Research Article

A Lightweight Image Encryption Algorithm Based on Message Passing and Chaotic Map

Hui Liu,1 Bo Zhao,1 Jianwen Zou,1 Linquan Huang,2 and Yifan Liu1

1School of Cyber Science and Engineering, Wuhan University, Wuhan, Hubei 430072, China
2Information School, Wuhan Vocational College of Software and Engineering, Wuhan, Hubei 430212, China

Correspondence should be addressed to Bo Zhao; zhaobo@whu.edu.cn

Received 16 February 2020; Revised 21 June 2020; Accepted 3 July 2020; Published 25 July 2020

Abstract

The popularization of 5G and the development of cloud computing further promote the application of images. The storage of images in an untrusted environment has a great risk of privacy leakage. This paper outlines a design for a lightweight image encryption algorithm based on a message-passing algorithm with a chaotic external message. The message-passing (MP) algorithm allows simple messages to be passed locally for the solution to a global problem, which causes the interaction among adjacent pixels without additional space cost. This chaotic system can generate high pseudorandom sequences with high speed performance. A two-dimensional logistic map is utilized as a pseudorandom sequence generator to yield the external message sets of edge pixels. The external message can affect edge pixels, and then adjacent pixels interact with each other to produce an encrypted image. A MATLAB simulation shows the cipher-image performs fairly uniform distribution and has acceptable information entropy of 7.996749. The proposed algorithm reduces correlation coefficients from plain-image 1 to its cipher-image 0, which covers all of the plain-image characters with high computational efficiency (speed = 18.200374 Mbit/s). Theoretical analyses and experimental results prove the proposed algorithm’s persistence to various existing attacks with low cost.

1. Introduction

1.1. Background. The rapid development of networking promotes multimedia communication and transmission. As one of the most important data carriers, multimedia contains large amounts of visual information and rich content. Multimedia plays important role and has widespread applications [1–4] in many scenarios. However, multimedia data are vulnerable to interception and modification during transmission on public communication channels. Additionally, mobile devices are vulnerable to theft and loss due to their small size in a public environment. In particular, mobile devices, such as mobile phones and tablets, integrate computing and storage. It is difficult to guarantee the security of personal information by relying solely on access control. Therefore, the loss of mobile devices has serious security risks of privacy leakage [5, 6]. In recent years, many interesting image encryption algorithms have been proposed based on various theories, such as Advanced Encryption Standard (AES) [7, 8], DNA coding [9, 10], discrete cosine transform (DCT) [11, 12], and Arnold transform [13–16]. These schemes require large computational cost that mobile terminals cannot afford. Due to the high parallelism of DNA molecules, some researchers have combined DNA technology to design highly efficient and secure encryption schemes [9, 10]. However, DNA coding takes a substantial amount of time, and many devices do not have a high level of parallelism. Therefore, the encryption scheme based on DNA coding is difficult to be widely used in most scenarios. DCT performs an efficient energy compaction and separability property when images have a high correlation between adjacent pixels. In [12], DCT is used for blocks’ transformation to lower pixel correlation in the frequency domain. But DCT is a lossy coding scheme. Singh et al. [15] utilized a fractional Hartley transform combined with an Arnold transform to encrypt images in the frequency domain. The Arnold transform is used for pixel scrambling in image encryption studies. Its drawback is that the width and height
of the original image must be identical, which limits its application scenarios to a large extent. Furthermore, the image encryption algorithm needs to have extremely high computational efficiency to reduce the impact on the user experience. Ideally, the user should have no perception of the encryption/decryption process. There is a great body of studies on chaotic systems [17–19] because of their many excellent intrinsic properties, such as ergodicity, pseudorandomness, fast computational speed, and high sensitivity. The image encryption algorithm combined with a chaotic system can yield high randomness, high key sensitivity, and fast computational speed. Parvaz and Zarebnia [17] define a two-dimensional logistic map as the pseudorandom sequence operations is proposed in [19]. In the paper, a two-dimensional logistic map is utilized as the pseudorandom generator to get the external message of edge pixels. The pseudorandom sequences participate in the calculation of parameters for chaotic behaviors, which is more suitable for cryptography. Furthermore, an image encryption algorithm based on a two-dimensional logistic map and DNA sequence operations is proposed in [19]. In the paper, a two-dimensional logistic map is utilized as the pseudorandom generator to get the external message of edge pixels. The pseudorandom sequences participate in the calculation of edge pixels and spread to the whole image with message-passing (MP) algorithm, which guarantees the randomness and low pixel correlation of cipher-images.

MP [20–22] is an interesting idea for performing complicated calculations using simple and commonly distributed hardware. Simple messages are passed locally among simple processors whose operations yield a solution for a global problem. Therefore, MP algorithms are widely used in various fields. The message-passing approach is intuitively appealing and suited to non-Gaussian models and nonlinear. Local impact on the global is an important feature to describe the scrambling of a cipher-image. Inspired by the idea, we discover a new application based on MP for high diffusion in the image encryption field. In this paper, as a prior message, the current pixel carries out mathematical calculations with an external message, whose result is stored in the current coordinate as a posterior message. The posterior message is passed to adjacent pixels as an external message for a new round of calculations. As the message passes to all pixels, we get the final cipher-image. The process of a message passing is based on the interaction among adjacent pixels of the image and accomplishes ciphertext security delivery. Therefore, there are no additional space costs, which realize secure image encryption with low space cost.

1.2. Contribution and Organization. A lightweight image encryption algorithm based on MP [20–22] and a chaotic map are proposed for content protection. A message-passing algorithm allows simple messages to be passed locally and leads to the solution of a global problem. Local impact on the global is an important feature to describe the scrambling of a cipher-image. The paper applies MP to scramble the image at the diffusion stage. Each pixel is viewed as the node of the network, and all nodes constitute the image. Two valid passing paths are chosen: one proceeds from the coordinate (1, 1) to (M, N) through a rightward and downward path, called forward propagation [23, 24]. The other proceeds from the coordinate (M, N) to (1, 1) by a leftward and upward path, called backpropagation [24–26]. Chaotic sequences can affect edge pixels, and then adjacent pixels interact with each other to realize the image encryption. The cipher-image is subject to the strict control of the two-dimensional logistic map. Therefore, the initial parameters of a two-dimensional logistic map are regarded as the security key for resistance against key sensitivity attacks. The major contributions of the proposed scheme are as follows:

1. We design a lightweight image encryption algorithm based on MP and two-dimensional logistic chaotic map, which has a high level of security with small space cost and high running performance.

2. We introduce MP to the image encryption field to yield a notable scrambling effect. Message passing yields an interaction among adjacent pixels without additional space consumption. Two valid passing paths are set to guarantee the scrambling effect associated with each pixel of the image.

3. MP allows the external message to affect edge pixels and then spread across the image. Based on this feature, we design a novel diffusion method that chaotic system is used to control the external message of MP. The security of the proposed algorithm relies heavily on a two-dimensional logistic map, which has initial parameters that are reserved as the security key. Hence, the proposed algorithm has a highly chaotic property and strong robustness against key sensitivity analysis.

The remaining sections of the paper are organized as follows. In Section 2, the preliminary proposed algorithm is introduced. In Section 3, the encryption and decryption algorithms are described. Section 4 provides simulation results and security analysis from a MATLAB platform. Finally, conclusions are drawn in Section 5.

2. Preliminary

2.1. Message Passing. The message-passing algorithm [20] can do complicated calculations by using simple and commonly distributed hardware. Simple messages are passed locally among simple processors to provide a solution to a global problem. As an example, consider the complex calculation of counting the number of soldiers in a line who communicate single integers to the two adjacent soldiers and add one to a number. The rule includes three steps as follows:

Step 1. If you are the front soldier in the line, say the number “one” to the soldier behind you

Step 2. If you are the rearmost soldier in the line, say the number “one” to the soldier in front of you

Step 3. If a soldier ahead of or behind you says a number to you, add one to it, and say the new number to the soldier on the other side
Its abstract model is given in Figure 1.

As shown in Figure 1, MP [20] has a local impact on the global, which is an important feature to yield the scrambling of the cipher-image. We introduce MP into image encryption for scrambling and define edge pixels as a set of pixels whose coordinates \( i = 1 \) or \( j = 1 \) or \( i = M \) or \( j = N \) in the \( M \times N \) image. To adapt to the bidimensionality of an image, this paper extends definitions of forward propagation [23, 24] and backpropagation [24–26] for a low correlation coefficient. Forward propagation proceeds from the coordinate \((1, 1)\) to \((M, N)\) on a rightward and downward path while backpropagation proceeds from the coordinate \((M, N)\) to \((1, 1)\) on a leftward and upward path. Based on the abstract model of message passing presented in Figure 1, we provide two-dimensional definitions of forward propagation and backpropagation of MP in the image below. Forward propagation is defined as follows:

\[
\text{Mp}^\prime(i, j) = \begin{cases} 
\text{ExF(Efr}(j), \text{Efc}(i)) \oplus \text{Mp}(i, j), & \text{if } i = 1 \text{ and } j = 1, \\
\text{ExF(Mp}^\prime(i, j - 1), \text{Efr}(j)) \oplus \text{Efc}(i) \oplus \text{Mp}(i, j), & \text{if } i = 1 \text{ and } j \neq 1, \\
\text{ExF(Mp}^\prime(i - 1, j), \text{Efc}(i)) \oplus \text{Efr}(j) \oplus \text{Mp}(i, j), & \text{if } i \neq 1 \text{ and } j = 1, \\
\text{ExF(Mp}^\prime(i - 1, j), \text{Mp}(i, j - 1)) \oplus \text{Efc}(i) \oplus \text{Efr}(j) \oplus \text{Mp}(i, j), & \text{if } i \neq 1 \text{ and } j \neq 1,
\end{cases}
\]

where the \( M \times N \) image \( \text{Mp} \) is calculated to be \( \text{Mp}^\prime \) by forward propagation. The function \( \text{ExF} \) returns the computed result of the external message. \( \text{Efr} \) of size \( 1 \times N \) and \( \text{Efc} \) of size \( N \times 1 \) represent forward external message sets. The coordinate \((i, j)\) proceeds from \((1, 1)\) to \((M, N)\). Backpropagation [24–26] is able to scramble the image from front to back. When a certain pixel is altered, all the pixels behind it change. Backpropagation [24–26] is able to scramble the image from front to back. When a certain pixel is altered, all the pixels behind it change. The combination of forward propagation and backpropagation provides the cryptosystem with a significant feature that a variation in one pixel can affect all the pixels behind it.

\[
\text{Mp}^\prime(i, j) = \begin{cases} 
\text{ExF(Ebc}(M), \text{Ebr}(N)) \oplus \text{Mp}(i, j), & \text{if } i = M \text{ and } j = N, \\
\text{ExF(Mp}^\prime(i, j + 1), \text{Ebr}(j)) \oplus \text{Ebc}(i) \oplus \text{Mp}(i, j), & \text{if } i = M \text{ and } j \neq N, \\
\text{ExF(Mp}^\prime(i + 1, j), \text{Ebc}(i)) \oplus \text{Ebr}(j) \oplus \text{Mp}(i, j), & \text{if } i \neq M \text{ and } j = N, \\
\text{ExF(Mp}^\prime(i + 1, j), \text{Mp}(i, j + 1)) \oplus \text{Ebc}(i) \oplus \text{Ebr}(j) \oplus \text{Mp}(i, j), & \text{if } i \neq M \text{ and } j \neq N,
\end{cases}
\]

where the \( M \times N \) image \( \text{Mp} \) is calculated to be \( \text{Mp}^\prime \) by backpropagation. The function \( \text{ExF} \) returns the computed result of the external message. \( \text{Ebr} \) of size \( 1 \times N \) and \( \text{Ebc} \) of size \( M \times 1 \) represent back external message sets. The coordinate \((i, j)\) proceeds from \((1, 1)\) to \((M, N)\).

2.2. Two-Dimensional Logistic Map. A two-dimensional logistic map [19, 27] contains many features, such as less periodic windows in bifurcation diagrams and a larger range of parameters for chaotic behaviors, which is more suitable for cryptography. As a nonlinear recursive algorithm, a two-dimensional logistic map is defined as follows:

\[
\begin{align*}
\phi(x_n) &= \mu_1 x_n (1 - x_n) + \gamma_1 y_n^2, \\
\phi(y_n) &= \mu_2 y_n (1 - y_n) + \gamma_2 (x_n^2 + x_n y_n),
\end{align*}
\]

where \( \mu_1, \mu_2, \gamma_1, \text{ and } \gamma_2 \) are control parameters. When \( 2.75 < \mu_1 \leq 3.4, \ 2.75 < \mu_2 \leq 3.45, \ 0.15 < \gamma_1 \leq 0.21, \) and \( 0.13 < \gamma_2 \leq 0.15, \) the system can generate outstanding pseudonumbers in the region \((0, 1)\).

2.3. Substitution Box. Substitution box (S-box) [8, 28] is an important nonlinear tool in cryptography. S-box is created by using a form of modulus mathematics that is called Rijndael’s Galois field. Its arithmetic has special properties that ensure values do not exceed \( 2^n \), which keeps everything within a byte and is great for computers [16]. As a lookup table, S-box generally divides each number into its most and least significant nibble (4 bits). The least significant nibble identifies the column, and the most significant nibble defines the row to use in Table 1.

3. Encryption and Decryption

The encryption approach consists of three stages, including external message generation, forward propagation, and backpropagation. The overall architecture of the proposed cryptosystem is shown in Figure 2. External message generation is constructed by a two-dimensional logistic map [19, 27], whose initial parameters are taken as the security key of the proposed cryptosystem. External message generation is utilized to generate external message sets to encrypt the edges of the image. Forward propagation [23, 24] is introduced to scramble the image from front to back. When a certain pixel is altered, all the pixels behind it change. Backpropagation [24–26] is able to scramble the image from back to front. When a certain pixel is altered, all the pixels before it change too. The combination of forward propagation and backpropagation provides the cryptosystem with a significant feature that a variation in one pixel can affect the whole image, which ensures the proposed method could resist against multiple advanced attack methods, e.g., differential attack and chosen-plaintext attack, etc. In this paper, forward propagation and backpropagation as defined in equations (1) and (2) are described in Figures 3 and 4,
respectively, where Efr, Efc, Ebr, and Ebc, respectively, represent external message along four directions.

3.1. Encryption Approach. The proposed algorithm takes the initial parameters of a two-dimensional logistic map as a security key. Two pairs of initial parameters \((x_1, y_1)\) and \((x_2, y_2)\) are substituted into equation (3), and then after iterating equation (3) for \(M\) and \(N\) times, respectively, the cryptosystem obtains four chaos sequences that participate in computations of forward propagation shown in Figure 3 and backpropagation shown in Figure 4. The detailed encryption steps are as follows:

1. Substituting two pairs of initial parameters \((x_1, y_1)\) and \((x_2, y_2)\) into equation (3) and iterating them for \(N + m\) and \(M + m\) times, respectively. Discarding the former \(m\) results in a new set of initial parameters \((x_1, y_1')\) and \((x_2, y_2')\). These new parameters are then fed into the logistic map to obtain chaotic sequences for encryption.

Table 1: S-box lookup table.

|   | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F |
|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| 3 | 04 | C7 | 23 | C3 | 18 | 96 | 09 | A0 | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| D | 70 | 3E | B5 | 6B | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| E | E0 | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 |
| F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

Figure 2: Overall architecture of the proposed cryptosystem.

Figure 1: Abstract model of message passing. Note. Prior message \(\text{prm} = 1\) and external message \(\text{exm} = \text{exm}_1 + \text{exm}_2 = n\). Posterior message \(\text{pom} = \text{prm} + \text{exm} = n + 1\). Therefore, the number of soldiers is equal to \(n + 1\).
values to avoid harmful effects. Four chaos sequences, including \( X_1 \) of size \( N \), \( Y_1 \) of size \( N \), \( X_2 \) of size \( M \), and \( Y_2 \) of size \( M \), are obtained, and they range from 0 to 1.

(2) Executing equation (4) to transform chaos sequences into external message sets \( Efr \) of size \( N \), \( Efc \) of size \( M \), \( Ebr \) of size \( N \), and \( Ebc \) of size \( M \):

\[
Efr = (X_1 \times M \times N \times 10^3) \mod 256,
Efc = (X_2 \times M \times N \times 10^3) \mod 256,
Ebr = (Y_1 \times M \times N \times 10^3) \mod 256,
Ebc = (Y_2 \times M \times N \times 10^3) \mod 256.
\]

(3) Defining the function \( \text{ExF} \) in equations (1) and (2) as follows:

\[
\text{ExF}(\mu, \lambda) = S[\mu \oplus \lambda].
\]

where the function \( S \) substitutes the value of the current argument [28] according to Table 1.

(4) Substituting the \( M \times N \) plain-image \( P \) into \( Mp \) and executing equation (1) from coordinate \((1, 1)\) to \((M, N)\) through forward propagation produce the image \( Cf \).

(5) Substituting the image \( Cf \) into \( Mp \) and executing equation (2) from coordinate \((M, N)\) to \((1, 1)\) through backpropagation produce the final cipher-image \( C \).

3.2. Decryption Approach. The proposed cryptosystem has an excellent feature in that the majority of encryption/decryption steps are the same. Therefore, the proposed cryptosystem is easy to implement in various platforms with low costs. The detailed decryption steps are given as follows:

(1) By executing steps (1–3) in Section 3.1, external message sets \( Efr, Efc, Ebr, \) and \( Ebc \) are obtained.

(2) Substituting the final cipher-image \( C \) into \( Mp \) and executing equation (2) from coordinate \((1, 1)\) to \((M, N)\) implement the converse of backpropagation and the image \( Cf \) is obtained.

(3) Substituting the image \( Cf \) into \( Mp \) and executing equation (1) from the coordinate \((M, N)\) to \((1, 1)\) implement the converse of forward propagation. Thus, the decryption process is complete, and the plain-image \( P \) is obtained.

4. Security Analysis

The adversary may attempt various attack methods to break up encryption algorithms. In order to verify the security of the proposed cryptosystem, we simulate multiple attack methods to conduct security analysis from many aspects, including statistical analysis, sensitivity analysis, key space analysis, information entropy, chosen-plaintext attack, time, and space costs. Color image is composed of red, green, and blue channels. The proposed cryptosystem is implemented
in three color channels to ensure the security of color images. For convenient comparison and analysis, standard grayscale images $256 \times 256$ Lena and $512 \times 512$ Peppers from the SIPI image database are used for the experiment. The simulations are implemented in MATLAB R2015b on a computer with a $2.30 \text{ GHz Intel Core i3 CPU}$ and $4 \text{ GB of RAM}$. For good chaotic characteristics, the cryptosystem sets the control parameters of the two-dimensional logistic map as $\mu_1 = 3.30$, $\mu_2 = 3.25$, $c_1 = 0.18$, and $c_2 = 0.14$. The two-dimensional logistic map discards the former $m = 100$ values to avoid the harmful effects of initial generations. We input the security keys $x_1 = 0.152461879512$, $y_1 = 0.587516341234$, $x_2 = 0.379856254561$, and $y_2 = 0.871468754210$ and encrypt $256 \times 256$ Lena and $512 \times 512$ Peppers. Plain-images and their cipher-images are presented in Figure 5.

4.1. Statistical Analysis

4.1.1. Histogram. The histogram [19, 29] represents the distribution of the pixel values of an image. For visual images, the distribution of their pixel values shows an obvious rule. A statistical attack is a common method to find statistical clues to break the cryptosystem. A secure cryptosystem can make the cipher-image have a uniform frequency distribution and provide as little statistical information as possible. We compare the distribution of the pixel values between the plain-image and cipher-image. Figure 6 shows that plain-images contain a large amount of statistical information while cipher-images have a fairly uniform distribution over the interval $[0, 255]$.

4.1.2. Correlation Coefficients. Due to the intrinsic features of the image, adjacent pixels perform high correlation. The correlation coefficient [29, 30] is a numerical measure to evaluate the statistical relationship between two variables. The high correlation means attackers could try to infer adjacent pixel values based on probability theory. An excellent image encryption algorithm can reduce the correlation of adjacent pixels and provide a smaller correlation coefficient. We randomly choose 5,000 pairs of adjacent pixels from plain-images and cipher-images along horizontal, vertical, and diagonal directions for a correlation test. The correlation coefficient is defined as follows:

$$E = \frac{1}{N} \sum_{i=1}^{N} x_i,$$

$$D(x) = \frac{1}{S} \sum_{i=1}^{S} (x_i - E(x))^2,$$

$$\text{Cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)),$$

$$r_{xy} = \frac{\text{Cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

where

| $P(1, 1)$ | $P(1, N-1)$ | $P(1, N)$ | Ebc (1) |
|----------|-------------|-----------|---------|
| $P(M-1, 1)$ | $P(M-1, N-1)$ | $P(M-1, N)$ | Ebc (M-1) |
| $P(M, 1)$ | $P(M, N-1)$ | $P(M, N)$ | Ebc (M) |
| Ebc (1) | Ebc (N-1) | Ebc (N) |

Figure 4: Backpropagation of the proposed algorithm.
where \( x \) and \( y \) are pixel values of adjacent pixels. The parameter \( S = 5000 \) is the total number of pixels. \( E(x) \) is mathematical expectations and \( D(x) \) is the variance of \( x \). \( \text{Cov}(x, y) \) is the covariance and \( r_{xy} \) is the correlation coefficient. Figure 7 shows the correlation distribution of Lena and its cipher-image along three directions. The correlation distribution of the plain-image is highly concentrated, while that of the cipher-image is random. It reveals that the high correlation of the image is obviously reduced. We calculate the correlation coefficients of plain-images and cipher-images according to equation (6). Table 2 reports that the correlation coefficients of plain-images are close to 1, while those of cipher-images are close to 0. Table 3 shows a comparison of correlation coefficients for the proposed scheme and other schemes from three directions for the image Lena. The proposed cryptosystem covers up all the plain-image characteristics and has confusion properties.

4.1.3. Mean Absolute Error. In statistics, mean absolute error (MAE) [31, 32] is a measure of the difference between two continuous variables. Here, MAE is a measure to assess the error between the plain-image \( P \) and the cipher-image \( C \). A enough large MAE means more secure encryption effects. The definition of MAE is given by

\[
\text{MAE} = \frac{1}{M \times N} \sum_{j=1}^{M} \sum_{i=1}^{N} |C(i, j) - P(i, j)|.
\]  

where \( M \times N \) is the size of the image. The results of MAE are reported in Table 4.

4.1.4. Root Mean Squared Error. In statistics, root mean squared error (RMSE) [32] reflects the average squared difference between the estimated values and what is estimated, which corresponds to the expected value of the squared error loss. RMSE is a measure to quantify the difference between the plain-image \( P \) and the cipher-image \( C \). The definition of RMSE is given by

\[
\text{RMSE} = \sqrt{\frac{1}{M \times N} \sum_{j=1}^{M} \sum_{i=1}^{N} (C(i, j) - P(i, j))^2}.
\]  

The larger the RMSE value, the better the encryption security. The results of the RMSE are reported in Table 4. The experiment results show the significant difference between plain-images and corresponding cipher-images, which indicates strong resistance against statistical attacks.

4.2. Sensitivity Analysis

4.2.1. Differential Attack. A differential attack [33–35] is an effective method to break up a cryptosystem that aims to input some slightly different plain-images and compare differences of their cipher-images for attack clues. To quantify the influence of a slight change on the cipher-image, two common parameters, including the number of pixels change rate (NPCR) and unified average changing intensity (UACI), are used to measure the differences between two cipher-images. NPCR and UACI are defined as follows:
NPCR = \frac{\sum_{i,j} D(i, j)}{M \times N} \times 100\%,
\tag{9}

UACI = \frac{1}{M \times N} \left[ \sum_{i,j} \left| C(i, j) - C'(i, j) \right| \right] \times 100\%,
\tag{10}

where \(M \times N\) is the size of cipher-images \(C\) and \(C'\).

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

NPCR reflects the difference in the number of different pixel values between the two images. And UACI reflects the difference of pixel intensity between two images. For two images with complete randomness, NPCR = 99.609375% and UACI = 33.463542%. Table 5 reports simulation results for a 1-bit change in plain-images for different pixels.

We add a random pixel value for two standard images to 1 and compute the results of NPCR and UACI for 1,000 times. The mean values are shown in Table 6. Table 7 reports the comparison of NPCR and UACI for the proposed scheme and other schemes in the image Lena. Results are very close to ideal values. The simulation demonstrates an excellent ability to resist differential attacks.

4.2.2. Key Sensitivity Test. The key sensitivity test \cite{10, 30} checks the sensitivity of the cryptosystem to the security key. The test method includes two aspects. One encrypts the plain-image with the security key and decrypts the corresponding cipher-image with a key that is wrong by a 1-bit change in the security key, as seen in Table 8 and Figure 8. The other encrypts images by two keys that differ by only 1 bit and measures the differences between their cipher-images using NPCR and UACI. Table 9 reports the average NPCR and UACI between two cipher-images when the security key is added error \(x_1 + 10^{-12}\). The results show that a slight change in the security key can cause significant differences, and the cryptosystem passes the key sensitivity test.
Table 5: The plain-image sensitivity test.

| Pixels     | (1, 1)       | (7, 124)      | (81, 243)     | (160, 74)      | (215, 12)      | (255, 255)      |
|------------|--------------|---------------|---------------|----------------|----------------|-----------------|
| NPCR       | Lena         | 0.996094      | 0.995789      | 0.996170       | 0.996094       | 0.995956        | 0.995865        |
|            | Peppers      | 0.996231      | 0.996082      | 0.995735       | 0.996017       | 0.996010        | 0.996246        |
| UACI       | Lena         | 0.334303      | 0.334879      | 0.334736       | 0.334289       | 0.333824        | 0.334528        |
|            | Peppers      | 0.334005      | 0.334987      | 0.335786       | 0.333705       | 0.334750        | 0.334005        |

Table 6: Average NPCR and UACI for the plain-image sensitivity test.

| Images | NPCR | UACI     |
|--------|------|----------|
| Lena   | 0.996097 | 0.334557 |
| Peppers| 0.996091 | 0.334798 |

Table 7: Comparison of the plain-image sensitivity test in the image Lena.

| Algorithm | NPCR | UACI     |
|-----------|------|----------|
| Proposed  | 0.996097 | 0.334557 |
| [29]      | 0.995964 | 0.334762 |
| [31]      | 0.996124 | 0.334591 |
| [34]      | 0.996216 | 0.336510 |
| [35]      | 0.996107 | 0.334436 |

Table 8: Key sensitivity test.

| Security key | Wrong key | Decryption |
|--------------|-----------|------------|
| x₁ = 0.152461879513  | y₁ = 0.587516341234  | False     |
| x₂ = 0.379856254561  | y₂ = 0.871468754210  | False     |
| x₃ = 0.152461879512  | y₃ = 0.587516341234  | False     |
| x₄ = 0.379856254561  | y₄ = 0.871468754210  | False     |
| x₅ = 0.871468754210  | y₅ = 0.587516341234  | False     |
| x₆ = 0.379856254561  | y₆ = 0.871468754210  | False     |

Figure 8: Key sensitivity test of several wrong decryption keys: (a) error x₁+10⁻¹², (b) error y₁+10⁻¹², (c) error x₂+10⁻¹², and (d) error y₂+10⁻¹².
4.3. Key Space Analysis. A brute-force attack means that attackers try all possible key spaces through an exhaustive key search until the correct one is found. A secure cryptosystem would have enough key space to defend against a brute-force attack. The proposed algorithm takes two pairs of initial parameters, \((x_1, y_1)\) and \((x_2, y_2)\), from the two-dimensional logistic map as the security key. The design provides a flexible size for the key space to meet requirements for all levels of security. The simulation employs a 10^{18}-bit security key, which is larger than 2^{128} [36, 37]. It provides enough key space to resist all kinds of brute-force attack. Thus, the proposed cryptosystem is suitable for privacy protection of photos in multiple terminal devices.

4.4. Information Entropy. Information entropy [8, 38] quantifies the amount of information in a stochastic source. As an important mathematical parameter, it is used to evaluate the consistent distribution of pixel values. When the probability of each gray value of the image is equal, the information entropy of the image is the maximum. The definition of information entropy is given as follows:

\[
H(s) = - \sum_{i=0}^{2^n-1} p(s_i) \log_2 p(s_i),
\]

where \(p(s_i)\) represents the probability of the symbol \(s_i\). The ideal information entropy is \(H(s) = 8\) for a 2^{8}-bit stochastic source. Therefore, the information entropy of cipher-images encrypted by a good cryptosystem should be close to 8 for grayscale images or a channel of color images. The calculation of information entropy for cipher-images Figure 5(a)–5(d) is presented in Table 10. Information entropy is related to the size of the image. Table 11 reports the comparison of average entropy between the proposed scheme and other schemes for 512 × 512 images. The results reveal the uncertainty and degree of ambiguity in the cipher-image.

4.5. Ciphertext and Plaintext Attack. In cryptography, the ciphertext and plaintext attacks are common methods to cryptanalyze a cryptosystem. Adversaries deploy specific attack approaches based on different scenarios and assumptions. According to adversary’s knowledge, the ciphertext and plaintext attacks could be divided into ciphertext-only attack, known-plaintext attack, and chosen-plaintext attack [9]. Ciphertext-only attack assumes that an adversary only could obtain a set of ciphertexts. Known-plaintext attack assumes that an adversary could obtain a set of plaintexts and corresponding ciphertexts. And chosen-plaintext attack assumes that an adversary could access arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. Obviously, chosen-plaintext attack provides the most information for adversaries among three attack assumptions. If the cryptosystem is able to defend the chosen-plaintext attack, it is also believed to resist against the other two attacks.

In the proposed cryptosystem, we apply the two-dimensional logistic map to generate the chaotic sequences as the external message, which cannot be recovered by means of chosen-plaintext images. Moreover, the novelty of the proposed algorithm is that we introduce MP to the image encryption process for a notable scrambling effect. As shown in equations (1) and (2), forward propagation and backpropagation allow the external message to affect edge pixels and then spread across the image. Therefore, the encryption result of every byte is affected by the contents of the previous bytes. The experimental results in Section 4.2.1 show high sensitivity of the proposed method to plain-images, which ensures the cryptosystem could resist against the chosen-plaintext attack.

4.6. Time and Space Cost. In the encryption algorithm based on chaotic sequences, a large amount of computation time is spent on multiplication for multiple rounds [39–41]. In this phase, the time complexity of the proposed algorithm is \(O(2^{M+N} + M \times N)\). In the encryption/decryption phase, forward propagation and backpropagation need to execute \(M \times N\) times. Considering the lack of high parallelism in mobile devices, the time complexity is \(O(2 \times M \times N)\). Thus, the time complexity of the cryptosystem is \(O(2 \times M \times N + M + N + m)\). The encryption process is simulated for 512 × 512 images 1000 times and gets the total time as 109.887583 s. Thus, the real encryption speed is 18.20037 Mbit/s. The cryptosystem performs with high encryption efficiency and is acceptable for mobile phone users. Table 12 compares the encryption efficiency with different encryption algorithms and displays a fast running performance for the proposed cryptosystem.

In terms of space cost, the proposed algorithm needs \(O(M+N)\) to store external message sets produced by a two-dimensional logistic map. In the encryption/decryption phase, message passing is conducted inside the image and does not have an extra space cost. However, the S-box occupies 256 bytes for nonlinear substitution. Thus, the space complexity of the cryptosystem is \(O(M+N+256)\), which is applicable to mobile phones.
Table 12: Comparison of the encryption efficiency.

| Algorithm          | Speed (Mbit/s) |
|--------------------|----------------|
| Proposed           | 18.20037       |
| [3]                | 1.62760        |
| [10]               | 1.02838        |
| [18]               | 1.10229        |

5. Conclusion

This paper demonstrates a lightweight image encryption algorithm based on message passing and a two-logistic map with low time and space costs. Compared to the $M \times N$ space cost of traditional chaotic algorithms, the proposed algorithm only requires $M + N$ bytes to store external message sets from a two-dimensional logistic map, which is utilized as a pseudorandom generator to yield the external message sets of edge pixels. The external message sets affect edge pixels, and then adjacent pixels interact with each other to realize the image encryption. Message passing provides a novel approach for scrambling pixels inside an image without additional space costs. The simulation shows the cipher-image performs fairly uniform distribution with correlation coefficients close to 0, an acceptable information entropy of 7.996749 with a high computational efficiency (speed = 18.200374 Mbit/s). Additionally, the cryptosystem provides a flexible size for the key space to meet requirements for all levels of security. The experiment proves that the algorithm can resist key sensitivity analysis even if the key space is large enough. The cryptosystem can resist various attack techniques, including statistical attack, differential attack, known-plaintext attack, and brute-force attack with low time and space overheads. Thus, we demonstrate that the proposed algorithm can resist various existing attacks with low time and space cost.

Data Availability

Our experimental data come from an open-source database.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this article.

Acknowledgments

The work was supported by the Wuhan Frontier Program of Application Foundation (no. 201801040111295) and the National Natural Science Foundation of China (no. U1936122).

References

[1] Y. Zhou, L. Zhang, C. Zhang, P. Li, and X. Li, “Perceptually aware image retargeting for mobile devices,” *IEEE Transactions on Image Processing*, vol. 27, no. 5, pp. 2301–2313, 2018.
[2] C. H. Chu, “Image deblur for 3d sensing mobile devices,” in *Proceedings of the IEEE International Conference on Multimedia and Expo*, San Diego, CA, USA, July 2018.
[3] R. Krishnamoorthi and P. Murali, “A selective image encryption based on square-wave shuffling with orthogonal polynomials transformation suitable for mobile devices,” *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 1217–1246, 2017.
[4] X. Wu, X. Lu, X. Han, and C. Liu, “An adaptive denoising method for colour images of mobile phone based on bivariate shrinkage function,” *International Journal of Embedded Systems*, vol. 10, no. 6, pp. 484–493, 2018.
[5] L. Wu, J. Wang, K.-K. R. Choo, and D. He, “Secure key agreement and key protection for mobile device user authentication,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 319–330, 2019.
[6] W. T. Li, Y. S. Shen, and P. Wang, “Breaking three remote user authentication systems for mobile devices,” *Journal of Signal Processing Systems*, vol. 90, no. 8-9, pp. 1179–1190, 2018.
[7] B. Sayantani, K. Marimuthu, S. Rajkumar et al., “Modification of AES using genetic algorithms for high-definition image encryption,” *International Journal of Intelligent Systems Technologies and Applications*, vol. 17, no. 4, pp. 452–466, 2018.
[8] V. M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso, and M. Aldape-Pérez, “Substitution box generation using Chaos: an image encryption application,” *Applied Mathematics and Computation*, vol. 352, pp. 123–135, 2019.
[9] J. Chen, Z.-l. Zhu, L.-b. Zhang, Y. Zhang, and B.-q. Yang, “Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption,” *Signal Processing*, vol. 142, pp. 340–353, 2018.
[10] S. Sun, “A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling,” *IEEE Photonics Journal*, vol. 10, no. 2, pp. 1–14, 2018.
[11] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, “A color image cryptosystem based on dynamic DNA encryption and chaos,” *Signal Processing*, vol. 155, pp. 44–62, 2019.
[12] X. Wang and C. Liu, “A novel and effective image encryption algorithm based on chaos and DNA encoding,” *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6229–6245, 2017.
[13] S. Lin, J. Xu, S. Liu et al., “A robust image watermarking scheme using Arnold transform and BP neural network,” *Neural Computing and Applications*, vol. 30, no. 8, pp. 2425–2440, 2018.
[14] N. Zhou, Y. Hu, L. Gong et al., “Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations,” *Quantum Information Processing*, vol. 16, no. 6, p. 164, 2017.
[15] P. Singh, A. K. Yadav, and K. Singh, “Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition,” *Optics and Lasers in Engineering*, vol. 91, pp. 187–195, 2017.
[16] Z. Ni, X. Kang, and W. Lei, “A novel image encryption algorithm based on bit-level improved Arnold transform and hyper chaotic map,” in *Proceedings of the IEEE International Conference on Signal and Image Processing*, pp. 156–160, Beijing, China, August 2017.
[17] R. Parvaz and M. Žaremba, “A combination chaotic system and application in color image encryption,” *Optics & Laser Technology*, vol. 101, pp. 30–41, 2018.
[18] G. Ye and X. Huang, “A secure image encryption algorithm based on chaotic maps and SHA-3,” *Security and Communication Networks*, vol. 9, pp. 2015–2023, 2016.
[19] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 88, pp. 197–213, 2017.

[20] D. J. C. Mackay, *Information Theory, Inference and Learning Algorithms*, pp. 241–247, Cambridge University Press, Cambridge, UK, 2003.

[21] C. Rush and R. Venkataramanan, “Finite sample analysis of approximate message passing algorithms,” *IEEE Transactions on Information Theory*, vol. 64, no. 11, pp. 7264–7286, 2018.

[22] F. Meyer, T. Kropfreiter, J. L. Williams et al., “Message passing algorithms for scalable multitarget tracking,” *Proceedings of the IEEE*, vol. 106, no. 2, pp. 221–239, 2018.

[23] X. Gong, S. Fong, and Y.-W. Si, “Fast multi-subsequence monitoring on streaming time-series based on Forward-propagation,” *Information Sciences*, vol. 450, pp. 73–88, 2018.

[24] Q. Zhang, Y. Wu, and S. C. Zhu, “Interpretable convolutional neural networks,” in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 8827–8836, Salt Lake City, UT, USA, June 2018.

[25] O. Krestinskaya, K. N. Salama, and A. P. James, “Analog backpropagation learning circuits for memristive crossbar neural networks,” in *Proceedings of the IEEE International Symposium on Circuits and Systems*, Florence, Italy, May 2018.

[26] V. Singh, B. Kumar, S. K. Singh, S. P. Ghoda, and A. Mohan, “Multiple watermarking technique for securing online social network contents using Back Propagation Neural Network,” *Future Generation Computer Systems*, vol. 86, pp. 926–939, 2018.

[27] R. Hamza, K. Muhammad, and G. Ramirez-Gonzalez, “Hash based encryption for keyframes of diagnostic hysteroscopy,” *IEEE Access*, vol. 6, pp. 60160–60170, 2018.

[28] N. Fips, “Announcing the advanced encryption standard (AES),” *Federal Information Processing Standards Publication*, vol. 29, no. 8, pp. 2200–2203, 2001.

[29] H. Umar and A. A. Naveed, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, pp. 391–402, 2019.

[30] L. Huang, S. Cai, M. Xiao, and X. Xiong, "A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion," *Entropy*, vol. 20, no. 7, pp. 535–554, 2018.

[31] M. Khan, T. Shah, and S. I. Batool, "Construction of S-box based on chaotic Boolean functions and its application in image encryption," *Neural Computing and Applications*, vol. 27, no. 3, pp. 677–685, 2016.

[32] M. Khan and T. Shah, "A novel statistical analysis of chaotic S-box in image encryption," *3d Research*, vol. 5, no. 3, pp. 1–8, 2014.

[33] M. Brindha and N. Ammasai Gounden, "A chaos based image encryption and lossless compression algorithm using hash table and Chinese Remainder Theorem," *Applied Soft Computing*, vol. 40, pp. 379–390, 2016.

[34] P. Praveen Kumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Triple chaotic image scrambling on RGB - a random image encryption approach," *Security and Communication Networks*, vol. 8, no. 18, pp. 3335–3345, 2015.

[35] L. Zhen, C. Peng, L. Li et al., "A novel plaintext-related image encryption scheme using hyper-chaotic system," *Nonlinear Dynamics*, vol. 94, no. 2, pp. 1319–1333, 2018.

[36] F. Yang, J. Mou, C. Ma et al., “Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application,” *Optics and Lasers in Engineering*, vol. 129, pp. 1–16, 2020.