New Encryption Algorithm Using Bit-Level Permutation and Non-Invertible Chaotic Map

ABDELRAHMAN A. KARAWIA, (Member, IEEE), AND YASSER A. ELMASRY

1Department of Mathematics, Faculty of Science, Mansoura University, Mansoura 35516, Egypt
2Department of Mathematics, Faculty of Science, King Khalid University, Abha 61413, Saudi Arabia

Corresponding author: Abdelrahman A. Karawia (abibka@mans.edu.eg)

This work was supported by the Deanship of Scientific Research through King Khalid University by the General Research Project under Grant GRP/189/42.

ABSTRACT Recently, a little research into image encryption has been used on chaotic economic maps. The current paper suggests a bit-level permutation and a non-invertible chaotic economic map to encrypt an image. First, the secret key generation is linked to the plain image. So, the suggested algorithm may resist both known-plaintext and chosen-plaintext attacks. Then a bit-level permutation is performed for all the binary bits of the plain image’s pixels, using the logistic map (permutation stage). It is used to improve the algorithm’s security. Then pixel diffusion is applied using the 2D non-invertible chaotic economic map and bit-wise XOR operations. It is used to change the pixels’ values and make them highly random. The results of the experiments and the security analyses show that the given image encryption algorithm is efficient with higher security. Some comparisons showed that the proposed algorithm outperformed many recent algorithms. Finally, the proposed algorithm may be able to withstand a variety of attacks.

INDEX TERMS Bit-level permutation, chaotic map, Cournot Duopoly game, image encryption, image decryption, security analysis.

I. INTRODUCTION

Multimedia communication has become increasingly useful as information technology and the internet have fast growth. Digital images are a major player in multimedia communication and are used in many fields, such as biology, medicine, the military, and social life. Since large amounts of data are carried in digital images and are widely disseminated on the internet, the protection of the data embedded in these images has become a significant and pressing issue. Digital images have certain inherent characteristics that text content does not, such as low entropy, high levels of redundancy, high correlation and large data capacities. Cryptography is one of the three methods which are used to protect digital images. The other two ways are steganography and watermarking. Steganography is the method of concealing a secret message (plain image) inside another message (cover image). Watermarking is the technique of embedding some identification information known as a watermark into the digital data by its owner. Cryptography is the process of encoding secret data via an algorithm that transforms data in such a way that unlicensed users can’t read it [1]. Classical algorithms like DES and AES are weak to carry out image encryption [2]. These methods are not suitable for digital images with a high degree of redundancy and correlation between adjacent pixels [3]. As a result, new algorithms must be proposed.

In [4], the authors presented a color image algorithm based on an enhanced evolutionary algorithm and the matrix semi-tensor product. A double color image encryption algorithm is suggested via combining 2D compressive sensing with an embedding technique [5]. In [6], the authors presented an image encryption algorithm using 2-D compressive sensing with a multi-embedding strategy. A color image compression and encryption algorithm is described based on compressive sensing and a double random encryption technique [7].

Chaotic systems are perfect for encryption of the image because of their sensitivity to initial values and control parameters, ergodicity, excellent pseudo-randomness, and determinism. As a consequence, several encryption techniques, methods and algorithms using chaotic maps have been proposed [8]–[12]. In [13], the authors proposed a new image encryption scheme via permutation-substitution networks and chaotic. Image encryption using new beta chaotic maps is described in [14]. In [15], the author presented an encryption algorithm using a cubic S-box and chaos.
A new image encryption using DNA approach and 2D Hénon-Sine map is given in [16]. The authors in [17] presented an image encryption via Henon chaotic map with nonlinear term. An algorithm via diffusion of Household and Tent-Dynamics coupled map lattices is given in [18]. In [19], an image encryption using compressive sensing and chaos systems is proposed. An image encryption scheme using double chaotic cyclic shift and Josephus problem is given in [20]. In [21], an algorithm via random dynamic mixing is proposed. All these algorithms used pixel permutations in which the position of the pixel is changed, but its value did not change. In bit-level permutation, the pixel position and value are both changed [22], [23]. In this paper, the permutation-diffusion model will be used. The bit-level permutation is applied during the permutation stage. For the diffusion stage, chaotic discrete dynamical systems possess some complicated characteristics such as bifurcations and chaos which have been reported in the literature. Indeed, such systems contain several parameters that are responsible for such characteristics. Any minor changes in the values of these parameters may result in distracting behavior in the future evolution of such systems. For these reasons, such chaotic systems have been adopted in the cryptographic process. In the current paper, we recall a more chaotic economic map introduced in [26]. Recent research has revealed that such systems have poor bifurcation and chaos as complicated properties on which they rely. In such systems, many types of bifurcations, such as folds, transcritical, and Neimark–sacker bifurcations, have been described and studied. When compared to other maps, such as the logistic map, the number of open windows in chaotic economic systems is low. On the other hand, there are few studies in the literature that use such economic systems in the encryption process. These systems are capable of providing a secure cryptographic technique [27]. Our contributions to the current paper are:

- calculated the secret key by the key mixing proportion factor based on the plain image [28], which is not fixed.
- applied the bit-level permutation on all bits of the plain image at once using a logistic map.
- used the Cournot Duopoly map, which is a competition game that exhibits a wide range of interesting phenomena, such as coexisting complex attractors and chaotic behaviors. The provided map is used to create random bits on the sender and legitimate receiver sides, which are then used in reliable data encryption.
- performed the analysis of the proposed algorithm for a secure and efficient image cipher.
- according to simulation and security analysis, the proposed algorithm provides a greater level of security than other image encryption algorithms.

The remainder of this paper is structured in the following manner. The 2D non-invertible chaotic economic map is presented in Section 2. In Section 3, the secret key generation is discussed in depth. The proposed algorithm is given in Section 4. In Section 5, we examine the proposed image ciphers’ security and results using histogram analysis, histogram statistics, information entropy analysis, key space analysis, correlation analysis, key sensitivity analysis, and other analyses. Section 6 gives the conclusion.

II. THE 2D NON-INVERTIBLE CHAOTIC ECONOMIC MAP

In [26], the authors introduced the nonlinear discrete dynamic map which is utilized to represent the dynamics of Cournot Duopoly game. In the economic market, Cournot Duopoly games attract many researchers because of their dynamic characteristics. The Cournot Duopoly game consists of two competing firms (or players or companies) and the interaction between those firms gives rise to complex dynamic behaviors that support economic markets with important expectations. Such kinds of games are defined by a two-dimensional map that is used to study the dynamic characteristics of such games. The authors calculated the fixed points for the map. They also examined their stability conditions, which attracted some chaotic behaviors due to the complex dynamics of the map being studied. They came to the conclusion that the game’s map is non-invertible of the type $Z_4 - Z_2$. The map is given as follows:

$$\begin{align*}
\begin{cases}
x(n + 1) &= x(n) + v_1x(n) \\
[a - (2 + c)x(n) - dy(n)], \\
y(n + 1) &= y(n) + v_2y(n) \\
[a - (1 + \omega + c)y(n) - dx(n)],
\end{cases}
\end{align*}$$

where $x$ and $y$ represent the quantities produced by the two companies.

The chaotic map (1) has six parameters, $a, c, d, \omega, v_1,$ and $v_2$. These parameters are economically significant; the maximum price represented by the constant $a > 0$ while the product differentiation represented by the constant $d \in [-0.5, 1]$. $c > 0$ denotes a fixed marginal cost parameter. The adjustment speed for the $i^{th}$ company is denoted by $v_i$, $i = 1, 2$ and the public ownership parameter is denoted by $\omega \in [0, 1]$. Figures 1(a) and 1(b) depict the bifurcation diagram for the effects of the parameters $v_1$ and $v_2$ on the quantities $x$ and $y$ at the parameters values, $a = 0.5$, $c = 0.2$, $d = 0.35$, and $\omega = 0.45$. Figures 1(c) and 1(d) validate the map’s chaotic behavior by introducing the largest Lyapunov exponents.

III. THE SECRET KEY GENERATION

Assuming that $\mathbf{A} = (a_{ij}), i = 1, 2, \ldots, M$, $j = 1, 2, \ldots, N$ is the plain image. The key mixing proportion factor can be used to calculate the secret key as follows [28]:

$$\begin{align*}
K_1 &= \frac{1}{256} \text{mod} \left( \sum_{i=1}^{M/4} \sum_{j=1}^{N} a_{ij}, 256 \right), \\
K_2 &= \frac{1}{256} \text{mod} \left( \sum_{i=M/4+1}^{M/2} \sum_{j=1}^{N} a_{ij}, 256 \right), \\
K_3 &= \frac{1}{256} \text{mod} \left( \sum_{i=M/2+1}^{M} \sum_{j=1}^{N} a_{ij}, 256 \right)
\end{align*}$$

(2)
A. A. Karawia, Y. A. Elmasry: New Encryption Algorithm Using Bit-Level Permutation and Non-Invertible Chaotic Map

FIGURE 1. (a), (b) Bifurcation graph regarding \( x \) and \( y \) on differing \( \nu_1 \) and \( \nu_2 \). (c), (d) The Largest Lyapunov exponents regarding \( \nu_1 \) and \( \nu_2 \).

The initial condition \( \Omega_0 \) is then modified using the equation:

\[
\Omega_0 = \frac{\Omega_0 + K_i}{2}, \quad i = 1, 2, 3,
\]

where \( \Omega_0 = x_0, x_1, y_1 \). Then, choose three initial values, \( x_0, x_1, y_1 \). On the other hand, the parameters \( \mu, a, c, d, \omega, \nu_1, \nu_2 \) for the logistic map and map (1) are computed as follows:

\[
\mu = 3.80 + 0.05 \ast K_1,
\quad a = 0.45 + 0.05 \ast K_1,
\quad c = 0.15 + 0.05 \ast K_1,
\quad d = 0.30 + 0.05 \ast K_2,
\quad \omega = 0.40 + 0.05 \ast K_2,
\quad \nu_1 = 5.85 + 0.05 \ast K_3,
\quad \nu_2 = 4.15 + 0.05 \ast K_3.
\]

In the current section, when the parameters fall into these periodic windows, the chaos is lost. So, all parameters are chosen to avoid the periodic windows in the chaotic ranges of the used chaotic economic map (1).

IV. THE PROPOSED ALGORITHM

Our proposed algorithm depends on the bit-level permutation diffusion model. The primary advantage of bit-level permutation is that it changes the position and value of the pixels at the same time. The first stage is applying the bit-level permutation to the plain image. Then, the second stage is to diffuse the result values of the first stage into the chaotic map sequence using bit-wise XOR.

A. THE BIT-LEVEL PERMUTATION

In the current stage, let \( A \) be the plain image of size \( M \times N \). The logistic map is defined by the following formula:

\[
x_{i+1} = \mu x_i (1 - x_i), \quad \mu \in (0, 4].
\]

It’s used to make a permutation of integers that’s random. The aim of this stage is to shuffle the bits of the plain image according to the generated random integers. The bit-level permutation algorithm may be processed as in Algorithm 1.

\[ p = [k \ i]: \text{means add the element } i \text{ to the vector } p. \]

\[ p([k \ i]) = p([i \ k]): \text{means swapping between } k \text{ and } i \text{ in the vector } p. \]

B. THE CHAOTIC MAP SEQUENCE

The aim of this stage is to use the chaotic map (1) to generate a sequence of random bits of length \( 8MN \). The algorithm for generating this sequence may be processed as in Algorithm 2.

C. THE ENCRYPTION ALGORITHM

The proposed encryption algorithm will employ two sequences of random bits, \( B \) and \( C \), via Algorithm 1 and
Algorithm 1 Bit-Level Permutation Algorithm

Input: $x_0$, $\mu$ and the plain image, $A$, with size $M \times N$.
Output: Sequence of random bits, $S$ of size $MN \times 8$.

Step 1: Reshape $A_{MN}$ to $A_{1 \times MN}$.
Step 2: Convert $A$ to binary vector, $B = \{b_1, b_2, \ldots, b_{8 \times MN}\}$.
Step 3: Set $p = 1, x = x_0$.
Step 4: For $i = 2$ to $8 \times MN$, compute
$$ p = [i \mod 8], $$
$$ k = \text{ceil}(i \times x), $$
$$ p([k \mod 8]) = p([i \mod 8]), $$
$$ x = \mu \times x \times (1 - x). $$
End For
Step 5: For $i = 1$ to $8 \times MN$, compute
$$ S(1, i) = B(1, p(i)) $$
End For
Step 6: Reshape $S_{1 \times 8MN}$ to $S_{MN \times 8}$.

Algorithm 2 Chaotic Map Sequence Algorithm

Input: $x_1, y_1, a, c, d, \omega, v_1, v_2$, and the sequence length, $n$.
Output: Sequence of random bits, $C$ of size $MN \times 8$.

Step 1: $x(1) = x_1, y(1) = y_1,$
$$ z(1) = (x(1) + y(1))/2, $$
Step 2: For $i = 1$ to $n + 999$, compute
$$ x(i + 1) = x(i) + v_1 \times x(i) \times (a - (2 + c) \times x(i) - d \times y(i)) $$
$$ y(i + 1) = y(i) + v_2 \times y(i) \times (a - (1 + \omega + c) \times y(i) - d \times x(i)) $$
$$ z(i + 1) = (x(i + 1) + y(i + 1))/2. $$
End For
Step 3: Set
$$ Z = \text{floor}(\text{mod}(z(1000 : n + 999) \times (10^{14}), 256)) $$
Step 4: Convert $Z$ to binary vector of size $n \times 8$.

Algorithm 3 The Encryption Algorithm

Input: The plain image $A_{MN}$, $x_0$, $x_1$, $y_1$, $\mu$, $a$, $c$, $d$, $\omega$, $v_1$, and $v_2$.
Output: The cipher image, $E$.
Step 1: Read the plain image $A_{MN}$.
Step 2: Set $S = \text{call Algorithm 1}(x_0, \mu, M, N)$.
Step 3: Set $C = \text{call Algorithm 2}(x_1, y_1, a, c, d, \omega, v_1, v_2, MN)$.
Step 4: Perform bit-wise XOR between $S$ and $C$, say $E = \text{XOR}(S, C)$.
Step 5: Convert $E$ to decimal values, $E_{1 \times MN}$.
Step 6: Reshape $E_{1 \times MN}$ to $E_{MN \times 8}$.

One can apply our algorithm to each channel and combine all the three results to get the encrypted image.

D. THE DECRYPTION ALGORITHM

The decryption algorithm is the opposite procedure of the encryption algorithm. First, the sequence produced by the chaotic map (1) should be obtained. Then, the bit-wise XOR between the sequence and the cipher image is performed. Finally, the plain image is obtained by the bit-level permutation inversion operation. The decryption algorithm may be processed as follows:

V. EXPERIMENTAL RESULTS AND SECURITY ANALYSES

The proposed algorithm’s results are presented and its performance using the most famous measurements, like histogram analysis, correlation coefficients, key space analysis, key sensitivity analysis, and differential analysis, is analyzed in the current section.

A. EXPERIMENTAL RESULTS

Algorithm 3 and Algorithm 4 are executed using Matlab R2016b. In addition, the laptop has a 2.40 GHz CPU and 12 GB of RAM with Windows 10 being used. Eight standard

Algorithm 4 The Decryption Algorithm

Input: The cipher image $E_{MN \times 8}$, $x_0$, $x_1$, $y_1$, $\mu$, $a$, $c$, $d$, $\omega$, $v_1$, and $v_2$.
Output: The plain image, $A$.
Step 1: Read the cipher image $E_{MN \times 8}$.
Step 2: Reshape $E_{MN \times 8}$ to $E_{1 \times MN}$.
Step 3: Convert $E$ to binary values, $E_{MN \times 8}$.
Step 4: Set $C = \text{call Algorithm 2}(x_1, y_1, a, c, d, \omega, v_1, v_2, MN)$.
Step 5: Perform bit-wise XOR between $E$ and $C$, say $S = \text{XOR}(E, C)$.
Step 6: Apply the inverse of Algorithm 1 on $S$, say the output is $D_{MN \times 8}$.
Step 7: Convert $D$ to decimal values, say $A_{1 \times MN}$.
Step 8: Reshape $A_{1 \times MN}$ to $A_{MN}$, the decrypted image.
grayscale images with a size of 256×256 were chosen: Lena, Barbara, Boat, Peppers, Cameraman, Airplane, Mandrill, and Moon surface images. Figure 3(b, e, h, k) displays the encryption results of four tested images. After applying the decryption algorithm, the original images can be exactly obtained as in Figure 3(c, f, i, l).

B. KEY SPACE ANALYSIS

One of the most important characteristics of a good encryption/decryption algorithm is a large key space, which is must be greater than $2^{100}$ [29]. The space of secret key for the proposed algorithm is consists of three initial values, $x_0$, $x_1$, $y_1$, one parameter for the logistic map, $\mu$, and six parameters for map (1), $a$, $c$, $d$, $\omega$, $v_1$, $v_2$. If the precision accuracy is $10^{-15}$ then the secret key space is $10^{15} \times 10^{15} = 10^{30}$ which is greater than $2^{100}$. Therefore, the current algorithm can withstand brute force attacks.

C. KEY SENSITIVITY ANALYSIS

An effective and accurate algorithm must be sensitive to even minor changes in the secret key. The wrong plain image will be restored when the tiniest modifications of the secret key to decrypt the cipher image are used. The cipher image is decrypted using three different test keys chosen at random to test its sensitivity. The results shown in Figure 4 illustrate how minor changes to key parameters can yield incorrect images.

D. INFORMATION ENTROPY ANALYSIS

The gray value distribution of an image is expressed by information entropy, which is an important index of randomness. The image’s information entropy increases as the gray value distribution becomes more uniform. The information entropy ($IE$) is calculated as follows:

$$IE(\theta) = -\sum_{i=1}^{256} p(\theta_i) \log_2 p(\theta_i)$$

where $p(\theta_i)$ denotes the probability of $\theta_i$. For the grayscale image, the exact theoretical value of information entropy is 8. Therefore, if it close to 8 then the attackers will have a difficult time decoding the cipher images. Table 1 presents the information entropies of plain and cipher images of all tested images. All cipher images in Table 1 have information entropies which are close to 8. The estimated local and global entropies for individual bit planes of the Lena image at size $256 \times 256$ are presented in Table 2. Table 3 compares the proposed algorithm to some recently published algorithms based on the information entropy of a Lena’s cipher image of size $256 \times 256$.

E. HISTOGRAM ANALYSIS

The cipher image’s histogram is a crucial property that shows whether the algorithm can withstand statistical analysis. It shows how an image’s pixel values are distributed. An attacker can get a particular amount of information via statistical analysis if the distribution isn’t uniform. As a result, a good image encryption must has a cipher image with uniform histogram distribution. The histograms for four tested images (Airplane, Cameraman, Moon Surface, and Peppers) are shown in Figure 5 before and after encryption.
encryption, the histogram for each of the plain images wasn’t uniform, but after encryption, the corresponding histogram for the cipher image was uniform. As a result, the proposed algorithm may complicate statistical analysis.

F. HISTOGRAM STATISTICS
To backing the results of visual examination in histograms, the variance and its standard deviation are used. The standard deviation is the square root of the variance. The lower the
FIGURE 4. Key sensitivity analysis result; (a) Decoding with true key, (b) Decoding with wrong key parameter $a = 0.500000000000001$, (c) Decoding with wrong key parameter $\omega = 0.450000000000001$, and (d) Decoding with wrong key parameter $\nu_1 = 5.899999999999999$.

TABLE 1. Information entropy before and after using our algorithm at $x_0 = 0.001, x_1 = 0.012, y_1 = 0.001, \sigma = 0.5, c = 0.2, d = 0.35, \omega = 0.45, \nu_1 = 5.9$, and $\nu_2 = 4.2$.

| Image       | $IE$ Plain image | $IE$ Cipher image |
|-------------|------------------|-------------------|
| Airplane    | 6.9667           | 7.9976            |
| Barbara     | 7.4893           | 7.9971            |
| Boat        | 7.0080           | 7.9971            |
| Cameraman   | 7.0097           | 7.9968            |
| Lena        | 7.4429           | 7.9973            |
| Mandrill    | 7.0097           | 7.9968            |
| Moon Surface| 6.7190           | 7.9970            |
| Peppers     | 7.5640           | 7.9969            |

TABLE 2. The estimated local and global entropies for individual bit planes of the Lena image using our algorithm at $x_0 = 0.001, x_1 = 0.012, y_1 = 0.001, \sigma = 0.5, c = 0.2, d = 0.35, \omega = 0.45, \nu_1 = 5.9$, and $\nu_2 = 4.2$.

| Bit-plane | Plain image | Cipher image |
|-----------|-------------|--------------|
| BP 1      | Local 0.9897 | Global 1     |
|           |             | 0.9907       |
| BP 2      | Local 0.9895 | Global 1     |
|           |             | 0.9911       |
| BP 3      | Local 0.9875 | Global 1     |
|           |             | 0.9905       |
| BP 4      | Local 0.9971 | Global 1     |
|           |             | 0.9908       |
| BP 5      | Local 0.8526 | Global 1     |
|           |             | 0.9909       |
| BP 6      | Local 0.6632 | Global 1     |
|           |             | 0.9905       |
| BP 7      | Local 0.5143 | Global 0.9812|
|           |             | 0.9903       |
| BP 8      | Local 0.3532 | Global 0.9996|
|           |             | 0.9906       |

FIGURE 5. Histogram analysis: (a) histogram of plain airplane, (b) histogram of cipher airplane, (c) histogram of plain cameraman, (d) histogram of cipher cameraman, (e) histogram of plain moon surface, (f) histogram of cipher moon surface, (g) histogram of plain peppers, and (h) histogram of cipher peppers.

\[ \bar{f} = \frac{1}{256} \sum_{i=1}^{256} f_i \]  
(8)

where \(f_i\): The frequency for each intensity value in the histogram.

Also, the standard deviation is calculated by the following formula:

\[ S = \sqrt{Var} \]  
(9)
TABLE 3. A comparison between our algorithm and some recent algorithms in the literature for Lena’s cipher image is based on information entropy.

| Image   | Our algorithm | Ref. [30] | Ref. [31] | Ref. [32] | Ref. [33] | Ref. [34] |
|---------|---------------|-----------|-----------|-----------|-----------|-----------|
| Lena    | 7.9973        | 7.9972    | 7.9971    | 7.9971    | 7.9894    |

TABLE 4. The variance and standard deviation of plain and cipher image.

| Image         | Var | S   | Var | S   |
|---------------|-----|-----|-----|-----|
| Airplane      | 1.2804 × 10^6 | 357.8291 | 216.9531 | 14.7293 |
| Cameraman     | 1.1097 × 10^5 | 333.1266 | 289.7266 | 17.0214 |
| Moon Surface  | 1.3409 × 10^5 | 366.1796 | 268.0547 | 16.3724 |
| Peppers       | 3.4809 × 10^4 | 186.5729 | 284.3672 | 16.8632 |

Table 4 shows VAR and S of the histogram for plain and cipher images. Based on the result of Table 4, the cipher images obtained by our algorithm have pixel values which are more uniform.

G. CORRELATION ANALYSIS BETWEEN ADJACENT PIXELS

In the horizontal, vertical, and diagonal directions, adjacent pixels in the plain image have a high correlation. The correlation coefficients of adjacent pixels in the cipher images should have a low enough correlation to withstand statistical attacks, according to an optimal algorithm. We randomly select 5,000 pairs of adjacent pixels from the plain image and its cipher image in each of the three directions to investigate and compare the two images based on the correlation coefficient. The correlation coefficient \( \rho_{xy} \) for each pair is calculated using the formula:

\[
\rho_{xy} = \frac{\text{Cov}(x, y)}{\sqrt{\text{Var}(x)\text{Var}(y)}},
\]

where

\[
\text{Cov}(x, y) = \frac{1}{n} \sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y}),
\]

\[
\text{Var}(x) = \frac{1}{n} \sum_{i=1}^{n} (x_i - \bar{x})^2,
\]

\[
\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i,
\]

\( x \) and \( y \): the values of two adjacent pixels in the image, \( n \): the total number of the selected pixels.

Figure 6 shows the correlation coefficients of two adjacent pixels for the plain and cipher images of Lena’s image via the proposed algorithm. On the other hand, the results are presented in Table 5 along with a comparison to some recent algorithms. The correlation coefficient of the plain image is close to 1 in all directions and is close to 0 in all directions for cipher image. Table 5 shows that the cipher image’s adjacent pixels have a very low correlation. As a result, our algorithm can successfully withstand a statistical attack.

H. DIFFERENTIAL ANALYSIS

The algorithm’s performance against differential attacks improves as the cipher image becomes more sensitive to the plain image. A good image encryption algorithm should ensure that any small modification in the plain image causes a large difference in the cipher image to resist a differential attack. For differential attack analysis, the number of pixels change rate (NPCR) and the unified average changing
The values of NPCR and UACI for the tested images at $x_0 = 0.001, x_1 = 0.012, y_1 = 0.001, \sigma = 0.5, c = 0.2, d = 0.35, \omega = 0.45, r_1 = 5.9$, and $p_2 = 4.2$.

| Image    | NPCR% | NPCR critical values [36] | UACI% | UACI critical values [36] |
|----------|-------|--------------------------|-------|---------------------------|
|          | $N_{0.05}$ | $N_{0.01}$ | $N_0.001$ | $U_{0.05}$ | $U_{0.01}$ | $U_0.001$ |
|          | 99.5693% | 99.5527% | 99.5341% | 33.6472% | 33.7016% | 33.7677% |
| Airplane | pass   | pass       | pass       | pass       | pass       | pass       |
| Barbara  | 99.6289% | pass | pass | pass | pass | pass |
| Boat     | 99.5987% | pass | pass | pass | pass | pass |
| Cameraman| 99.6145% | pass | pass | pass | pass | pass |
| Lena     | 99.6099% | pass | pass | pass | pass | pass |
| Mandarin | 99.6140% | pass | pass | pass | pass | pass |
| Moon Surface | 99.6214% | pass | pass | pass | pass | pass |
| Peppers  | 99.6368% | pass | pass | pass | pass | pass |
| Average  | 99.6135% | pass | pass | pass | pass | pass |

compression intensity (UACI) are commonly used. These measurements have optimal values of $NPCR = 99.6094\%$ and $UACI = 33.4635\%$ [35]. They are computed as follows:

$$ NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\% $$ (14)

$$ UACI = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} |C_1(i, j) - C_2(i, j)|}{M \times N \times 255} \times 100\% $$ (15)

where:

$$ D(i, j) = \begin{cases} 0 & \text{if } C_1(i, j) = C_2(i, j) \\ 1 & \text{otherwise} \end{cases} $$ (16)

where $C_1$ and $C_2$ are two cipher images of the plain image and the modified plain image, with $a$, with a one-pixel difference.

From each plain image, one pixel is selected randomly. The value of this pixel is changed to create a modified plain image, the modified plain image, with a one-pixel difference.

Table 7 compares the proposed algorithm to some recent published algorithms. The NPCR and UACI values for the tested images at $x_0 = 0.001, x_1 = 0.012, y_1 = 0.001, \sigma = 0.5, c = 0.2, d = 0.35, \omega = 0.45, r_1 = 5.9$, and $p_2 = 4.2$.

The plain image $P$ is generated by performing XOR operations between the pixels of $E_P$ and $E_Z$. Figure 7 shows that the decrypted image is entirely different from the plain image. As a consequence, our encryption algorithm is immune to chosen-plaintext attacks.

J. ROBUSTNESS ANALYSIS

1) QUALITY METRICS ANALYSIS

The Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) can be used to assess the accuracy of digital images [40], [41]. The $MSE$ is a metric to determining how different two images are. It is defined as follows:

$$ MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (P_{ij} - D_{ij})^2 $$ (17)

where $P$ and $D$ represent the plain image and the decrypted image, respectively. The size of the original image is $M \times N$. The better the encryption efficiency, the lower the $MSE$ value. On the other hand, the $PSNR$ is the ratio of a signal’s maximal potential power to the power of distorting noise, which influences the accuracy of the signal’s representation. It is evaluated by:

$$ PSNR = 10 \log_{10} \left( \frac{255^2}{MSE} \right) \text{db} $$ (18)

The smaller the $MSE$ value, the higher the $PSNR$ value, indicating that the images being compared are very similar.
The $MSE$ between the plain Lena image with size $(256 \times 256)$ and the decrypted image using our algorithm is 0, and the PSNR is $\infty$. The results indicate that the image examined has high quality metrics.

2) OCCLUSION ATTACK ANALYSIS
To put the occlusion attack to the test, we chose 12.5%, 25%, and 50% occlusion in the Lena cipher image with a size of $256 \times 256$. The occlusion attack results are shown in Figure 8. Table 8 gives the $MSE$ and PSNR between the cipher image with occlusion and its corresponding decrypted image. Also, the comparison between our algorithm and the recent algorithm in [37] is given in Table 8. The results conclude that the proposed algorithm can withstand an occlusion attack effectively.

3) NOISE ATTACK ANALYSIS
To test the proposed algorithm’s anti-noise efficiency, the cipher image is corrupted by salt and pepper noise of various intensities. As a result, Lena’s cipher image is altered by adding salt and pepper noise with intensities of 0.1, 0.15, and 0.20. Then, the modified cipher image is decrypted. Figure 9 shows the results. The $MSE$ and PSNR between the plain image and the decrypted image are given in Table 8. Also, the comparison between our proposed algorithm and the recent algorithm in [37] is given in Table 9. It can be shown that after the noise image is decrypted, the original image can be restored in its entirety. As a result, the proposed algorithm has some anti-noise attack potential.

K. COMPUTATIONAL TIME ANALYSIS
The computational time was computed on a laptop with the following characteristics: a 2.40GHz processor, 12GB of RAM, and Windows 10. Table 10 shows the time of encryption and the time of decryption for the image of Lena.

L. NIST STATISTICAL TESTS
The NIST statistical tests are used to test the random characteristics of cipher images. The proposed algorithm generates one hundred cipher images of Lena$_{256 \times 256}$ using different
A. A. Karawia, Y. A. Elmasry: New Encryption Algorithm Using Bit-Level Permutation and Non-Invertible Chaotic Map

FIGURE 9. Noise attack analysis: (a) cipher with intensity 0.10 of salt and pepper noise, (b) decrypted image of (a), (c) cipher with intensity 0.15 of salt and pepper noise, (d) decrypted image of (c), (e) cipher with intensity 0.20 of salt and pepper noise, and (f) decrypted image of (e).

TABLE 9. Comparison between the proposed algorithm and the recent algorithm [37] based on MSE and PSNR.

| intenisty ratio | Proposed Algorithm | Ref. [37] |
|-----------------|--------------------|-----------|
|                 | MSE    | PSNR   | MSE    | PSNR   |
| 10%             | 116.9  | 27.5   | 8837.0 | 8.7    |
| 15%             | 1597.2 | 16.1   | 9333.3 | 8.4    |
| 20%             | 2063.6 | 14.9   | 9926.9 | 8.2    |

TABLE 10. The analysis of computational time.

| Image         | Time (in seconds) |
|---------------|-------------------|
| Lena (256 x 256) | Encryption: 1.8936 s, Decryption: 1.8353 s |

TABLE 11. Statistical result of NIST test for 100 cipher images at $x_0 = 0.001, \sigma = 0.5, \mu = 0.2, d = 0.35, \omega = 0.45, \gamma_1 = 5.9, \gamma_2 = 4.2$ and random values for $x_1$ and $y_1$ between 0 and 1.

| Statistical test       | Proposed algorithm | Result |
|------------------------|--------------------|--------|
| Frequency              | 96/100             | $P$    |
| Block Frequency        | 97/100             | $P$    |
| Cumulative Sums        | 96/100             | $P$    |
| Runs                   | 98/100             | $P$    |
| Longest Runs           | 98/100             | $P$    |
| Rank                   | 100/100            | $P$    |
| FFT                    | 99/100             | $P$    |
| Non Overlapping Templates | 98/100         | $P$    |
| Overlapping Templates  | 100/100            | $P$    |
| Universal              | 98/100             | $P$    |
| Approximate Entropy    | 100/100            | $P$    |
| Random Excursion       | 26/27              | $P$    |
| Random excusion Variant| 27/27              | $P$    |
| Serial                 | 98/100             | $P$    |
| Linear Complexity      | 100/100            | $P$    |

$P$ means PASS.

VI. CONCLUSION

In this paper, a new image encryption algorithm based on bit-level permutation and a 2D non-invertible chaotic economic map has been proposed. Since it is built on two chaotic maps and a bit-level permutation, it can overcome the common weaknesses of low-dimensional chaotic map and pixel permutation algorithms. The bit-level permutation and XOR coding strengthen the security of the algorithm. Experimental results for key space, key sensitivity, information entropy, histogram, and correlation between adjacent pixels analyses confirmed that our image encryption algorithm can be used to encrypt images efficiently. Based on differential attack, chosen/known-plaintext attack and robustness analyses, the proposed algorithm can be avoid different attacks. Also, the NIST statistical tests support that the proposed algorithm has a high degree of randomness. Therefore, the proposed algorithm can be applied to image encryption. Since the logistic map depends on only one parameter, we can examine other maps like the Henon map, the Skew tent map, and the Gauss map. In future work, the authors should use quantum image encryption to increase the security of the algorithm.

ACKNOWLEDGMENT

The authors would like to thank the Editor and anonymous reviewers for their time and effort in presenting helpful and useful comments that greatly improved the original manuscript. They would also like to thank Dr. Awad Shawky for proofreading the article.

REFERENCES

[1] M. Kumar, R. Lahcen, R. Mohapatra, C. Alwala, and S. Kurella, “Review of image encryption techniques,” J. Comput. Eng., vol. 14, no. 1, pp. 31–37, 2020.
[2] S. Li, G. Chen, A. Cheung, B. Bhargava, and K.-T. Lo, “On the design of perceptual MPEG-video encryption algorithms,” IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 2, pp. 214–223, Feb. 2007.
[3] K. U. Shahna and A. Mohamed, “A novel image encryption scheme using both pixel level and bit level permutation with chaotic map,” Appl. Soft Comput., vol. 90, May 2020, Art. no. 106162.
[4] X. Chai, X. Zhi, Z. Gan, Y. Zhang, Y. Chen, and J. Fu, “Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption,” Signal Process., vol. 183, Jan. 2021, Art. no. 108041.
X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen, “An efficient approach for encrypting double color images into a visually meaningful fingerprint image using 2D compressive sensing,” *Inf. Sci.*, vol. 556, pp. 305–340, May 2021.

X. Chai, H. Wu, Z. Gan, Y. Zhang, and Y. Chen, “Hiding cipher-images generated by 2D compressive sensing with a multi-embedding strategy,” *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107525.

X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, “Color image compression and encryption scheme based on compressive sensing and double random encryption strategy,” *Signal Process.*, vol. 176, Nov. 2020, Art. no. 107684.

W. Liu, K. Sun, and C. Zhu, “A fast image encryption algorithm based on chaotic map,” *Opt. Lasers Eng.*, vol. 84, pp. 26–36, Sep. 2016.

M. Mollaeefar, A. Sharif, and M. Nazari, “A novel encryption scheme for colored image based on high level chaotic maps,” *Multimed. Tools Appl.*, vol. 76, no. 1, pp. 607–629, Jan. 2017.

X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, “An image encryption algorithm based on chaotic system and compressive sensing,” *Signal Process.*, vol. 148, pp. 124–144, Jul. 2018.

G. Ye, K. Jiao, C. Pan, and X. Huang, “An effective framework for chaotic image encryption based on 3D logistic map,” *Secur. Commun. Netw.*, vol. 2018, Oct. 2018, Art. no. 8402578.

I. Yasser, F. Khalifa, M. Mohamed, and A. Samrah, “A new image encryption scheme based on hybrid chaotic maps,” *Complexity*, vol. 2020, Jul. 2020, Art. no. 9597619.

A. Belazi, A. A. El-latif, and S. Belghith, “A novel image encryption scheme based on substitution-permutation network and chaos,” *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.

R. Zahmoul, R. Ejbali, and M. Zaied, “Image encryption based on new Beta chaotic maps,” *Opt. Lasers Eng.*, vol. 96, pp. 39–49, Sep. 2017.

Z. Yong, “The unified image encryption algorithm based on chaos and cubic S-Box,” *Inf. Sci.*, vol. 450, pp. 361–377, Jun. 2018.

J. Wu, X. Liao, and B. Yang, “Image encryption using 2D Henon-sine map and DNA approach,” *Signal Process.*, vol. 153, pp. 11–23, Dec. 2018.

H. Luo and B. Ge, “Image encryption based on henon chaotic system with nonlinear term,” *Multimedia Tools Appl.*, vol. 78, no. 24, pp. 34323–34352, Dec. 2019.

X. Wang, W. Xue, and J. An, “Image encryption algorithm based on tent-dynamics coupled map lattices and diffusion of household,” *Chaos, Solitons Fractals*, vol. 141, Dec. 2020, Art. no. 110309.

A. Hadj Brahim, A. Ali Pacha, and N. Hadj Said, “Image encryption based on compressive sensing and chaos systems,” *Opt. Laser Technol.*, vol. 132, Dec. 2020, Art. no. 106489.

R. Wang, G.-Q. Deng, and X.-F. Duan, “An image encryption scheme based on double chaotic cyclic shift and Josephus problem,” *J. Inf. Secur.*, vol. 58, May 2021, Art. no. 106837.

X. Wang, S. Chen, and Y. Zhang, “A chaotic image encryption algorithm based on random dynamic mixing,” *Opt. Laser Technol.*, vol. 138, Jun. 2021, Art. no. 106837.

C. Fu, B.-B. Lin, Y.-S. Miao, X. Liu, and J.-J. Chen, “A novel chaos-based bit-level permutation scheme for digital image encryption,” *Opt. Commun.*, vol. 284, no. 23, pp. 5415–5423, 2011.

H. Liu and X. Wang, “Color image encryption using spatial bit-level permutation and high-dimension chaotic system,” *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, Aug. 2011.

S. Askar, A. Karawia, A. Al-Khedhairi, and F. Al-Ammar, “An algorithm of image encryption using logistic and two-dimensional chaotic economic maps,” *Entropy*, vol. 21, no. 1, p. 44, Jan. 2019.

H. Huang, S. Yang, and R. Ye, “Efficient symmetric image encryption by using a novel 2D chaotic system,” *IET Image Process.*, vol. 14, no. 6, pp. 1157–1163, May 2020.

S. S. Askar and A. A. Elsadany, “Nonlinear dynamics of cournot duopoly game: When one firm considers social welfare,” *Discrete Dyn. Nature Soc.*, vol. 2021, pp. 1–11, Jun. 2021, 6697341.

S. S. Askar, A. A. Karawia, and F. S. Alamarah, “Cryptographic algorithm based on pixel shuffling and dynamical chaotic economic map,” *IET Image Process.*, vol. 12, no. 1, pp. 158–167, Jan. 2018.

D. Enzeng, C. Zengguang, Y. Zhuhui, and C. Zaiqing, “A chaotic images encryption algorithm with the key mixing proportion factor,” in *Proc. Int. Conf. Inf. Manage., Innov. Manage. Ind. Eng.*, Taipei, Taiwan, Dec. 2008, pp. 169–174, doi: 10.1109/ICIIE.2008.25.

L. Y. Zhang, C. Li, K.-W. Wong, S. Shu, and G. Chen, “Cryptanalyzing a chaos-based image encryption algorithm using alternate structure,” *J. Syst. Softw.*, vol. 85, no. 9, pp. 2077–2085, 2012.