2024, doi: 10.1016/j.chaos.2023.114361.

[58] L.-H. Gong, H.-X. Luo, R.-Q. Wu, and N.-R. Zhou, "New 4D chaotic system with hidden attractors and self-excited attractors and its application in image encryption based on RNG," *Phys. A Stat. Mech. its Appl.*, vol. 591, p. 126793, Apr. 2022, doi: 10.1016/j.physa.2021.126793.

[59] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 333–350, Jun. 2020, doi: 10.1016/j.future.2020.02.029.

[60] Y. Zhang, "Statistical test criteria for sensitivity indexes of image cryptosystems," *Inf. Sci. (Ny).*, vol. 550, pp. 313–328, Mar. 2021, doi: 10.1016/j.ins.2020.10.026.

[61] S. Dash, S. Padhy, S. Anjali Devi, S. Sachi, and K. A. K. Patro, "An efficient Intra-Inter pixel encryption scheme to secure healthcare images for an IoT environment," *Expert Syst. Appl.*, vol. 231, no. June, p. 120622, 2023, doi: 10.1016/j.eswa.2023.120622.

[62] M. G. A. Malik, Z. Bashir, N. Iqbal, and M. A. Imtiaz, "Color Image Encryption Algorithm Based on Hyper-Chaos and DNA Computing," *IEEE Access*, vol. 8, pp. 88093–88107, 2020, doi: 10.1109/ACCESS.2020.2990170.

[63] A. Setyono, D. R. I. M. Setiadi, and M. Muljono, "StegoCrypt method using wavelet transform and one-time pad for secret image delivery," in *2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, Oct. 2017, pp. 203–207. doi: 10.1109/ICITACEE.2017.8257703.

[64] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Processing*, vol. 141, pp. 109–124, Dec. 2017, doi: 10.1016/j.sigpro.2017.04.006.

[65] Y. Liu and J. Zhang, "A Multidimensional Chaotic Image Encryption Algorithm based on DNA Coding," *Multimed. Tools Appl.*, vol. 79, no. 29–30, pp. 21579–21601, Aug. 2020, doi: 10.1007/s11042-020-08880-z.

[66] Q. H. Dang, "Secure Hash Standard," Gaithersburg, MD, Jul. 2015. doi: 10.6028/NIST.FIPS.180-4.

[67] A. Rukhin *et al.*, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," Fort Belvoir, 2001. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA393366

[68] K. A. K. Patro, B. Acharya, and V. Nath, "Secure, Lossless, and Noise-resistive Image Encryption using Chaos, Hyper-chaos, and DNA Sequence Operation," *IETE Tech. Rev.*, vol. 37, no. 3, pp. 223–245, May 2020, doi: 10.1080/02564602.2019.1595751.

[69] L. H. Gong and H. X. Luo, "Dual color images watermarking scheme with geometric correction based on quaternion FrOOFMMs and LS-SVR," *Opt. Laser Technol.*, vol. 167, no. July, p. 109665, 2023, doi: 10.1016/j.optlastec.2023.109665.

[70] C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "Robust and imperceptible image watermarking by DC coefficients using singular value decomposition," in *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2017. doi: 10.1109/EECSI.2017.8239107.

[71] S. Dash, S. Padhy, B. Parija, T. Rojashree, and K. A. K. Patro, "A Simple and Fast Medical Image Encryption System Using Chaos-Based Shifting Techniques," *Int. J. Inf. Secur. Priv.*, vol. 16, no. 1, pp. 1–24, Jul. 2022, doi: 10.4018/IJISP.303669.

EDY WINARNO received a Doctoral degree in Computer Science from the Department of Computer Science in 2016. He is currently an Associate Professor at the Faculty of Information Technology and Industry at Stikubank University. His research interests include computer vision, image processing and security, and artificial intelligence. He can be contacted at email: edywin@edu.unisbank.ac.id.

WIWIEN HADIKURNIAWATI received her Bachelor's degree in Electrical Engineering from Semarang University, Indonesia, in 1999. She completed her Master's degree in Information Systems at Diponegoro University, Indonesia, in 2010. She is a lecturer at the Faculty of Information Technology and Industry at Stikubank University, Indonesia. Her research focuses on machine learning and decision making. She can be contacted via email at wiwien@edu.unisbank.ac.id

KRISTIAWAN NUGROHO is a lecturer and researcher at the Faculty of Information Technology and Industry, Stikubank University. He obtained a bachelor's degree 2001 in the information systems department, Faculty of Computer Science, Dian Nuswantoro University. In 2007, he obtained a Master's degree in Informatics Engineering Dian Nuswantoro University. He also obtained a Doctoral degree in Computer Science with a concentration in Machine Learning and Artificial Intelligence in 2022 at Dian Nuswantoro University Semarang. He has researched machine learning, image recognition, speech recognition and sentiment analysis. He can be contacted via email at kristiawan@edu.unisbank.ac.id

VERONICA LUSIANA received a Bachelor's degree in Electrical Engineering from Semarang University, Indonesia 2000. She completed a Master's in Information Systems at Diponegoro University, Indonesia, in 2009. She is a lecturer at the Faculty of Information and Industrial Technology, Stikubank University, Indonesia. Her field of science is cryptography and image processing. She can be contacted via email at vero@edu.unisbank.ac.id.

Integrating Quadratic Polynomial and Symbolic Chaotic Map-based Feistel Network to Improve Image Encryption Performance

ORIGINALITY REPORT

20%	11%	19%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Edy Winarno, Kristiawan Nugroho, Prajanto Wahyu Adi, De Rosal Ignatius Moses Setiadi. "Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption Based on Hyperchaotic System", IEEE Access, 2023 Publication	2%
2	www2.mdpi.com Internet Source	1%
3	Qiang Lai, Hanqiang Hua, Xiao-Wen Zhao, Uğur Erkan, Abdurrahim Toktas. "Image encryption using fission diffusion process and a new hyperchaotic map", Chaos, Solitons & Fractals, 2023 Publication	1%
4	publikasi.dinus.ac.id Internet Source	1%
5	Morteza SaberiKamarposhti, Amirabbas Ghorbani, Mehdi Yadollahi. "A comprehensive survey on image encryption: Taxonomy,	1%

	challenges, and future directions", Chaos, Solitons & Fractals, 2024 Publication	
6	inass.org Internet Source	1 %
7	www.mdpi.com Internet Source	1 %
8	De Rosal Ignatius Moses Setiadi, Nova Rijati. "An Image Encryption Scheme Combining 2D Cascaded Logistic Map and Permutation-Substitution Operations", Computation, 2023 Publication	<1 %
9	iris.polito.it Internet Source	<1 %
10	Khalid M. Hosny, Sara T. Kamal, Mohamed M. Darwish. "A novel color image encryption based on fractional shifted Gegenbauer moments and 2D logistic-sine map", The Visual Computer, 2022 Publication	<1 %
11	Sanjay Kumar, Deepmala Sharma. "A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm", Artificial Intelligence Review, 2024 Publication	<1 %
12	link.springer.com Internet Source	<1 %

13	Dani Elias Mfungo, Xianping Fu. "Fractal-Based Hybrid Cryptosystem: Enhancing Image Encryption with RSA, Homomorphic Encryption, and Chaotic Maps", Entropy, 2023 Publication	<1 %
14	Wei Feng, Jing Zhang, Yao Chen, Zhentao Qin, Yushu Zhang, Musheer Ahmad, Marcin Woźniak. "Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption", Expert Systems with Applications, 2024 Publication	<1 %
15	prr.hec.gov.pk Internet Source	<1 %
16	Submitted to HTM (Haridus- ja Teadusministeerium) Student Paper	<1 %
17	uia.brage.unit.no Internet Source	<1 %
18	Qingjiang Xiao, Jinrong Zhao, Sheng Feng, Guyue Li, Aiqun Hu. "Securing NextG networks with physical-layer key generation: A survey", Security and Safety, 2023 Publication	<1 %
19	brightideas.houstontx.gov Internet Source	<1 %

20	Eljadi, Fardous Mohamed, and Imad Fakhri Al-Shaikhli. "Statistical Analysis of the eSTREAM Competition Winners", 2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 2015. Publication	<1 %
21	ijece.iaescore.com Internet Source	<1 %
22	Dawei Ding, Haifei Zhu, Hongwei Zhang, Zongli Yang, Dong Xie. "An n-dimensional polynomial modulo chaotic map with controllable range of Lyapunov exponents and its application in color image encryption", Chaos, Solitons & Fractals, 2024 Publication	<1 %
23	Jiming Zheng, Tianyu Bao. "An Image Encryption Algorithm Using Cascade Chaotic Map and S-Box", Entropy, 2022 Publication	<1 %
24	Mohamed Gabr, Yousef Korayem, Yen-Lin Chen, Por Lip Yee, Chin Soon Ku, Wassim Alexan. " —Rescale, Rotate, and Randomize: A Novel Image Cryptosystem Utilizing Chaotic and Hyper-Chaotic Systems ", IEEE Access, 2023 Publication	<1 %

25	Yang Liu, Lin Teng. "An image encryption algorithm based on a new Sine-Logistic chaotic system and block dynamic Josephus scrambling", The European Physical Journal Plus, 2024 Publication	<1 %
26	Zhuoyi Lei, Jiacheng Yang, Hanshuo Qiu, Xiangzi Zhang, Jizhao Liu. "Color Image Encryption Based on a Novel Fourth-Direction Hyperchaotic System", Electronics, 2024 Publication	<1 %
27	Fu-Yan Sun. "Digital image encryption with chaotic map lattices", Chinese Physics B, 04/2011 Publication	<1 %
28	Mohammed Es-Sabry, Nabil El Akkad, Mostafa Merras, Khalid Satori, Walid El-Shafai, Torki Altameem, Mostafa M. Fouda. "Securing Images Using High Dimensional Chaotic Maps and DNA Encoding Techniques", IEEE Access, 2023 Publication	<1 %
29	Shuliang Sun, Yongning Guo, Ruikun Wu. "A Novel Image Encryption Scheme Based on 7D Hyperchaotic System and Row-column Simultaneous Swapping", IEEE Access, 2019 Publication	<1 %

30	Submitted to University of Technology Student Paper	<1 %
31	Submitted to Flinders University Student Paper	<1 %
32	Ebrahim Zareimani, Reza Parvaz. "Secure Multiple-Image Transfer by Hybrid Chaos System: Encryption and Visually Meaningful Images", Mathematics, 2024 Publication	<1 %
33	csrc.nist.gov Internet Source	<1 %
34	"Advances in Cyber Security", Springer Science and Business Media LLC, 2021 Publication	<1 %
35	Xiaoming Song, Guodong Li, Ping He. "Design of three-dimensional encryption algorithm for image based on improved 6th-order cellular neural network", Physica Scripta, 2024 Publication	<1 %
36	Uğur Erkan, Abdurrahim Toktas, Qiang Lai. "2D hyperchaotic system based on Schaffer function for image encryption", Expert Systems with Applications, 2023 Publication	<1 %
37	Xiuli Chai, Haiyang Wu, Zhihua Gan, Yushu Zhang, Yiran Chen. "Hiding cipher-images	<1 %

	generated by 2-D compressive sensing with a multi-embedding strategy", Signal Processing, 2020 Publication	
38	Ali Broumandnia. "The 3D modular chaotic map to digital color image encryption", Future Generation Computer Systems, 2019 Publication	<1%
39	Daniel Lemire. "Number parsing at a gigabyte per second", Software: Practice and Experience, 2021 Publication	<1%
40	Heping Wen, zhaoyang feng, Bai Chixin, Yiting Lin, Xiangyu Zhang, Wei Feng. "Frequency-domain image encryption based on IWT and 3D S-box", Physica Scripta, 2024 Publication	<1%
41	Hossein Movafegh Ghadirli, Ali Nodehi, Rasul Enayatifar. "An overview of encryption algorithms in color images", Signal Processing, 2019 Publication	<1%
42	W. S. Mada Sanjaya, Akhmad Roziqin, Agung Wijaya Temiesela, M. Fauzi Badru Zaman, Aria Dewa Wibiksana, Dyah Anggraeni. "Enhancing Voice Security through Rikitake Chaosbased Encryption System", 2023 IEEE 9th	<1%

	Information Technology International Seminar (ITIS), 2023 Publication	
43	Xiaoqiang Zhang, Xuesong Wang. "Digital image encryption algorithm based onelliptic curve public cryptosystem", IEEE Access, 2018 Publication	<1 %
44	www.nature.com Internet Source	<1 %
45	www.random.org Internet Source	<1 %
46	www.researchsquare.com Internet Source	<1 %
47	Ayşegül İhsan, Nurettin Doğan. "An innovative image encryption algorithm enhanced with the Pan-Tompkins Algorithm for optimal security", Multimedia Tools and Applications, 2024 Publication	<1 %
48	Liming Guo, Jianqing He, Guodong Ye. "Image encryption algorithm based on ElGamal cryptography and selective random diffusion", Physica Scripta, 2023 Publication	<1 %
49	Wenzheng Ma, Xianli Li, Tingting Yu, Zhuang Wang. "A 4D discrete Hopfield neural	<1 %

	network-based image encryption scheme with multiple diffusion modes", Optik, 2023 Publication	
50	Yuwen Sha, Jun Mou, Santo Banerjee, Yushu Zhang. "Exploiting Flexible and Secure Cryptographic Technique for Multi-Dimensional Image Based on Graph Data Structure and Three-Input Majority Gate", IEEE Transactions on Industrial Informatics, 2024 Publication	<1 %
51	www.joig.net Internet Source	<1 %
52	Chengye Zou, Lin Wang. "A visual DNA compilation of Rössler system and its application in color image encryption", Chaos, Solitons & Fractals, 2023 Publication	<1 %
53	Chenkai Zhang, Baoxiang Du. "A fast piecewise image encryption scheme combining NC1DNSM and P-Box", Integration, 2022 Publication	<1 %
54	Hsiao, Hung-I, and Junghsi Lee. "Color image encryption using chaotic nonlinear adaptive filter", Signal Processing, 2015. Publication	<1 %

55	Kim, Dong Hwan, Yong Ri Piao, Sung Jin Cho, and Seok Tae Kim. "3D Image Encryption Using Integral Imaging Scheme and MLCA Technology", Applied Mechanics and Materials, 2013. Publication	<1 %
56	Mingjie Zhao, Lixiang Li, Zheng Yuan. " A multi-image encryption scheme based on a new -dimensional chaotic model and eight-base DNA ", Chaos, Solitons & Fractals, 2024 Publication	<1 %
57	Muhammad Hanif, Sagheer Abbas, Muhammad Adnan Khan, Nadeem Iqbal, Zia Ul Rehman, Muhammad Anwaar Saeed, Ehab Mahmoud Mohamed. "A Novel and Efficient Multiple RGB Images Cipher Based on Chaotic System and Circular Shift Operations", IEEE Access, 2020 Publication	<1 %
58	Qiuxia Qin, Zhongyue Liang, Shuang Liu, Xiao Wang, Changjun Zhou. "A Dual-domain Image Encryption Algorithm Based on Hyperchaos and Dynamic Wavelet Decomposition", IEEE Access, 2022 Publication	<1 %
59	Shahna K.U., Anuj Mohamed. "Novel hyper chaotic color image encryption based on pixel	<1 %

	and bit level scrambling with diffusion", Signal Processing: Image Communication, 2021 Publication	
60	Xiaopeng Yan, Xingyuan Wang, Yongjin Xian. "Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation", Multimedia Tools and Applications, 2021 Publication	<1 %
61	Xingyuan Wang, Cheng Liu, Donghua Jiang. "A novel visually meaningful image encryption algorithm based on parallel compressive sensing and adaptive embedding", Expert Systems with Applications, 2022 Publication	<1 %
62	Xingyuan Wang, Pengbo Liu. "A New Image Encryption Scheme Based on a Novel One-Dimensional Chaotic System", IEEE Access, 2020 Publication	<1 %
63	Zhiheng Lu, NKAPKOP Jean De Dieu, Donghua Jiang, Nestor Tsafack, Jianping Xiong, Zeric Njitacke, Jacques Kengne. "Novel Duffing chaotic oscillator and its application to privacy data protection", Physica Scripta, 2023 Publication	<1 %
64	downloads.hindawi.com Internet Source	<1 %

65	ijai.iaescore.com Internet Source	<1%
66	jis-eurasipjournals.springeropen.com Internet Source	<1%
67	mjpas.uomustansiriyah.edu.iq Internet Source	<1%
68	oaji.net Internet Source	<1%
69	research.riphah.edu.pk Internet Source	<1%
70	univ-usto.dz Internet Source	<1%
71	www.emerald.com Internet Source	<1%
72	www.iapress.org Internet Source	<1%
73	Ankita Raghuvanshi, Muskan Budhia, K. Abhimanyu Kumar Patro, Bibhudendra Acharya. "FSR-SPD: an efficient chaotic multi-image encryption system based on flip-shift-rotate synchronous-permutation-diffusion operation", Multimedia Tools and Applications, 2023 Publication	<1%

74 Fei Yu, Shuai Xu, Yue Lin, Ting He, Chaoran Wu, Hairong Lin. "Design and Analysis of a Novel Fractional-Order System with Hidden Dynamics, Hyperchaotic Behavior and Multi-Scroll Attractors", Mathematics, 2024 <1%

Publication

75 Hamid El Bourakkadi, Abdelhakim Chemlal, Hassan Tabti, Mourad Kattass, Abdellatif Jarjar, Abdellhamid Benazzi. "Enhanced Color Image Encryption Utilizing a Novel Vigenere Method with Pseudorandom Affine Functions", Acadlore Transactions on AI and Machine Learning, 2024 <1%

Publication

76 Jinlong Zhang, Heping Wen. "Dynamic feedback bit-level image privacy protection based on chaos and information hiding", Scientific Reports, 2024 <1%

Publication

77 RongQing Lei, LingFeng Liu, Xuan Huang, BingXue Jin, ZiWen Zhu, LiuQin Fan. "Thumbnail-preserving encryption by sum-preserving within blocks based on exponential chaotic map", Nonlinear Dynamics, 2024 <1%

Publication

78 Shafali Agarwal. "A New Composite Fractal Function and Its Application in Image <1%

Encryption", Journal of Imaging, 2020
Publication

---

79 Xiaopeng Yan, Qing Hu, Lin Teng, Yining Su. "Unmanned ship image encryption method based on a new four-wing three-dimensional chaotic system and compressed sensing", Chaos, Solitons & Fractals, 2024
Publication
<1%

---

80 Yang Lu, Mengxin Gong, Lvchen Cao, Zhihua Gan, Xiuli Chai, Ang Li. "Exploiting 3D fractal cube and chaos for effective multi-image compression and encryption", Journal of King Saud University - Computer and Information Sciences, 2023
Publication
<1%

---

81 Yuwen Sha, Yinghong Cao, Huizhen Yan, Xinyu Gao, Jun Mou. "An image encryption scheme based on IAVL permutation scheme and DNA operations", IEEE Access, 2021
Publication
<1%

---

82 Parnab Das, Santanu Mandal. "A physical memristor-based chaotic system and its application in colour image encryption scheme", Physica Scripta, 2023
Publication
<1%

---

83 Rim Amdouni, Mohamed Ali Hajjaji, Abdellatif Mtibaa. "Hardware study and implementation of image encryption algorithm based on a
<1%

hyperchaotic key generator", Physica Scripta, 2024

Publication

84	Vinay Kumar Sharma, Janki Ballabh Sharma. "Harris Hawk Optimization driven adaptive Image encryption integrating Hilbert Vibrational Decomposition and Chaos", Applied Soft Computing, 2024 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		

Integrating Quadratic Polynomial and Symbolic Chaotic Map-based Feistel Network to Improve Image Encryption Performance

GRADEMARK REPORT

FINAL GRADE

/100

GENERAL COMMENTS

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16