ELECTRICAL & ELECTRONIC ENGINEERING | RESEARCH ARTICLE

An efficient color image encryption scheme based on a matrix scrambling method and a new hybrid chaotic map

Hidayet Ogras

Abstract: In this paper, an efficient chaos-based image encryption scheme for color images is proposed. This paper includes a strong displacement structure through a specified matrix scrambling method for pixel positions and a new hybrid chaotic map as a key generator for encryption. Chaotic Logistic map is used to generate binary bitstream for controlling diffusion process. The designed map exhibits superior performance in terms of key space range, complexity and chaotic substantiality that enhances security of the whole system. NPCR, UACI, MSE and PSNR values, which are frequently used in performance and security analysis in the field of image encryption, are at a satisfactory level and all parameters have successfully met the necessary conditions. For instance, in a good image encryption algorithm, ideal values of NPCR and UACI parameters should be 99.60% and 33.46%, respectively. The average results obtained in this study are very close to their ideal values as 99.6046 and 33.4733 for NPCR and UACI, respectively. According to a scientific study presented in the similar field, MSE value should be greater than 9,555; PSNR value must be less than 8.3875. In this study, average MSE and PSNR values calculated for six different test images are 10,315 and 7.9961, respectively. Some important analysis results have been compared to that of well-known Advanced Encryption Standard (AES) algorithm and a similar study presented in this field. Theoretical analysis and experimental results confirm that the proposed algorithm has great security and effectively encrypts and decrypts the color images with different sizes as well.

Subjects: Digital Signal Processing; Image Processing; Computer & Software Engineering

ABOUT THE AUTHOR
HIDAYET OGRAS was born in Diyarbakir, Turkey in 1983. He received the B.S. degree in Electrical and Electronics Engineering from the University of Gaziantep in 2008 in Turkey. He received M.S degree in Electrical and Electronics Engineering from the University of Firat in Elazig, Turkey in 2010 and received Ph.D. degree in Electrical and Electronics Engineering from the University of Firat in Elazig, Turkey in 2017. He is currently an Assistant Professor at department of Electronics Communication in Batman University and his research interests cover chaos-based Cryptography and Steganography. He is also interested in secure communication systems and signal processing.

PUBLIC INTEREST STATEMENT
A different and alternative approach to the standard encryption techniques has been used for image information in this scientific study. Inspired by chaos dynamics, an image encryption algorithm based on confusion and diffusion structures has been designed. The statistical and differential analyses results of the designed encryption algorithm are at a satisfactory level and significantly meet the required performance and security criteria. Another important result of this study is that more complex chaotic systems can be developed for a specific purpose and that these systems can be used effectively as cryptographic key generators.
Keywords: chaos; hybrid map; image encryption; matrix scrambling

1. Introduction
Among the multimedia information, digital image plays an important role in people’s daily life due to the increasing demand for real-time visual communication in social society. In this sense, security and protection of digital information gains importance. The first solution that comes to mind is use of data encryption algorithms for the protection of digital information confidentially. Most of the available encryption methods such as DES (Data Encryption Standard) and AES (Advanced Encryption Standard) are not generally used for image data (Liu et al., 2015; Chen et al., 2015; Qayyum et al., 2020) due to the requirement of much more processing power, bandwidth and longer time which causes low-level efficiency and significant latency during the encryption and decryption processes (Som & Sen, 2013). As a result, traditional encryption algorithms cannot be used effectively for image data.

Chaos in nonlinear dynamics systems has been attracted much attention of several different scientific areas especially in engineering science such as secure communication, cryptography and steganography for the last decades. For instance, chaos is applied in communication systems in An et al. (2011), Eisenrcraft et al. (2012), Hu et al. (2010), Jiang et al. (2011), Kaddoum et al. (2010), Kang et al. (2014), Ryu and Lee (2013), Türk and Oğraş (2011), Yang et al. (2015), Yang and Zhu (2013); used for image cryptosystems in Chen et al. (2015), Z. L. Zhu et al. (2011), Murillo-Escobar et al. (2015), Oğraş and Türk (2016), Patidar et al. (2011), Telem et al. (2014), Wang et al. (2011), Ye (2011), Ye and Guo (2014), N. Zhou et al. (2011), and H. Zhu et al. (2013); for power systems in Yíbei et al. (2011), Ginarsa et al. (2013), Yau et al. (2015), Ghasemi et al.,(2014), Chen et al. (2015); X. Zhou et al. (2012); Tur and Ogras (2021); for Steganographic systems in Ogras (2019), Kar et al. (2018), Bilal et al. (2014), Battikh et al. (2014), and Saeed (2013). There are also some important studies using chaotic systems as secret key or bit generators in cryptography (Addabbo et al., 2009; Alhadawi et al., 2019; Moysis et al., 2020; Oğraş & Mustafa, 2017). All scientific studies here show that the concept of chaos can be used effectively in data security as an alternative to modern digital encryption techniques. According to the information security principles, a powerful encryption algorithm should generate a random cipher data and must be extremely sensitive to the secret key parameters. Chaotic systems exhibit similar features of sensitivity to initial conditions and control parameters, as well as random-like behavior (Yoon & Kim, 2010), which meet Shannon’s requirements of confusion and diffusion in cryptography (Fu et al., 2018). These special features make chaotic systems a good candidate for data encryption and create the phenomena of chaos-based cryptography.

Many chaos-based image cryptosystems are proposed in this field recently and most of them contain confusion and diffusion structures. However, some of them are successfully broken (Fan & Li, 2017; Mastan & Pandian, 2020) due to their small key spaces, limited key parameters and weak encryption algorithms (Alhadawi et al., 2019). Among these weaknesses, the most serious one is that system parameters that are used to generate secret key are limited due to the chaotic system used in the cipher does not have sufficient complexity. In this study, two different chaotic systems, Sine map and Cubic map are combined under a single model thus the total number of parameter belonging the system is increased and the result is a better, more complex and larger key space of the system. In the designed model, the existence of the chaos dynamics will ensure that the whole system will be sensitive to key parameters. A new hybrid chaotic model containing Sine map and Cubic map, called SINCU map is used as a key generator for the proposed image encryption structure in this paper. Chaos-based discrete time systems, shortly chaotic maps have high efficiency comparing with the continuous time chaotic systems because of their implementations in both software and hardware are easy to apply. However, these systems have disadvantages of limited or discontinuous range of chaotic behaviors and generally show non-uniform data distribution of output sequences. This situation may create serious drawbacks in a cryptosystem such as small key space, weak security and poor efficiency.
which threat the security of the whole cryptosystem (Alowida et al., 2019). As a result, there are many studies that use different approaches to develop weaker chaotic maps to achieve better chaotic features such as in Gong et al. (2020). In this field, these new chaotic maps have been used in real-time applications especially in secure multimedia data communication. For instance, in Al-Saidi et al. (2020), a new hyperchaotic map is designed for a secure data communication and successfully implemented on a digital hardware for real-time message data transmission. In another study presented by Ogras and Türk in 2017, the hardware simulation of the chaotic Cubic map was successfully applied in the FPGA environment. In short, these studies show that existing and improved chaotic maps can be successfully implemented in a real-time hardware environment.

In this paper, an effective and secure color image encryption scheme is proposed. Proposed algorithm involves permutation process of matrix scrambling in confusion stage and two mixing operations in diffusion stage. Mixing operation is designed such a current cipher pixel is dependent the previous one which accelerates the overall diffusion effect in the algorithm. Depending on the chaotic control bit series, the structure of the encryption algorithm used in the diffusion process also changes. This property offers a stronger and more secure diffusion effect to encryption. The scrambling operation used in the proposed scheme is a changeable matrix based permutation of all pixel coordinates. This operation is easy and simple which leads to increase computational speed of the algorithm. The proposed algorithm has an iteration structure for diffusion stage which enhances the security of the whole cryptosystem. For a secure encryption algorithm, key generator should be stochastic and supposed to yield uniform output which has sufficient randomness. SINCU system is designed to provide these properties well in this study.

The statistical and differential analyses performed in this study are provided in computer environment with MATLAB software. Some important analysis results are also compared with AES algorithm that is widely used in the field of electronic data encryption. In addition, the major security analysis result of the proposed algorithm is also compared with a similar study that is presented recently in image encryption field. The rest of the paper is organized as follows: Section 2 gives a brief overview of the Sine map, Cubic map and chaotic Logistic map. Section 3 introduces a hybrid chaotic map with its statistical analysis. Then, the proposed color image encryption algorithm is given in detail under Section 4. Security analyses and performance evaluation of the proposed algorithm have been given in Section 5. Finally, the conclusion will be discussed in Section 6.

2. Standard chaotic maps

2.1. Sine map
Sine map is one of the simplest discrete systems that exhibit chaos and defined by

\[ x_{n+1} = K \sin(\pi x_n) \]  

(1)

where \( K \) is a control parameter and has a range of \( 0 < K \leq 1 \). Here, \( x_n \) refers the state of the system with \( x_n \in (0, 1) \). When \( K = 1 \), then the map demonstrates perfect chaotic behavior in which the output is not periodic, non-convergent and very sensitive to initial value \( x_0 \).

2.2. Cubic map
Cubic map is a one-dimensional map that demonstrates chaos and having an iterated equation as in Equation (2).

\[ x_{n+1} = a.x_n(1 - x_n^2) \]  

(2)
Here, $a$ refers a control parameter of the map and is limited to 3. If $a$ is bigger than 2.3, then $x_n$ values spread from 0 to 1 and occur unpredictably. In this case, the map has pseudo-random output with sufficient uncertainty.

### 2.3. Logistic map

Logistic map is one of the well-known and probably the most frequently used chaotic system in the field where the concept of chaos is utilized. The map is defined by

$$x_{n+1} = r x_n (1 - x_n) \quad (3)$$

where $r$ refers the control parameter of the map and has a real value satisfying $0 < r \leq 4$. When $r$ is between 3.57 and 4, then the map is in chaos state where $x_n$ series have chaotic properties showing non periodicity and sensitivity to initial and system parameter.

### 3. Designing a hybrid chaotic map

Many of the standard chaotic maps have disadvantages of low level complexity, limited system parameters and small Lyapunov value which shows the degree of sensitivity for a dynamical system (Hathal et al., 2014). These shortcomings negatively affect the system security where such maps are used, as well as the cryptographic usability of the yielded key from the maps. A chaotic system intended to be used as a key generator in a cryptographic algorithm is expected to generate random sequences with the greatest uncertainty possible. Furthermore, the entropy produced by the chaotic system must provide the necessary confusion and diffusion in the encryption algorithm used. Basically, the unpredictable and random-like behavior of the chaotic systems has contributed to the use of these systems in the design of cryptographic algorithms (Ahmad & Hwang, 2015). In this paper, firstly, a new discrete system with a higher degree of chaos and better complex behavior has been designed for generating encryption keys to be used in the proposed algorithm. This hybrid chaotic model uses two well-known different chaotic maps in a cascade form and is utilized as a key generator in the proposed encryption algorithm. The hybrid map is modeled by coupling Sine and Cubic maps, namely SINCU which is defined in Equation (4).

$$x_{n+1} = K \sin(\pi(a x_n (1 - x_n^2))) \quad (4)$$

Now, SINCU has two independent system parameters and an initial value. Furthermore, SINCU has an extra key parameter in its mathematical equation that provides larger key space which leads to improve the security of the encryption algorithm. When considering the sensitivity of the system parameters on output, the more system parameters mean the more different output data. This feature will also help the encryption algorithm against brute-force cryptographic attack. Sine map and Cubic map are effectively coupled together resulting greater complexity that produces more complex behaviors, better randomness and uncertainty. In order to prove the superiority of the hybrid model, Sine map, Cubic map and hybrid one are compared in terms of statistical analysis such as chaotic trajectory, Lyapunov value and uncertainty. To perform performance comparison, the systems parameters for all chaotic maps are selected as $K = 1$ and $a = 3$ with the same initial value of $x_0 = 0.123$.

### 3.1. Chaotic trajectory

Chaotic trajectory can be defined as a behavior movement over time with a specified initial value for a dynamical system. Since the chaotic systems exhibit aperiodic and random behavior, the trajectory of these systems is never in the form of repetitive curve. Thus, chaotic trajectory can be used to determine the degree of randomness for an output sequence of any chaotic system. If a trajectory of a system can cover a large area in phase space, then this system is more complex and shows better randomness. The trajectories in phase space for three chaotic maps are shown in Figure 1. According to the Figure 1 results, it is clear that the trajectory of SINCU map gets larger
area than the other two maps. Therefore, SINCU map can produce much better output sequences in terms of randomness.

3.2. Lyapunov analysis
Lyapunov value refers to a degree of diverging for very close trajectories in a dynamical system. Hence, Lyapunov value can be used as a measure of a system’s sensitivity to changes in its initial condition. It is defined in Equation (5).

\[ \lambda = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln|f'(x_i)| \]  

(5)

\( \lambda \) indicates Lyapunov value and if this value is positive then the system is chaotic. Furthermore, bigger \( \lambda \) describes much more complicated behavior in the system, hence better performance of the chaotic behavior (Moysis et al., 2020). Lyapunov analyses for all chaotic maps are shown in Figure 2.

From the Lyapunov analysis, one can see that the largest Lyapunov values for Sine map is less than 1 and it is 0.6982. The maximum \( \lambda \) for Cubic map is around 1 and its value is 1.0977. On the other hand, the maximum \( \lambda \) for the SINCU map is 2.5729, which is significantly greater that the results of other two maps analysed. Thus, SINCU has better mixing property and chaotic performance than others. Furthermore, Cubic map and Sine map have a finite range of control parameter such as maximum limited value of \( K = 1 \) for Sine map and \( a = 3 \) for Cubic map. On the other hand, SINCU has an infinite range for its control parameter that leads larger key space as a key generator.
3.3. Uncertainty analysis

In this section, the entropy values for all the maps are calculated to perform uncertainty analysis. Information entropy, shortly entropy defines uncertainty of a specified random sequence (Yasser et al., 2020) and it is determined by

\[
Ent = - \sum_{i=1}^{N} p(x_i) \log_2 p(x_i)
\]  

(6)

where \( p(x_i) \) shows the probability of \( x_i \). For example, suppose a uniform bitstream as \( x = \{0, 1, 0, 1\} \) with equal probability of ‘0’ and ‘1’, then the entropy for this sequence is 1, which is the maximum result. Big entropy value indicates uniform distribution and great uncertainty in a sequence as well as resists entropy attacks (N. R. Zhou et al., 2015). In order to perform uncertainty analysis, the output of the all chaotic maps should be converted to serial bitstream containing 0 and 1 values. To do this, Equation (7) is used.

\[
b_n = \begin{cases} 
1 & x_n \geq \text{Threshold} \\
0 & x_n < \text{Threshold} 
\end{cases}
\]  

(7)

Since Logistic map, Cubic map and Sine map have an output of between 0 and 1, threshold level is selected as 0.5 to get sequential chaotic series. On the other hand, SINCU map provides output between -1 and 1 if its control parameter is above 2.598. Hence, threshold level can be 0 for SINCU map to perform the analysis. As a result, the entropy values of the chaotic series from the all chaotic maps with same initial value are calculated and given in Table 1. Number of iteration is selected as 1 million for the uncertainty analysis.
According to the entropy results, it is the SINCU map that is closest to 1. This means that SINCU has maximum uncertainty and unpredictability of all maps analyzed. From the all statistical analyses, it can be concluded that the new hybrid chaotic system has a potential to be used as a key generator in the proposed algorithm. Nevertheless, in a good cryptographic algorithm, encryption keys and cipher data are well random. Therefore, randomness degree of the output of the SINCU map must be evaluated before being used in the proposed image encryption algorithm.

3.4. Randomness test
Randomness means the lack of predictability or incomprehensible pattern in a sequence of data. NIST (National Institute of Standards and Technology) standard is used to evaluate the degree of randomness of the outputs. NIST consists of fifteen tests (Rukhin et al., 2001) and each test produces a p-value which is a real number in [0, 1]. If p-value is greater than a predefined threshold, called significance level (α = 0.01), then the statistical test is passed successfully and the generator is considered as random with 99% confidence. It is required 1,000,000 bits to perform NIST and the results are given in Table 2. To obtain sequential bit streams, the transformation method in Equation 7 is applied to the SINCU map.

### Table 1. Results of the uncertainty analysis

| Chaotic Map   | Control Parameter | # of “0” | # of “1” | Entropy       |
|---------------|-------------------|----------|----------|---------------|
| Logistic      | \( r = 4 \)       | 499,373  | 500,627  | 0.999998865   |
| Cubic         | \( \sigma = 2.597 \) | 502,231  | 497,769  | 0.999985638   |
| Sine          | \( K = 0.995 \)   | 505,883  | 494,117  | 0.999900135   |
| SINCU         | \( 8.934 \) (\( K = 0.995 \)) | 500,431  | 499,569  | 0.999999464   |

### Table 2. Results of the NIST

| Test name                  | p-value | Result   |
|---------------------------|---------|----------|
| Frequency                 | 0.9362  | Success  |
| Block frequency           | 0.2736  | Success  |
| Runs                      | 0.1597  | Success  |
| Long runs of ones         | 0.1484  | Success  |
| Rank                      | 0.6484  | Success  |
| Spectral DFT              | 0.3684  | Success  |
| Non-overlapping templates | 0.9320  | Success  |
| Overlapping templates     | 0.8690  | Success  |
| Universal (L = 7; Q = 1280) | 0.3369 | Success  |
| Linear complexity         | 0.0513  | Success  |
| Serial-1 (m = 5)          | 0.9486  | Success  |
| Serial-2 (m = 5)          | 0.9667  | Success  |
| Approximate entropy       | 0.8972  | Success  |
| Cumulative sums forward   | 0.5753  | Success  |
| Cumulative sums reverse   | 0.6476  | Success  |
| Random excursions (x = +1) | 0.2995 | Success  |
| Random excursions variant (x = -1) | 0.6508 | Success  |
According to the results, it can be concluded that SINCU map is quite stochastic and generates sequences which has sufficient randomness. Hence, it can be used as a key generator in the proposed encryption scheme.

4. The proposed color image encryption scheme

Chaos-based image encryption systems are generally composed of two stages: permutation of pixel positions by confusion process and modification of pixel gray values by diffusion process (Ye, 2011). In traditional chaos-based image cryptosystems, permutation is usually chosen as a first process and then confusion is performed to complete the encryption. In the proposed algorithm, confusion and diffusion stages are carried out one after the other. Both processes are simple and fast so the encryption time will be reduced. To increase the security of the cryptosystem, diffusion step can be iterated several times. However, the numerical results show that the high security and performance of the proposed image encryption algorithm can be achieved even in a single iteration. The architecture of the proposed algorithm is shown in Figure 3.

In the proposed scheme, a plain image can be a gray image or any component of a color image. If the control bit generated from the chaotic logistic system is ‘1’, the diffusion structure in Algorithm-1 will be used for encryption, otherwise the encryption will continue with Algorithm-2. If the image to be encrypted is in color, then the encryption structure presented in Figure 3 will also be implemented for the three components of the color image. Then, all encrypted components of the image are combined to obtain the ciphered form of the corresponding color image.

![Figure 3. The architecture of the proposed image encryption scheme.](https://example.com/figure3.png)
A 24-bit color image is an image consisting of three layers named Red, Green and Blue, where each pixel value is represented by 8-bit in the range [0,255]. Firstly, the RGB image is separated into Red, Green and Blue components before the encryption. Then each layer of the input image is permuted using matrix scrambling based permutation in confusion stage. In the rest of the section, confusion and diffusion stages are explained in detail.

4.1. Confusion stage
In any standard image, adjacent pixels have strong correlation and this correlation needs to significantly reduced or totally broken before the basic encryption. This may contributes much better cipher image at output. In the proposed algorithm, matrix scrambling method is used in the confusion stage to break strong correlations of the all adjacent pixels in the plain image. Here, the plain image defines a source image which is a layer of any color image or it can be a straight gray image. In mathematics, permutation refers the process of changing the linear order of an ordered sequence. In this study, permutation is used as the replacement of all pixel positions to their new positions with a user defined matrix-based algorithm. Thus, all pixel positions in a plain image are changed with permutation and as a result, the strong correlations between all adjacent pixels having close values are effectively broken. In the next section, matrix based scrambling process is discussed in detail.

4.2. Matrix-based scrambling
Matrix-based scrambling is a transformation method that can be generalized in Equation (8).

\[ \tilde{p}_k = A \tilde{p}_{k-1} \mod N \]  \hspace{1cm} (8)

In Equation (8), \( A \) is a scrambling matrix with a size of \( n \times n \) and \( k \) is a positive integer that refers scrambling times of the image. All the elements of \( A \) are integers such that \( \det(A) \neq 0 \). A matrix-based scrambling transformation can be given in Equation (9).

\[ \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \mod N \]  \hspace{1cm} (9)

where \((x_n, y_n) \in [0, N-1] \times [0, N-1]\) is the pixel position of the plain image with \( N \times N \) in size and \((x_{n+1}, y_{n+1})\) is the new pixel position for the permuted image. In order to make the scrambling reversible, \( \det(A) = a_{11}a_{22} - a_{12}a_{21} \neq \pm 1 \). In this study, \( A \) matrix in Equation (10) is used as scrambling operator for the plain image to be permuted.

\[ A = \begin{pmatrix} p & p^2 + 1 \\ p^3 - 1 & p \end{pmatrix} \]  \hspace{1cm} (10)

where \( p \) is a positive integer and at all \( p \) values, \( \det(A) = 1 \) that makes the scrambling operation reversible. The inverse scrambling matrix is defined in Equation (11).

\[ A^{-1} = \begin{pmatrix} p^3 & p^2 - 1 \\ 1 - p^2 & p \end{pmatrix} \]  \hspace{1cm} (11)

Using the inverse matrix of \( A \), it is possible to get back from permuted image to the original one. The \( p \) value used here can also be considered as a coefficient that varies depending on the user preference and determines the degree of permutation for an image. In addition, representing the elements in the \( A \) matrix as the square and the cube of the \( p \) parameter will significantly increase the difference in value between the elements, which effectively changes the pixel positions even in small iterations. Moreover, there will be no need to make repetitive iteration. For instance, Figure 4 shows “Lena.jpg” test image and its corresponding permuted images under a single iteration for different \( p \) values. Here, the same \( p \) parameter is preferred for each component of the plain image to be permuted.
By choosing a different $p$ value for each component of the Lena image, a completely meaningless permuted image can also be obtained as in Figure 5. Here, $p$ values are used as 10, 15 and 20 for the Red, Green and Blue components, respectively for just one iteration.

Table 3 shows the average correlation coefficients results of each layer for all directions as Horizontal (H), Vertical (V) and Diagonal (D) between original “Lena” image and permuted “Lena” image in Figure 5. The average correlation coefficient between adjacent pixels of “Lena” and its permuted is listed in Table 4.

Negative value of correlation means that for two variables, an increase in one of them is associated with a decrease in the other. According to the Tables 3 and 4 results, the strong correlations of adjacent pixels are decreased significantly for all directions. This result confirms an effective permutation has taken place in confusion stage.
This encryption round describes the process of changing each pixel value of the original image to a new value. This change is achieved using a secret key and the parameters of the SINCU map. Each component of the color image, such as Red, Green, and Blue, is used to generate a decimal value between 0 and 255. To mix the pixel value with a secret key, the key must be identical to the pixel value in order to change its value through an algorithm. Hence, Equation (12) is used at the output of SINCU for the key generation.

\[
\text{key} = \text{mod(round}(x_n,10^9), 256)
\]  

(12)

Multiplying the SINCU output by $10^9$ will create an precision up to 9 digits for the key. If a small change of initial value or system parameters in SINCU map, then corresponding key is completely changed due to the chaos phenomenon. For instance, Table 5 shows the correlation coefficient value between two different keys generated with a very small initial value in SINCU map.

Table 5 result confirms that the generated encryption key from the SINCU map is highly sensitive to the initial value and system parameters. This also suggests that the encrypted data will also be extremely sensitive to such parameters. Hence, the proposed algorithm will effectively resist differential attacks. In order to increase the strength of the encryption, the proposed algorithm uses two mixing operations depend on the control bit series generated from the chaotic Logistic system.

\[
K_i = 0.999999999 vs K_2 = 0.999999998
\]

\[
\sigma_1 = 2.299999999 vs \sigma_2 = 2.3
\]
map in diffusion stage. In addition, since the initial value of the Logistic map depends on the initial value of the SINCU map and all system parameters as in Equation (13), the small change in these parameters changes the encryption keys as well as the mixing process defined in Equation (14).

\[ x_{0, \text{Log}} = (x_{0, \text{SINCU}} + K + a + r) \mod 1 \]  

(13)

According to the Table 1 results, generated control bit series has uniform distribution so the probability of one of these two mixing operation is approximately 50 percent. The length of the bitstream generated is equal to the number of pixels in the plain image. Mixing operations for different control bits are shown in Equation (14).

\[ c(i) = \begin{cases} k(i) \oplus (p(i) + (c(i - 1) + k(i))) \mod 256, & \text{control bit } = '1' \\ k(i) \oplus (p(i) - (c(i - 1) + k(i))) \mod 256, & \text{control bit } = '0' \end{cases} \]  

(14)

Here, \( p(i), c(i), c(i - 1) \) and \( k(i) \) represent current plain pixel, output cipher pixel, previous cipher pixel and encryption key, respectively. Modular operation provides the cipher data to the range of \([0,255]\). Such a mixing operation is very efficient because simple modular arithmetic and logical operations can be performed in high speed. Furthermore, the current cipher pixel depends on the previous one that reflects the diffusion to whole cipher image. In this study, the first cipher value is encoded the first pixel data of the permuted image. However, it can also be used as a secret key parameter for the algorithm. The proposed encryption algorithm has a symmetric structure that means identical key has to be used for decryption process. The decryption is a reverse diffusion algorithm that is defined in Equation (15).

\[ p(i) = \begin{cases} (k(i) \oplus c(i)) - (c(i - 1) + k(i)) \mod 256, & \text{control bit } = '1' \\ (k(i) \oplus c(i)) + (c(i - 1) + k(i)) \mod 256, & \text{control bit } = '0' \end{cases} \]  

(15)

For the decryption algorithm, it is obvious that it cannot be decrypted successfully without knowing the encryption keys as well as the control bits. The confusion and diffusion processes complete the proposed image encryption algorithm. For example, “Baboon.jpg” image with a size of \(256 \times 256\) is encrypted for one iteration \(n = 1\) by the proposed algorithm with the key parameters of \(x_0 = 0.7285; \ a = 8.9340; \ K = 0.9987\) in SINCU map and \(x_0 = 0.6518; \ r = 3.9945\) in Logistic map for Red component of the plain image; for Green component it is used as \(x_0 = 0.2639; \ a = 13.5882; \ K = 0.9916\) in SINCU map and \(x_0 = 0.3407; \ r = 3.9991\) in Logistic map; for Green component \(x_0 = 0.8304; \ a = 29.2375; \ K = 0.9993\) in SINCU map and \(x_0 = 0.1168; \ r = 3.9982\) in Logistic map. The results are shown in Figure 6.

The performance of the proposed image encryption scheme has been also evaluated for different test images. In this sense, three different test images (Peppers, Landscape and

Figure 6. Results of the proposed encryption algorithm (a) Plain Baboon image (b) Encrypted Baboon image (c) Decrypted Baboon image.
5. Security and performance analyses

The key space size tells the total number of different keys used in a cryptosystem. To make brute-force attack infeasible, it should be larger than $2^{100}$ (Fu et al., 2018) for a good encryption algorithm and this criterion is referred to as conditionally secure in cryptology. The computational precision for 64-bit double type gives 53 bits (Fu et al., 2018). In the proposed algorithm, key parameters as $x_0, K, a, r$ are floating-point values. Even different matrix scrambling parameters for each layer and number of iteration are ignored, the total number of possible secret key is approximately,

$$key = 2^{53+4} = 2^{212}$$

which is sufficiently large to resist brute-force attack.

5.1. Key sensitivity analysis

Key sensitivity analysis can be examined for two different situations: (i) if slightly different keys are used to encrypt the identical images, then completely different cipher images should be produced; (ii) if a very small difference exists in decryption key, then the cipher image should not be decrypted correctly. For the first case, a test plain image Lena is encrypted with a randomly chosen Key-1 as $x_0 = 0.123456; a = 8.987654; K = 0.999888; r = 3.999999$ in one iteration. Then a very small change of one in a million is applied to the one of the parameters while others remain same and then repeats the encryption using the same plain image. Then, correlation coefficients for each component of the corresponding cipher images are computed and compared.

![Figure 7. Results of the encryption (a) “Peppers” image (b) “Landscape” image (c) “Airplane” image (d) Cipher “Peppers” image (e) Cipher “Landscape” image (f) Cipher “Airplane” image.](image-url)
with other two results in Table 6. Here, Reference-A refers the (Murillo-Escobar et al., 2015) and Reference-B refers the study presented by (Patidar et al., 2011).

For the second case, another test plain image Baboon is encrypted using Key-1. Then the decryption processes are performed with four slightly different keys and Key-1. The visual results are shown in Figure 8.

According to the key sensitivity analyses, it is clear that if a slightly different key is used in decryption process, then the encrypted image could not be decrypted correctly. Hence, the proposed image cryptosystem is quite sensitive to all key parameters.

**Table 6. Results for key sensitivity analysis-I**

| Key     | Components | Correlation coefficients |         |         |         |
|---------|------------|--------------------------|---------|---------|---------|
|         |            | Proposed                | Reference-A | Reference-B |
| Key-1 vs Key-2 | R       | -0.001097               | -0.1281   | 0.0039  |
|         | G         | -0.000085               | 0.0683    | 0.0048  |
|         | B         | 0.004075                | 0.0529    | 0.0072  |
| Key-1 vs Key-3 | R       | 0.006985                | -0.0361   | 0.0096  |
|         | G         | -0.000448               | 0.0856    | -0.0040 |
|         | B         | 0.005098                | -0.0155   | 0.0018  |
| Key-1 vs Key-4 | R       | 0.000848                | —         | 0.0025  |
|         | G         | 0.001113                | —         | -0.0017 |
|         | B         | -0.004508               | —         | 0.0013  |
| Key-1 vs Key-5 | R       | 0.002215                | —         | 0.0083  |
|         | G         | 0.001570                | —         | 0.0018  |
|         | B         | 0.001914                | —         | 0.0011  |

**Figure 8. Results for key sensitivity analysis-II**

(a) Encrypted Baboon image with Key-1
(b) Wrong decrypted image with a slightly difference of $x_0$
(c) Wrong decrypted image with a slightly difference of $K$
(d) Wrong decrypted image with a slightly difference of $a$
(e) Wrong decrypted image with a slightly difference of $r$
(f) Correct decrypted image with Key-1.
5.2. Histogram analysis

In an encrypted image, equal probability distribution of cipher pixels creates a uniform histogram which is more robust against statistical attacks (Khan et al., 2020; H. Zhu et al., 2013). Hence, the ideal histogram of an encrypted image should be fairly uniform and very different from that of the plain image. For instance, the histograms of all components of the Tiger image and corresponding cipher one are shown in Figures 9 and 10, respectively. The histogram results show that the cipher image is significantly different from that of the plain image and uniformly distributed over all possible intensity values.

5.3. Mean square error (MSE) and Peak signal-to-noise ratio (PSNR) analyses

A cipher image must significantly differ from its original state. Mean square error (MSE) defines the cumulative squared error between original and corresponding cipher images (Ahmad and Hwang, 2016) and it is given by,

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (C(i,j) - P(i,j))^2$$

where $P(i, j)$ is the pixel value of the original image and $C(i, j)$ is the encrypted pixel value at location $(i, j)$ in the cipher mage. The MSE value can be considered as a criterion for the encryption level of a cryptosystem. Larger the MSE value means the better encryption security. PSNR analysis is a method that refers encryption quality level and the greater this value, the closer the encrypted image to the original image (Ahmad and Hwang, 2013). Thus, a smaller PSNR value means better encryption for a cryptosystem. PSNR is defined as in Equation (18).

$$PSNR = 20 \log_{10} \left[ \frac{P_{max}}{\sqrt{MSE}} \right]$$

Here, $P_{max}$ is the maximum value that a pixel can get in a gray image. In a presented scientific study (Norouzi et al., 2013), it was stated that the MSE value should be greater than 9,555 and
PSNR value should be smaller than 8.3875 as an encryption security criterion. Different test images with different sizes have been used for MSE and PSNR analyses and the results are listed in Table 7.

The large MSE value obtained from the results proves that there is a significant difference between the plaintext image and the corresponding cipher image. The results show that the effectiveness of the proposed method is evident by bigger MSE values and lower values of PSNR and it also meets the security criterion.

Table 7. Results for MSE and PSNR analyses

| Test image     | Components | MSE | PSNR (dB) |
|----------------|------------|-----|-----------|
| Lena (256 × 256) | R          | 10,672 | 7.8479   |
|                | G          | 8,957  | 8.6088   |
|                | B          | 7,156  | 9.5839   |
| Baboon (256 × 256) | R          | 9,735  | 8.2473   |
|                | G          | 7,215  | 9.5482   |
|                | B          | 9,192  | 8.4965   |
| Peppers (256 × 256) | R          | 9,611  | 8.3031   |
|                | G          | 10,878 | 7.7652   |
|                | B          | 10,983 | 7.7232   |
| Landscape (512 × 512) | R          | 7,955  | 9.1242   |
|                | G          | 8,470  | 8.8519   |
|                | B          | 11,284 | 7.6059   |
| Airplane (512 × 512) | R          | 9,861  | 8.1911   |
|                | G          | 10,493 | 7.9214   |
|                | B          | 10,387 | 7.9656   |
| Tiger (1024 × 1024) | R          | 16,014 | 6.0856   |
|                | G          | 8,464  | 8.8547   |
|                | B          | 18,355 | 5.4931   |
Table 8. Results for entropy analysis

| Test images                  | Proposed cryptosystem |
|------------------------------|-----------------------|
|                              | R         | G         | B         |
| Flower (128 × 128) Cipher image | 7.872094 | 7.46514  | 6.744829  |
| Lena (256 × 256) Cipher image | 7.599532 | 7.490264 | 7.087746  |
| Baboon (512 × 512) Cipher image | 7.325257 | 7.499966 | 7.612827  |
| Cat (1024 × 1024) Cipher image | 7.347401 | 7.999862 | 6.816230  |
| Tiger (2048 × 2048) Cipher image | 7.724188 | 7.999934 | 7.522007  |

5.4. Entropy analysis

Entropy is a measure of uncertainty associated with a random series and determines unpredictability of the series. Generally, the more uncertain or random source is, the more entropy it will contain (H. Zhu et al., 2013). Maximum entropy is achieved in the case of uniform probability distribution. The entropy of an information source with a length of N is determined in Equation (6). Five color test images with different sizes are encrypted using the proposed scheme. Table 8 shows the entropy results of the cipher images.

It is obvious that the entropies of the cipher images are very close to ideal value which means that the proposed encryption algorithm yields high unpredictability at output. Table 8 also shows that as the size of the plain image increases, the entropy value for the corresponding cipher image also increases. Some important analysis of the proposed encryption algorithm has also been compared with AES algorithm, which is frequently used today for data encryption. AES is a symmetric algorithm chosen by the U.S. government to protect classified information and can be implemented in software and hardware throughout the world. Entropy analysis results for both AES in (Arab et al., 2019) and proposed algorithm for three test images with same sizes is given in Table 9. Test images are grayscale images for entropy comparison.

According to the Table 9 results, the proposed algorithm is better at entropy comparison. The entropy results are also compared to a chaos-based color image encryption algorithm, Reference-C of (Fu et al., 2018) that has been recently presented in this field. Entropy results for Reference-C and the proposed scheme are listed in Table 10. The test images (Lena, Baboon and Pepper) used for entropy comparison are 512 × 512 in size.

5.5. Correlation analysis

A meaningful image has a property of strong correlation between all adjacent pixels since the adjacent pixels have close values. A good image cipher produces low pixel correlation of adjacent pixels. To evaluate the correlation coefficients for all the pairs of the adjacent pixels, Equation (19) is used for the analysis.

Table 9. Entropy comparison between AES and the proposed algorithm

| Entropy | Lena     | Cameraman | Pepper    |
|---------|----------|-----------|-----------|
| AES     | 7.8693   | 7.8761    | 7.8734    |
| Proposed algorithm | 7.9971   | 7.9973    | 7.9974    |
\[
cc = \frac{\sum_{i=1}^{N} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\left(\sum_{i=1}^{N} (x_i - \bar{x})^2\right)\left(\sum_{i=1}^{N} (y_i - \bar{y})^2\right)}}
\] (19)

Here, \((\bar{x}, \bar{y})\) are mean values defined as \(\bar{x} = \frac{1}{N} \sum_{i=1}^{N} x_i\) and \(\bar{y} = \frac{1}{N} \sum_{i=1}^{N} y_i\). \(N\) shows the total number of pairs of adjacent pixels. The results of the correlation coefficients for diagonally adjacent pixels for three test images and their corresponding cipher images are given in Table 11.

It is clear that the proposed scheme significantly reduces the correlation between adjacent pixels of the plain image. Correlation coefficients of adjacent pixels in cipher images for both AES and Reference-C and the proposed algorithm are performed for three images with same size. The result is given in Table 12.

### Table 10. Entropy comparison between Reference-C and the proposed algorithm

| Entropy          | Test images |
|------------------|-------------|
|                  | Lena        | Baboon      | Pepper      |
| Reference-C      | 7.999772    | 7.999778    | 7.999788    |
| Proposed Algorithm | 7.999814    | 7.999680    | 7.999767    |

### Table 11. Correlation coefficients analysis

| Color image | Component | Plain image | Cipher image |
|-------------|-----------|-------------|--------------|
| Flower      | R         | 0.9465      | -0.0660      |
|             | G         | 0.9238      | -0.0275      |
|             | B         | 0.8783      | -0.0453      |
| Lena        | R         | 0.9317      | 0.0528       |
|             | G         | 0.8960      | -0.0106      |
|             | B         | 0.9054      | -0.0453      |
| Baboon      | R         | 0.9755      | -0.0109      |
|             | G         | 0.9601      | 0.0432       |
|             | B         | 0.9794      | 0.0437       |
| Cat         | R         | 0.9370      | 0.0083       |
|             | G         | 0.9158      | 0.0136       |
|             | B         | 0.9405      | -0.0391      |
| Tiger       | R         | 0.9610      | -0.0180      |
|             | G         | 0.9481      | 0.0581       |
|             | B         | 0.9563      | -0.0026      |

### Table 12. Correlation coefficients of adjacent pixels in cipher image

| Test image | Direction | AES       | Proposed Algorithm | Reference-C |
|------------|-----------|-----------|---------------------|-------------|
| Lena       | Horizontal| 0.2724    | 0.0261              | 0.0033      |
|            | Vertical  | 0.2681    | 0.0349              | 0.0155      |
|            | Diagonal  | 0.0765    | 0.0122              | 0.0158      |
| Cameraman  | Horizontal| 0.2729    | 0.0095              | —           |
|            | Vertical  | 0.2723    | -0.0813             | —           |
|            | Diagonal  | 0.0682    | -0.0474             | —           |
| Pepper     | Horizontal| 0.2704    | 0.0135              | 0.0133      |
|            | Vertical  | 0.2709    | -0.0023             | 0.0146      |
|            | Diagonal  | 0.0736    | -0.0075             | 0.0008      |
Figure 11 shows the diagonal correlation of the red component of the “Lena” image, where the graph has linear distribution due to the high correlation of adjacent pixels. On the other hand, Figure 11(d) shows correlation distribution of the corresponding component of the cipher image, where the graph has random distribution due to the low correlation. Hence, the proposed algorithm can resist statistical attacks.

5.6. Differential attack analysis

If a very small change in any key parameter in the algorithm changes the cipher image significantly, then the algorithm is resistant to differential attacks (Xu et al., 2015). Two common analysis, namely, NPCR (number of pixels change rate) and UACI (unified average changing intensity) are used to test the differential attack analysis. They are defined in Equation (20) and Equation (22), respectively.

\[
NPCR = \frac{1}{W \times H} \left[ \sum_{i=1}^{W} \sum_{j=1}^{H} D(i,j) \right] \times 100 \%
\]  

Equation (20)

where \( D(i,j) \) is defined as

\[
D(i,j) = \begin{cases} 
0, & \text{if } C_1(i,j) = C_2(i,j) \\
1, & \text{if } C_1(i,j) \neq C_2(i,j)
\end{cases}
\]  

Equation (21)

\[
UACI = \frac{1}{W \times H} \left[ \sum_{i=1}^{W} \sum_{j=1}^{H} \left| \frac{C_1(i,j) - C_2(i,j)}{255} \right| \right] \times 100 \%
\]  

Equation (22)

Here, \( W \) and \( H \) are the width and height of the cipher image and \( C_1, C_2 \) are the two cipher images corresponding to two plain images with a very small key parameter. NPCR measures how many pixels are different between \( C_1 \) and \( C_2 \) for the same plain image under a very small key parameter and UACI is used to measure the average intensity of differences between two images. In order resist differential attacks, the ideal values for NPCR and UACI should be 99.6% and 33.4%, respectively.
respectively (Fu et al., 2012). Lena test image, denoted by P is encrypted to C1 by the parameters of Key-1 with one iteration of encryption. Then, all system parameters as x₀, a, K and r are changed sequentially by one millionth using same plain image and encryption is repeated and results C₂. The numerical results of NPCR and UACI are listed in Table 13.

| Key Parameter | Test | NPCR (%) | UACI (%) |
|---------------|------|----------|----------|
| Δx₀ | NPCR (%) | 99.227 | 33.524 |
|       | UACI (%) | 99.224 | 33.389 |
| Δa  | NPCR (%) | 99.631 | 33.476 |
|       | UACI (%) | 99.625 | 33.574 |
| ΔK  | NPCR (%) | 99.618 | 33.326 |
|       | UACI (%) | 99.613 | 33.512 |
| Δr  | NPCR (%) | 99.591 | 33.456 |
|       | UACI (%) | 99.607 | 33.394 |
|       | Blue    | 99.218 | 33.569 |

It is obvious that both NPCR and UACI values are very close to their ideal values so the proposed scheme is highly sensitive at key parameters and has a good ability against differential attacks even one iteration of encryption. Results for differential attacks analysis of AES and proposed algorithm are given in Table 14.

Comparing NPCR and UACI values of the AES and proposed algorithm, it can be concluded that the security of the proposed algorithm against differential is more than AES one. NPCR and UACI values are also compared with the corresponding results of Reference-C for different iteration values between 1 and 4. In Reference-C, the authors obtained the relevant results by making a very small change in the plain image. The analysis results are listed in Tables 15 and 16.

5.7. Encryption and decryption speed analysis

In order to evaluate the running speed of the proposed cryptosystem, enough number of test images is encrypted 10 times by the proposed scheme. Then, the average encryption and decryption speed results are listed in Table 14.

| Algorithm | Test | Lena | Cameraman | Pepper |
|-----------|------|------|-----------|--------|
| AES       | NPCR (%) | 0.0778 | 0.0870 | 0.0885 |
|           | UACI (%) | 0.0093 | 0.0097 | 0.0101 |
| Proposed  | NPCR (%) | 99.601 | 99.586 | 99.627 |
|           | UACI (%) | 33.477 | 33.515 | 33.428 |

5.7.1. Comparison of encryption speed results

Table 15. NPCR and UACI results for Reference-C

| Test image | Test (%) | Number of iteration |
|------------|----------|---------------------|
|            |          | 1       | 2       | 3       | 4       |
| Lena       | NPCR     | 6.21    | 99.62   | 99.60   | 99.61   | 99.61   |
|            | UACI     | 2.08    | 33.46   | 33.48   | 33.44   | 33.44   |
| Baboon     | NPCR     | 90.90   | 99.61   | 99.60   | 99.60   | 99.60   |
|            | UACI     | 30.34   | 33.46   | 33.44   | 33.45   | 33.45   |
| Peppers    | NPCR     | 81.66   | 99.60   | 99.61   | 99.60   | 99.60   |
|            | UACI     | 27.34   | 33.44   | 33.45   | 33.46   | 33.46   |
Table 16. NPCR and UACI results for the proposed scheme

| Test image | Test (%) | Number of iteration |
|------------|----------|---------------------|
|            |          | 1                   | 2     | 3     | 4     |
| Lena       | NPCR     | 99.60 | 99.62 | 99.59 | 99.60 |
|            | UACI     | 33.47 | 33.42 | 33.45 | 33.46 |
| Baboon     | NPCR     | 99.62 | 99.61 | 99.61 | 99.60 |
|            | UACI     | 33.42 | 33.47 | 33.44 | 33.43 |
| Peppers    | NPCR     | 99.62 | 99.58 | 99.63 | 99.61 |
|            | UACI     | 33.42 | 33.43 | 33.46 | 33.41 |

Table 17. Speed performance analysis of the proposed scheme

| Color images | Encryption time (sec) | Decryption time (sec) | Encryption rate (Mbps) | Decryption rate (Mbps) |
|--------------|-----------------------|-----------------------|------------------------|------------------------|
| 128 × 128    | 0.0386                | 0.0413                | 10.18                  | 9.52                   |
| 256 × 256    | 0.1317                | 0.1640                | 11.94                  | 9.59                   |
| 512 × 512    | 0.5731                | 0.6582                | 9.71                   | 8.10                   |
| 1024 × 1024  | 2.5920                | 3.1065                |                        |                        |

decryption rate is calculated using Intel Core i7 3.4 GHz CPU with 4 GB RAM running on Windows 7 and MATLAB R2015a. The average execution time for speed analysis can be found in Table 17.

6. Conclusion

A fast and secure chaos based color image cryptosystem containing a new matrix scrambling method intended for confusion and a changeable encryption structure for diffusion is proposed in this paper. Using a simple but effective matrix scrambling operation in the confusion stage breaks the strong correlation of close pixels very well without iteration which reduces overall encryption time. The behavior of the newly chaotic model meets the requirements for sufficient randomness according to the NIST results and the encryption keys highly sensitive to the system parameters of the new map, hence the proposed algorithm has a good ability against differential attacks even one iteration of encryption. In addition, histogram and correlation coefficient analyses results show that the proposed encryption structure is resistant to statistical attacks. The results of NPCR and UACI show that the proposed encryption scheme takes only one round of iteration to achieve sufficient diffusion effect. Both theoretical and simulation results are satisfactory when compared with standard AES algorithm. Important security analyses have been carried out in detail to evaluate security level of the proposed algorithm and it is also concluded that the proposed scheme is highly secure thanks to its large key space, high sensitivity to the encryption keys. The practical usage of the proposed algorithm with the developed chaotic map is possible direction for future works.

Funding

The author received no direct funding for this research.

Author details

Hidayet Ogras1
E-mail: hidayet.ogras@batman.edu.tr
1 Electronic Communication Technology, Batman University, Batman, Turkey.

Citation information

Cite this article as: An efficient color image encryption scheme based on a matrix scrambling method and a new hybrid chaotic map, Hidayet Ogras, Cogent Engineering (2021), 8: 1940638.

References

Addabbo, T., Fort, A., Rocchi, S., & Vignoli, V. (2009). Chaos based generation of true random bits. In Kocarev L., Gallas Z., Lian S. (eds), Intelligent computing based on Chaos (pp. 355–377). Springer.

Ahmad, J., & Hwang, S. O. (2015). Chaos-based diffusion for highly autocorrelated data in encryption algorithms. Nonlinear Dynamics, 82(4), 1839–1850. https://doi.org/10.1007/s11071-015-2281-0

Ahmad, J., & Hwang, S. O. (2016). A secure image encryption scheme based on chaotic maps and affine transformation. Multimedia Tools and Applications, 75(21), 13951–13976. https://doi.org/10.1007/s11042-015-2973-y
Alowida, M., Samsudin, A., Teh, J. S., & Alkhawaldeh, R. S. (2019). A new hybrid digital chaotic system with applications in image encryption. Signal Processing, 160, 45–58. https://doi.org/10.1016/j.sigpro.2019.02.016

Alhadjawi, H. S., Zalikpil, M. F., Ismail, S. M., & Lambić, D. (2019). Designing a pseudorandom bit generator based on LFSRs and a discrete chaotic map. Cryptologia, 43(3), 190–211. https://doi.org/10.1080/01611194.2018.1548390

Ali-Saidi, N. M., Younus, D., Netiz, H. K., Ariffin, M. R., Asbullah, M. A., & Mohad, Z. (2020). A new hyperchaotic map for a secure communication scheme with an experimental realization. Symmetry, 12(11), 1–17. https://doi.org/10.3390/sym12111881

An, X. L., Yu, J. N., Li, Y. Z., Chu, Y. D., Zhang, J. G., & Li, X. F. (2011). Design of a new multistage chaos synchronized system for secure communications and study on noise perturbation. Mathematical and Computer Modelling, 54(1–2), 7–18. https://doi.org/10.1016/j.mcm.2011.01.020

Arab, A., Rostami, M. J., & Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. The Journal of Supercomputing, 75(10), 6663–6682. https://doi.org/10.1007/s11227-019-02087-7

Battikh, D., El Assad, S., Bakhache, B., Déforges, O., & Khlil, M. (2014). Chaos-based spatial steganography system for images. International Journal of Chaotic Computing, 3(1), 36–44. https://doi.org/10.20533/ijcc.20643359.2014.0005

Bilal, M., Irtiaz, S., Abdul, W., Ghouzali, S., & Asif, S. (2014). Chaos based Zero-steganography algorithm. Multimedia Tools and Applications, 72(2), 1073–1092. https://doi.org/10.1007/s11042-013-1415-y

Chen, J. X., Zhu, Z. L., Fu, C., Yu, H., & Zhang, L. B. (2015). A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Communications in Nonlinear Science & Numerical Simulation, 20(3), 846–860. https://doi.org/10.1016/j.cnsns.2014.06.032

Chen, Q., Ren, X., & No, J. (2015). Robust finite-time chaos synchronization of uncertain permanent magnet synchronous motors. ISA transactions, 58, 262–269. https://doi.org/10.1016/j.isatra.2015.07.005

Eisenbraut, M., Fanganniello, R. D., Gryzowski, J. M. V., Soriano, D. C., Attux, R., Batista, A. M. A., Maccio, E. E. N., Monteiro, L. H. A., Roman, J. M. T., Sayama, R., & Yoneyama, T. (2012). Chaos-based communication systems in non-ideal channels. Communications in Nonlinear Science & Numerical Simulation, 17(12), 4707–4718. https://doi.org/10.1016/j.cnsns.2011.05.030

Fan, H., & Li, M. (2017). Cryptanalysis and improvement of chaos-based image encryption scheme with circular-inter-intra-pixels bit-level permutation. Mathematical Problems in Engineering, 2017, 1–11. https://doi.org/10.1155/2017/8124912

Fu, C., Chen, J. J., Zou, H., Meng, W. H., Zhan, Y. F., & Yu, Y. W. (2012). A chaos-based digital image encryption scheme with an improved diffusion strategy. Optics Express, 20(3), 2363–2378. https://doi.org/10.1364/OE.20.002363

Fu, C., Zhang, G. Y., Zhu, M., Chen, Z., & Lei, W. M. (2018). A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy. Security and Communication Networks, 2018, 1–13. https://doi.org/10.1155/2018/2708512

Ghasemi, M., Ghavidel, S., Aghaei, J., Giltizadeh, M., & Falah, H. (2014). Application of chaos-based chaotic invasive weed optimization techniques for environmental OPF problems in the power system. Chaos, Solitons, and Fractals, 69, 271–284. https://doi.org/10.1016/j.chaos.2014.10.007

Ginarsa, I. M., Soeprijanto, A., & Purnomo, M. H. (2013). Controlling chaos and voltage collapse using an ANFIS-based composite controller-static var compensator in power systems. International Journal of Electrical Power & Energy Systems, 46, 79–88. https://doi.org/10.1016/j.ijepes.2012.10.005

Gong, L., Wu, R., & Zhou, N. (2020). A New 4D Chaotic system with coexisting hidden chaotic attractors. International Journal of Bifurcation and Chaos, 30 (10), 2050142. https://doi.org/10.1142/S0218127420501424

Hathol, H. M., Abdulhussein, R. A., & Ibrahim, S. K. (2014). Lyapunov exponent testing for AWGN Generator system. Communications and Network, 6(04), 201. https://doi.org/10.4236/cn.2014.64022

Hu, J., Mo, J., & Lin, J. (2010). Chaos synchronization and communication of mutual coupling lasers ring based on incoherent injection. Optik, 121(24), 2227–2229. https://doi.org/10.1016/j.ijleo.2009.09.006

Jiang, N., Pan, W., Yan, L., Luo, B., Xiang, S., Yang, L., & Li, N. (2013). Chaos synchronization and communication in multi-Sunflower delayed concealed semiconductor lasers driven by a third laser. IEEE Journal of Selected Topics in Quantum Electronics, 17(5), 1220–1227. https://doi.org/10.1109/JSTQE.2011.210638

Kaddoura, G., Coulon, M., Roviras, D., & Chargé, P. (2010). Theoretical performance for asynchronous multi-user chaos-based communication systems on fading channels. Signal Processing, 90(11), 2923–2933. https://doi.org/10.1016/j.sigpro.2010.04.013

Kang, Z., Sun, J., Ma, L., Qi, Y., & Jian, S. (2014). Multimode synchronization of chaotic semiconductor ring laser and its potential in chaos communication. IEEE Journal of Quantum Electronics, 50(3), 148–157. https://doi.org/10.1109/JQE.2014.2299593

Kar, N., Mandal, K., & Bhattacharya, B. (2018). Improved chaos-based video steganography using DNA alphabets. ICT Express, 4(1), 6–13. https://doi.org/10.1016/j.ictex.2018.01.003

Khan, J. S., Bouilla, W., Ahmadian, J., Rubaiiee, S., Rehman, A. U., Alrobaei, R., & Buchanan, W. J. (2020). DNA and plaintext dependent chaotic visual selective image encryption. IEEE Access, 8, 159732–159744. https://doi.org/10.1109/ACCESS.2020.3020917

Liu, Q., Li, P. Y., Zhang, M. C., Sui, Y. X., & Yang, H. J. (2015). A novel second generation algorithm based on chaos maps with Markov properties. Communications in Nonlinear Science & Numerical Simulation, 20(2), 506–515. https://doi.org/10.1016/j.cnsns.2014.06.005

Mastan, J. K. M., & Pandian, R. (2020). Cryptanalysis of two similar chaos-based image encryption schemes. Cryptologia, 1–12. https://doi.org/10.1080/01611194.2020.1810747

Moyis, L., Tutuavea, U., Volos, C., Butusov, D., Munoz-Pacheco, J. M., & Nistazakis, H. (2020). A two-parameter modified logistic map and its application to random bit generation. Symmetry, 12(5), 829. https://doi.org/10.3390/sym12050829

Munirro-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R. M., & Del Campo, O. A. (2015). A RGB image encryption algorithm based on total plain image characteristics and chaos. Signal Processing, 109, 119–131. https://doi.org/10.1016/j.sigpro.2014.10.033

Ougas, H. (2019). An efficient steganography technique for images using chaotic bitstream. International Journal of Computer Network and Information Security, 10(2), 21. https://doi.org/10.5815/ijcnis.2019.02.03
Ogras, H., & Mustafio, T. (2017). FPGA implementation of a chaotic quadratic map for cryptographic applications. Turkish Journal of Science and Technology, 12(2), 113–119. https://dergipark.org.tr/en/download/article-file/345040

Ogras, H., & Türk, M. (2016). A robust chaos-based image cryptosystem with an improved key generator and plain image sensitivity mechanism. Journal of Information Security, 8(01), 23. https://doi.org/10.4236/jis.2017.81003

Patidar, V., Pareek, N. K., Purohit, G., & Sud, K. K. (2011). A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. Optics Communications, 284(19), 4331–4339. https://doi.org/10.1016/j.optcom.2011.05.028

Qayyum, A., Ahmad, J., Boullia, W., Rubaiee, S., Masood, F., Khan, F., & Buchan, W. J. (2020). Chaos-based confusion and diffusion of image pixels using dynamic substitution. IEEE Access, 8, 140876–140895. https://doi.org/10.1109/ACCESS.2020.3012912

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., & Barker, E. (2001). A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Technology.

Ryu, H. G., & Lee, J. H. (2013). High security wireless CDMA-based chaotic communication with new chaos map. In MILCOM 2013-2013 IEEE Military Communications Conference (pp. 786–790). USA: IEEE. https://doi.org/10.1109/MILCOM.2013.139.

Saeed, M. J. (2013). A new technique based on chaotic steganography and encryption text in DCT domain for color image. Journal of Engineering Science and Technology, 8(5), 508–520. http://jestec.taylors.edu.my/Vol%208%20Issue%205%20October%202013/Volume%208%20Issue%205%20508-520.pdf

Som, S., & Sen, S. (2013). A non-adaptive partial encryption of grayscale images based on chaos. Procedia Technology, 10, 663–671. https://doi.org/10.1016/j.protcy.2013.12.008

Telem, A. N. K., Segning, C. M., Kenne, G., & Fotsin, H. B. (2016). A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network. Advances in Multimedia, 2014, 1–13. https://doi.org/10.1155/2014/602921

Tur, B., & Ogras, H. (2020). Transmission of frequency balance instructions and secure data sharing based on chaos encryption in smart grid-based energy systems applications. IEEE Access, 9, 27323–27332. https://doi.org/10.1109/ACCESS.2021.3058106

Türk, M., & Ogras, H. (2011). Classification of chaos-based digital modulation techniques using wavelet neural networks and performance comparison of wavelet families. Expert Systems with Applications, 38(3), 2557–2565. https://doi.org/10.1016/j.eswa.2010.08.045

Wang, Y., Wang, K. W., Liao, X., & Chen, G. (2011). A new chaos-based fast image encryption algorithm. Applied Soft Computing, 11(1), 514–522. https://doi.org/10.1016/j.asoc.2009.12.011

Xu, L., Li, Z., Li, J., & Hua, W. (2016). A novel bit-level image encryption algorithm based on chaotic maps. Optics and Lasers in Engineering, 78, 17–25. https://doi.org/10.1016/j.optlasteng.2015.09.007

Yang, J., Chen, Y., & Zhu, F. (2019). Associated observer-based synchronization for uncertain chaotic systems subject to channel noise and chaos-based secure communication. Neurocomputing, 167, 587–595. https://doi.org/10.1016/j.neucom.2015.04.030

Yang, J., & Zhu, F. (2013). Synchronization for chaotic systems and chaos-based secure communications via both reduced-order and step-by-step sliding mode observers. Communications in Nonlinear Science & Numerical Simulation, 18(4), 926–937. https://doi.org/10.1016/j.cnsns.2012.09.009

Yasser, I., Khalifa, F., Mohamed, M. A., & Samrah, A. S. (2020). A new image encryption scheme based on hybrid chaotic maps. Complexity, 2020, 1–23. https://doi.org/10.1155/2020/9597619

You, H. T., Wang, M. H., Wang, T. Y., & Chen, G. (2015). Signal clustering of power disturbance by using chaos synchronization. International Journal of Electrical Power & Energy Systems, 64, 112–120. https://doi.org/10.1016/j.ijepes.2014.07.014

Ye, R. (2011). A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Optics Communications, 284(22), 5290–5298. https://doi.org/10.1016/j.optcom.2011.07.070

Ye, R., & Guo, W. (2014). An image encryption scheme based on chaotic systems with changeable parameters. International Journal of Computer Network and Information Security, 6(4), 37. https://doi.org/10.5815/ijcns.2014.04.05

Yibe, W., Man, L., Yanting, X., & Hougui, C. (2011). Research on chaos phenomena in power system. In 2011 IEEE Power Engineering and Automation Conference Vol 2, 453–456. Wuhan, China: IEEE. https://doi.org/10.1109/PEAM.2011.6135097.

Yoon, J. W., & Kim, H. (2010). An image encryption scheme with a pseudorandom permutation based on chaotic maps. Communications in Nonlinear Science & Numerical Simulation, 15(12), 3998–4006. https://doi.org/10.1016/j.cnsns.2010.01.041

Zhou, N., Wang, Y., Gong, L., He, H., & Wu, J. (2011). Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform. Optics Communications, 284(12), 2789–2796. https://doi.org/10.1016/j.optcom.2011.02.066

Zhou, N. R., Huo, T. X., Gong, L. H., Pei, D. J., & Liao, Q. H. (2013). Quantum image encryption based on generalized Arnold transform and double random-phase encoding. Quantum Information Processing, 14(4), 1193–1213. https://doi.org/10.1007/s11128-015-0926-z

Zhou, X., Li, J., & Youjie, M. (2012). Chaos phenomena in dc-dc converter and chaos control. Procedia Engineering, 29, 470–473. https://doi.org/10.1016/j.proeng.2011.12.744

Zhu, H., Zhao, C., & Zhang, X. (2013). A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem. Signal Processing: Image Communication, 28(6), 670–680. https://doi.org/10.1016/j.image.2013.02.004

Zhu, Z. L., Zhang, W., Wong, K. W., & Yu, H. (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Sciences, 181(6), 1171–1186. https://doi.org/10.1016/j.ins.2011.10.009
