Int. J. Nonlinear Anal. Appl.
Volume 12, Special Issue, Winter and Spring 2021, 903-921
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/IJNAA.2021.5520

# Color image encryption using linear feedback shift registers by three-dimensional permutation and substitution operations

ali momeni asl[a], ali broumandnia[b,*], seyed javad mirabedini[c]

[a]Departament of computer engineering, Qom Branch, Islamic Azad University, Qom, Iran.
[b]Departament of computer engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran.
[c]Department of Computer engineering, Center Tehran Branch, Islamic Azad University, Tehran, Iran

(Communicated by Ehsan Kozegar)

**Abstract**

This study proposes a scale-invariant digital color image encryption method that includes three main steps the pre-substitution, the 3D scale-invariant modular chaotic map, and the post-substitution. 1) The pre-substitution: At the first stage, pixels of plain sub-images are XOR with different key patterns. By starting from one of the plain sub-images, the pixels of the selected plain sub-image is XOR with the initial key, and the result is used as the cipher sub-image and as the next key pattern for performing XOR operations on the next plain sub-image. In other words, the XOR result of each step is used as the next step key pattern, 2) the 3D permutation: At the second stage, first the red, green, and blue components of a $M \times N$ color image is divided to m sub-images with size $n \times n$. Then m sub-images are partitioned into $k = \lceil \frac{m}{n} \rceil$ windows $W_1$ to $W_k$ with size $n \times n$ sub-images. The last two $W_k - 1$ and $W_k$ windows may be overlap in several sub-images. Finally, the three-dimensional modular chaotic maps are performed on the $W_1$ to $W_k$ windows with MIPF keys and selected by LFSR, 3) the post-substitution: At the final stage, the $M \times N$ color image is initially divided into a set of color sub-images. Then, the 24-bit pixels of each sub-images are circularly shifted with several bits specified in the secret key. Modular arithmetic is used in the 3D scale-invariant chaotic maps to increase keyspace and enhance security parameters. With repeat at least one round of main steps, the proposed encryption scheme reaches optimum parameter values and it is highly sensitive to minor differences in both secret key and plain image. The proposed encryption method for images improves the standard parameters of evaluation such as entropy, adjacent pixel correlations, histogram, and expanded keyspace.

*Keywords:* Image encryption, 3D chaotic map, Modular arithmetic, LFSR, Keyspace

*Corresponding author
*Email addresses:* alimomeni-stu@qom-iau.ac.ir (ali momeni asl), broumandnia@azad.ac.ir (ali broumandnia), mirabedini@iauctb.ac.ir (seyed javad mirabedini)

*Received:* September 2020 *Accepted:* September 2021

## 1. Introduction

Extensive changes have recently occurred through the expansion of computer networks for different purposes in our activities and lives, meaning that different individuals and organizations make their data accessible to others through a connection to the World Wide Web.

Therefore, information security is more important than ever. One of the important points that should be considered in internet information security is to ensure that people do not have access to information.

Thus far, there have been offered various ways for information security, such as restriction of the use of the Internet, use of security tools, and data encryption. Meanwhile, cryptography has been widely used for different purposes. One of the most usual methods to keep the information safe is to encrypt it.

In cryptography, the information sent is changed using the password key and the password algorithm by which only the person who has the key, and the algorithm can extract the main information from the password information. If one does not know one or both of these, he cannot have access to the information.

The use of cryptography has a long history. Before the information age, most people who used information encryption were governments, especially military users. The data encryption history dates back to the Roman Empire.

Today, most methods and models of information encryption are used in connection with the computer. Access to the information that does not have any scientific method of cryptography and is normally stored or exchanged through computer networks, will be easily possible by unauthorized persons without the need for special expertise. Recently, with the growth of digital image transmission over the Internet, communication channels must be sufficiently secure and not be attacked by hackers; therefore, maintenance of security and authentication of images is crucial.

However, the implementation of cryptographic methods for image data is challenging compared to text messaging. Image data are not secured efficiently and quickly by classical text encryption algorithms such as RSA and DES due to features such as bulkiness, high additions, and high correlation between image points, particularly in real-time applications. Another problem with these algorithms is the length, and their key is that due to the volume of encrypted data, the use of limited length keys makes the method vulnerable to encrypted text attacks.

Recently, various image encryption techniques have been proposed that use the concepts of permutation and diffusion to provide resistance to known unsaved image attacks.

Encryption of digital images can be complete in standard, non-standard, and hybrid methods. In standard encryption methods, the image is transformed into a data bits stream, and it is divided into equal size blocks and encrypted with the shared key encryption methods. The most common standard shared key cryptography is the DES and AES which are also called block ciphers. In the DES and AES block ciphers, data streams are divided into blocks with sizes of 64-bits and 128-bits correspondingly. Given that standard block cipher techniques have been designed with several rounds and each round includes complex operations, as a result, encryption of digital images with high volumes of data is highly time-consuming. In recent research to speed up and improve security desires, most non-standard encryption methods are used to encrypt digital media. Non-standard methods use substitution, permutation, of image pixels to achieve the main properties of encryption, namely, confusion and diffusion. In most of the studies and methods used to encrypt digital images, the chaotic maps are used to perform pixels substitution, pixels permutation, and/or key generation.

For this reason, non-standard methods are also known as chaos-based methods. The chaos-based image encryption methods have some common features and limitations as follows [7]: 1) the secret

key of continuous chaotic maps such as logistic map usually depends on initial conditions and system parameters. As a result, continuous chaos-based image ciphers depend on a quantized value of the secret key to suit the range of the chaotic parameter and phase space of the initial condition [7, 23, 12, 4]. 2) The length of the generated chaotic path is normally equal to the number of image pixels. Using multiple one-dimensional chaotic maps to generate chaotic points will be costly and unusable for larger images [7, 19]. 3) Usually, the discrete chaotic map such as the Arnold cat map has small period points and have many silent points. In the permutation operation, silent points do not change, and permute as a result could lead to security problems [24]. 4) Although the maximal Lyapunov exponent of the generalized Arnold cat map is positive, it is a metric measuring the overall dynamics of a system, which may be unsuccessful to prove the complex dynamics of the system in a local domain [21, 24].

In this study, color image encryption is presented through the confusion and diffusion method and the use of chaotic 3D mappings with the following features:1) is independent of size, in other sense, encryption operations on images without restrictions Image size performs, 2) Encryption operations are performed in the 3D environment to accelerate encryption and robustness against attacks, 3) Provide 3D turbulence mapping to perform 3D permutation operations to achieve clutter feature, 4) Performs two operation steps Replacing the jump to the release property, 5) increasing keyspace and 6) allows increase speed and parallelizing some cryptographic operations.

The structure of this article is as follows: In the second part, we will have an overview of digital color image encryption techniques. In the third part, the concepts of cryptography, types of algorithms, and cryptographic methods are described. This section provides an overview of image encryption methods based on the chaotic mapping. In the fourth section, we present the theory and concepts related to a three-dimensional chaotic map. In the fifth section, we will explain the proposed method of color image encryption using a step-by-step diagram block. In the last part, we will evaluate the results with standard analyses and compare the proposed method to other methods.

## 2. Related work

The most important digital image cryptographic operations are based on permutation and substitution of image pixels. These operations will have two basic properties of image diffusion and confusion. Diffusion hides the relationship between the cipher image and the plain image, and confusion hides the relationship between the cipher image and the key [18]. The permutation operation changes the arrangement and position of pixels in the digital image with a suitable key. The Arnold cat map and the Hilbert transform curve are examples of permutation operations [4]. The substitution operation change gray level pixels of a digital image by using XOR, circular shift, and the appropriate key. These encryption operations should be reversible by the same key which has been encrypted by the plain image. The experimental findings and various statistical and differential analyses have shown that high security with diffusion and confusion can be achieved by using permutation and substitution operations, and these operations allow decrypting the selected region independently of other parts of the image. These are very useful for real-time applications [4]. 2018 from the viewpoint of an image cryptanalyst [1].

In this section, several digital image encryptions that have been proposed in the literature to date will be reviewed. Algorithms of digital image encryption presented in the works are classified into standard, non-standard, and hybrid.

### *2.1. Standard cryptography*

Standard cryptography methods are divided into three categories: a symmetric block cipher, symmetric stream cipher, and asymmetric cipher. The most important symmetric block cipher

methods that are used to encrypt data and images are DES and AES. Yong Zhang in ref [22] an image encryption program based on AES in cipher block chaining (CBC) the mode was designed with C language. V. M. Silva-Garcia et al. extend triple-DES (3DES) for the block cipher to 96-bit encryption, which is called Triple-DES-96 and is used to color image encryption [16]. Most encryption methods and algorithms are based on symmetric block cipher (DES, AES, 3DES) and symmetric stream cipher (RC4, RC6) have been surveyed and implemented in [4]. Due to the low speed of asymmetric encryption methods such as RSA, less is used in image encryption. The most common uses of this type of encryption are integrity and authentication with the help of watermarking and steganography techniques and so on.

### *2.2. Non-standard cryptography*

In the chaos-based cryptography literature, designers use chaotic systems as entropy sources, and entropy source sets include hyper chaos, spatiotemporal chaos, chaotic maps, and time delay chaotic system, DNA encoding, and chaotic systems [21]. In general, discrete-time and continuous-time systems have been used as chaotic systems in the encryption algorithm [21]. The structures of continuous-time chaotic systems are more complex than those of discrete-time chaotic systems [21]. In the design image encryption approaches, the role of chaotic systems is chaotic key generation or permutation [21]. In addition, various structures such as DNA [31, 3, 9], a secure hash function such as MD5 [34], perceptron model [21], have been used to improve the performance of the algorithms [21]. Also, chaos-based image encryption algorithms are used cryptographic primitives such as XOR operation, mod operation, S-box structure, DNA computing, nonlinear operation, etc. [21]. Zhang et al. [31] suggested an image encryption scheme by the spatiotemporal chaotic system that has the features of a larger parameter range, better randomness, and more chaotic DNA sequences. Zhang et al. [27] suggested another encryption scheme for color images encryption using a spatiotemporal chaotic system. That is secure and suitable for encrypting color images in different sizes. Liu et al. [34] designed a stream-cipher algorithm based on one-time keys and robust chaotic maps, for obtaining high security and improving the dynamical degradation. They utilized the piecewise linear chaotic map as the generator of a pseudo-random keystream sequence. The initial conditions were generated by the true random number generators, the MD5 of the mouse positions. Liu et al. [5] also suggested a bit-level permutation and high- dimension chaotic map for encryption of color images. Liu et al. [3] proposed a novel confusion and diffusion method for image encryption. The key generation is according to the plain image and the common keys, which can result in an automatic change in the initial conditions of the chaotic maps through all encryption processes. Wang et al. [32]. Based on the high-dimension Lorenz chaotic system and perceptron model within a neural network, a chaotic image encryption system with a perceptron model is proposed. Wang et al. [9] developed a novel image encryption scheme based on DNA sequence operations and the spatiotemporal system. Wang et al. [8] suggested a new block image encryption scheme based on hybrid chaotic maps and dynamic random growth techniques. Since cat map is periodic and it can be easily cracked by the chosen-plaintext attack, they use cat map in another securer way which can eliminate the cyclical phenomenon and resist chosen-plaintext attack. Zhang Ying-Qian et al. [33] developed an image encryption algorithm that is based on spatiotemporal non-adjacent coupled map lattices. The system of non-adjacent coupled map lattices has more outstanding cryptography features in dynamics than the logistic map or coupled map lattices do. Hua et al. [14] introduce an image cipher by using block-based scrambling and image filtering. In chaos-based encryption algorithms, security is evaluated based on algorithm structure and chaos mapping performance [7, 14]. Cryptographic algorithms are broken down due to various security attacks if the designed image cryptography is not sufficiently secure [15, 2, 26, 18]. In other words, by developing methods for the detection of chaotic

methodologies and cryptanalysis, experts have concluded that if chaos utilization is weak, some chaos maps will face security problems [4, 1, 24]. Therefore, as they have confusion and diffusion properties, the chaotic maps used for image encryption should be robust against all security attacks. There are many articles on cryptanalysis; some of them are as follows: Zhang et al. [6] analyzed the potential flaws in Zhu's algorithm in detail and developed a chosen-plaintext attack and chosen-cipher text attack on Zhu's algorithm. The proposed attack indicates that the Arnold cat map applied directly in image encryptions is not suitable for cryptography. Analyzed the security of an image encryption algorithm suggested by Ye and Huang. Using this as a typical counterexample, security defects in the design of the Ye-Huang algorithm are summarized.

### *2.3. Hybrid cryptography*

Some research on image cryptography uses a combination of standard and non-standard methods for image encryption and key generation. Some of these new researches are as follows:

Manish Kumar et al. proposed a new algorithm for image security using Elliptic Curve Cryptography (ECC) diversified with DNA encoding. The algorithm first encodes the RGB image using DNA encoding followed by asymmetric encryption based on Elliptic Curve Diffie-Hellman Encryption [26]. Lihua Gong et al. present an encryption scheme based on compressing sensing and RSA algorithm [8]. DENA S. ALANI et al. a new encryption algorithm proposed using a chaotic Henon map with the RC4 algorithm. In the first step of this paper, a new basis is presented to reduce the amount of data required to present the image. In the second step of this paper, the combination of the RC4 algorithm and the chaotic Henon map function is used to generate sub-keys with N rounds. The sub-key is generated to encrypt one block in each round so that N of rounds is equal to N of the blocks for the compressed image [35]. Manju Kumari et al. proposed an image encryption scheme that uses intertwining chaotic maps and RC4 stream cipher to encrypt/decrypt the images. The scheme employs a chaotic map for the confusion stage and the generation of the key for the RC4 cipher.

The proposed methods for digital image encryption should include the following features and specifications [11]: 1) Low correlation: The correlation between the original image and the encrypted image should be below. Ideally, it is close to zero, 2) Large Key Space: To tackle with brute-force attacks, the keyspace should be very large, 3) Key and image sensitivity: The proposed algorithm should be sensitive to key and image changes, in other words, a large change is made in the encrypted image by changing at least a bit of key and image 4) Entropy: A random criterion, which should be close to 8 for cryptography of digital gray-level images with eight-bit pixels, and 5) time complexity or low execution speed.

## 3. The 3D modular chaotic map

In this study, by extending the Arnold cat map we present a three-dimensional chaos mapping based on modular mathematics that includes robust features with increasing keyspace and speed. This 3D mapping can be used to encrypt grayscale images, color images, and video. The 3DMCM is defined by Eq. (3.1).

$$\begin{aligned} X_{m+1} &= (A \times X_m) \bmod n \\ \begin{matrix} X_{m+1} \\ Y_{m+1} \\ Z_{m+1} \end{matrix} &= \left( \begin{bmatrix} a & b & c \\ a & e & f \\ g & h & i \end{bmatrix} \times \begin{bmatrix} X_m \\ Y_m \\ Z_m \end{bmatrix} \right) \bmod n \end{aligned} \tag{3.1}$$

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 56 & 21 & 19 \end{bmatrix} \quad A^{-1} = \begin{bmatrix} 3 & 22 & 11 \\ 63 & 41 & 53 \\ 63 & 1 & 0 \end{bmatrix}$$
$$|A| = 35 \qquad |A^{-1}| = 11$$
$$\gcd(|A| \ , \ 64) = \gcd\left(\left|A^{-1}\right| \ , \ 64\right) = 1$$

Figure 1: Residue Matrix $A$ and its inverse ($A^{-1}$) in modulo 48

In Equation A, the matrix is 3×3 modules n. The proposed three-dimensional turbulence mapping can be reversed if the condition $\gcd(|A| \ , \ n) = 1$ is met. In this case, the inverse is obtained as a relation (3.2).

$$X_{m+1} = \left(A^{-1} \times X_m\right) \bmod n$$
$$\begin{matrix} X_{m+1} \\ Y_{m+1} \\ Z_{m+1} \end{matrix} = \left( \begin{bmatrix} a & b & c \\ a & e & f \\ g & h & i \end{bmatrix}^{-1} \times \begin{bmatrix} X_m \\ Y_m \\ Z_m \end{bmatrix} \right) \bmod n \tag{3.2}$$

*3.1. Linear-feedback shift register Algorithm*

LFSR is a shift register that creates a sequence of binary values. The sequences are repetitive in nature known as pseudorandom sequences. Feedback paths are established after registers in the LFSR structure called taps and constitute exclusive-OR or NOR to make random series. Fig. 2 shows LFSR with XOR configuration. At this point, D flip-flops are used as registers and Q is the output for each register.

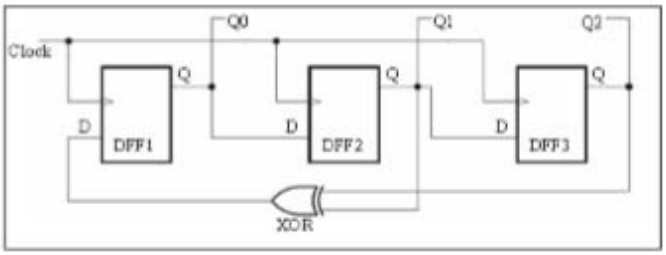


Figure 2: Linear Feedback Shift Register [31]

The created sequence is independent of any other component so that it is random. The sequence is deterministic because after specific elements it again starts its original value. Hence, it is called pseudo. If one knows the present state as well as the positions of the XORs gate in the LFSR architecture, one can predict the next state. The input bits are linear functions of the previous step and functions coming from XORs or XNORs are also linear. An LFSR generates a pseudorandom sequence of length $(2^n - 1)$ states where n is the number of shift registers used in the given LFSR architecture. An LFSR generates all potential values of $(2^n - 1)$ states are called maximal length sequences. The highest length sequence can be obtained by a combination of more than a tap in an LFSR system. A 4-bit shift register with feedback taps at the 3rd and 4th bit is a maximal sequence. The LFSR sequence depends upon initial values (seed value), tap positions, and feedback types. There are two methods for the realization of the LFSR system. One is the Fibonacci configuration and the other one is the Galois configuration shown in Figure 4.1.

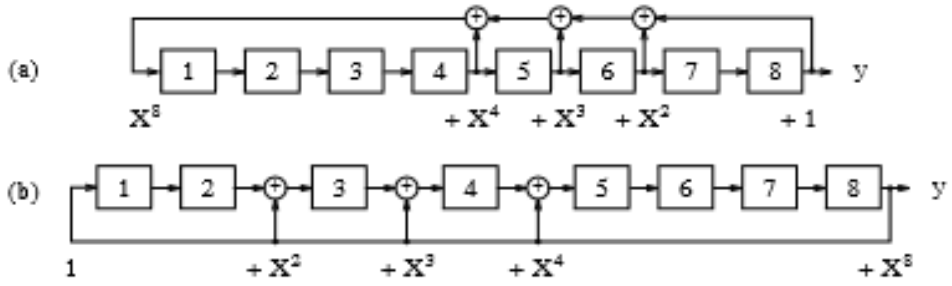


Figure 3: (a) Fibonacci configuration (b) Galois configuration [5]

*3.2. Fast modular inversion algorithm for Hardware implementation*

Suitable for VLSI implementation in this Letter we use a fast algorithm for modular inversion in prime fields (algorithm MIPF), which involves only ordinary addition/subtraction, and does not need any modular operations or multiplication and division by lacking the parallelism of hardware realization into account. The following is the pseudo-code of algorithm MIPF.

Algorithm MIPF.
Input: $p, a$ prime number and $x \in (0\ ,\ p)$
Output: $y$, satisfying $xy \equiv 1 \mod p$
Step 1; Set $u \leftarrow p$ ; $v \leftarrow x$ ; $r \leftarrow 0$ ; $s \leftarrow 1$; if ($x$ is even), go to Step 3; else,
go to Step 4.
Step 2: Set $v \leftarrow -v$
$s \leftarrow ((s >> 1) + p >> 1) + 1$; if ($v$ is even), go to Step 3; else, go to Step 4.
Step4: Set$u' \leftarrow v$ ; $v \leftarrow u - v$ ; $u \leftarrow -u'$ ; $y \leftarrow s$.
Step 5: If ($u = I$), return $y$; else, if ($v > o$), set $r \leftarrow ts$ ; $s \leftarrow r$ ; $r \leftarrow r'$; go to Step 3; else, set $r' \leftarrow s$ ; $s \leftarrow -s - r$ ; $r \leftarrow r'$; go to Step 2

The initial values of the variables are: $u = p, v = x, r = 0$ and $s = 1$, hence two equations hold:

$$xr \equiv u \mod p$$
$$xs \equiv v \mod p$$

It can be seen that (3.1) and (3.2) always hold after each iteration of algorithm MIPF. When the algorithm is finished with $u = I$, we know $xy = 1 mod p$ from (3.1).

## 4. Encryption independent of image size

Fig. 6 presents the general block diagram of the proposed size-independent encryption based on pre-replacement operations, size-independent 3D chaotic mapping, and post-replacement operations. The following parts describe the proposed encryption steps and their reverse operations in detail.

*4.1. Converting a two-dimensional image to a three-dimensional one*

In this step, we convert the 2D image to 3D to perform the next operations in the proposed encryption. In this step, we divide the color image with the size $M \times N$ with three color spectra of red, green, and blue into $m$ below the square image of the size $n \times n$ . In other words, the color image is transformed into a three-dimensional state with dimensions $n \times n \times m$ to optimize computations

```
library IEEE;
use IEEE.STD_LOGIC_1164.ALL;
use ieee.std_logic_arith.ALL;

entity multiple4_1fsr is
   Port ( clk : in  STD_LOGIC;
          y : out  STD_LOGIC_VECTOR (8 downto 1));
end multiple4_1fsr;

architecture Behavioral of multiple4_1fsr is

SIGNAL ff : STD_LOGIC_VECTOR(8 DOWNTO 1) := (OTHERS => '0');
BEGIN
PROCESS
 BEGIN
 WAIT UNTIL clk = '1';
 ff(8) <= ff(4);
 ff(7) <= ff(3);
 ff(6) <= ff(2);
 ff(5) <= ff(1);
 ff(4) <= NOT (ff(7) XOR ff(8));
 ff(3) <= NOT (ff(6) XOR ff(7));
 ff(2) <= NOT (ff(5) XOR ff(6));
 ff(1) <= NOT (ff(4) XOR ff(5));
 END PROCESS ;
PROCESS (ff)
 BEGIN -- Connect to I/O cell
FOR k IN 1 TO 8 LOOP
y(k) <= ff(k);
END LOOP;
 END PROCESS;

end  Behavioral;
```

Figure 4: VHDL code for four-step length-8 LFSR

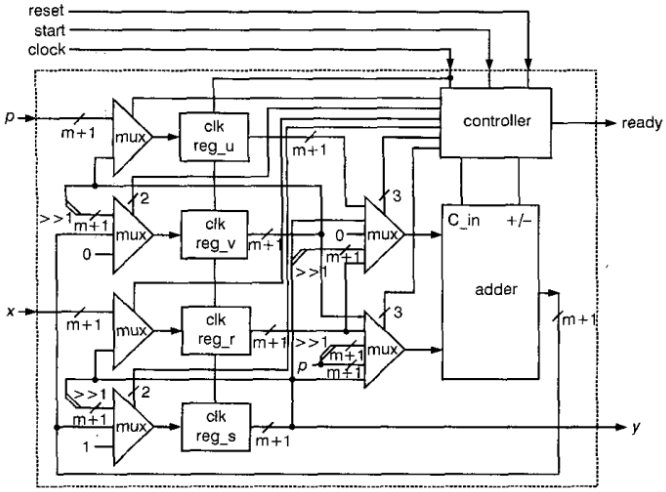


Figure 5: Architecture for hardware implementation

and cryptographic operations, the best choice for m and n parameters is to have the following two conditions together:

1) The total number of the sub-images of the three spectra of red, green, and blue is greater than or equal to the number of rows or columns below the images,

$$3 \times \left\lfloor \frac{M}{n} \right\rfloor \times \left\lfloor \frac{N}{n} \right\rfloor \geqslant n \; or \; 3 \times M \times M \geqslant n^3 \; or \; n \leqslant \left\lfloor \sqrt[3]{3 \times M \times N} \right\rfloor \tag{4.1}$$

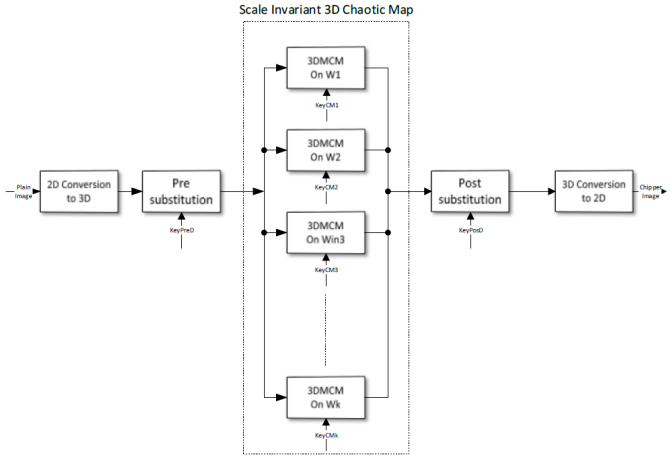


Figure 6: The block diagram of proposed scale-invariant color image encryption

2) Being equal to the relation divisor against the common dimensions of $M$ and $N$. The color image is the largest value of $n$ in the relation (4.1) If $\gcd(M\ ,\ N) = 1$, ($M$ and $N$ are relatively prime) the parameter n is selected, so that the expression $\left[\frac{M+N}{n} - \left\lfloor\frac{M}{n}\right\rfloor - \left\lfloor\frac{N}{n}\right\rfloor\right]$ is minimized.

The optimal parameter m or the total number of images below is gained by selecting the optimal parameter n as a relation (4.2).

$$M = 3 \times \left\lfloor \frac{M+N}{n^2} \right\rfloor \tag{4.2}$$

For instance, for an image of 1920 × 1200, the largest optimal amount of $n$ in the relation (4.1) (true) $n \leqslant 190$ and divisible by the common $M$ and $N$ is $n = 120$. Therefore, if I choose $n = 120$, the following number of Images according to the relation (4.2) (value will be $m = 480$. Figure 3 shows the 3D conversion of a color image to 48 sub-images with size 48 × 48. In this image, the rows and columns of each color spectrum are divided into 4 equivalent parts. After dividing the color image into the sub-images with equal size, sub-images will be arranged in the direction of three axes of $X, Y$, and $Z$, the axes $X$ and $Y$ specify the rows and columns of the sub-images, and the axis $Z$ specifies the sub-image number. As shown in Fig. 7, for processing in the next steps, sub-images are named in row-major order from the red, green, and blue, respectively by $Z_1$ to $Z_m$.

For an image $M \times N$ with sub-images $n \times n$, the relationship between the 2D points $(x, y)$ and the 3D points $(X, Y, Z)$ of the color image is obtained by selecting by LFSR

$$X = x \ mod \ M \tag{4.3}$$

$$Y = y \ mod \ n \tag{4.4}$$

$$Z = RGB \times \left\lfloor \frac{M}{n} \right\rfloor \times \left\lfloor \frac{N}{n} \right\rfloor + \left\lfloor \frac{x}{n} \right\rfloor + \left\lfloor \frac{y}{n} \right\rfloor \times \left\lfloor \frac{N}{n} \right\rfloor \quad RGB \in \{0,\ 1,\ 2\} \tag{4.5}$$

*4.2. The pre-substitution operations*

In the pre-substitution phase, it is possible to change the content of each pixel or group of pixels with the XOR function. In this step below, we will change $Z_1$ to $Z_n$ images of the previous step

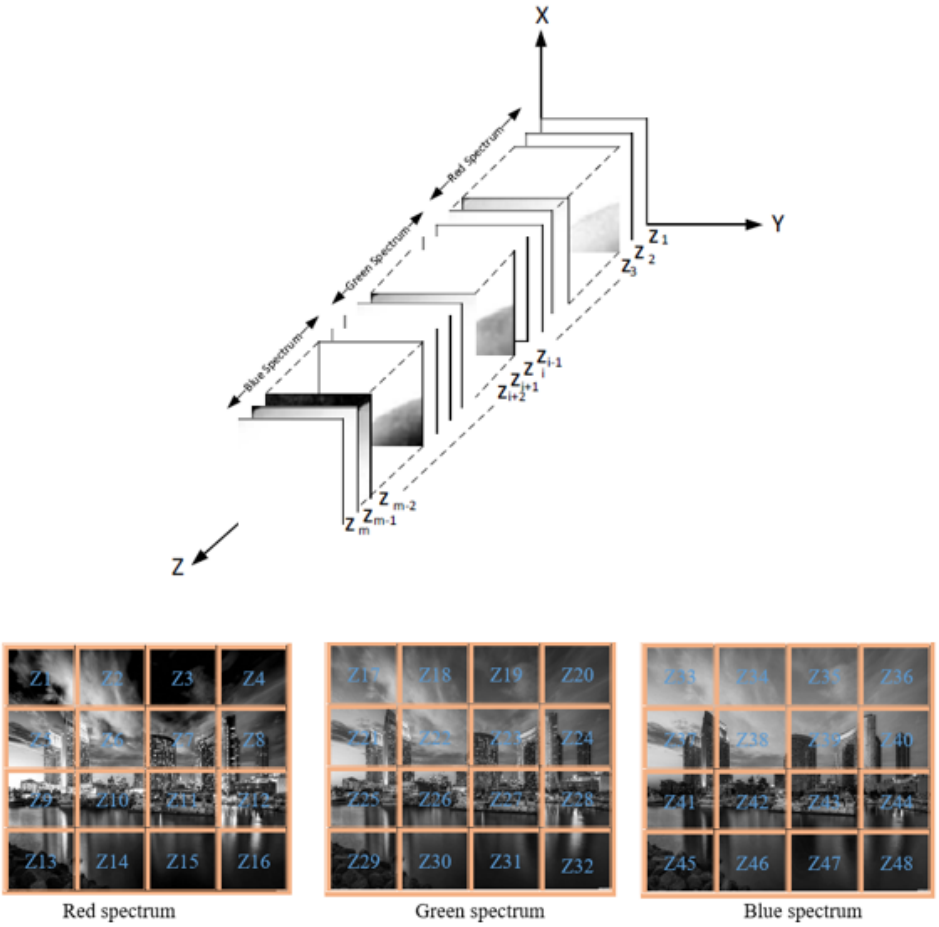


Figure 7: The 3D conversion color image to $n$ sub-images with size $n \times n$

with the help of a key. Starting from below the image $z_{i0}$ shown in Figure 3, we will perform the replacement operation concerning (4.6) below the images

$$Z_i' = \begin{cases} keypreD \oplus Z_i & if\ i = i_0 \\ Z_{i-1}' \oplus Z_i' & other\ wise = i_0;,,.....,... : (i+m) \bmod\ m \end{cases} \tag{4.6}$$

KeyPreD is an $n \times n$ as a pattern in the above relation that is considered a key, $0i$ represents the starting point, $Z_i$ the i-image, and $Z'$ the encrypted i-image. Using the KeyPreD key and the starting point $0i$, the reverse pre-replacement operation is performed by Equation (4.7).

$$Z_i = \begin{cases} keypreD \oplus Z_i & if\ i = i_0 \\ Z_{i-1}^{'\oplus Z_i'} & other\ wise = i_0;,,.....,... : (i+m) \bmod\ m \end{cases} \tag{4.7}$$

In Figure 8, pre-replacement encryption is shown on a 1920 x 1200 image with 480 below the 120 x 120 square image.

### *4.3. Size-independent three-dimensional chaos mapping*

To perform three-dimensional chaotic mapping operations independent of size with the aid of three-dimensional dimensional chaotic mapping with the relation (3.2), initially the third dimension of $Z$, the image is three-dimensional or the same below the images to k window with n below the

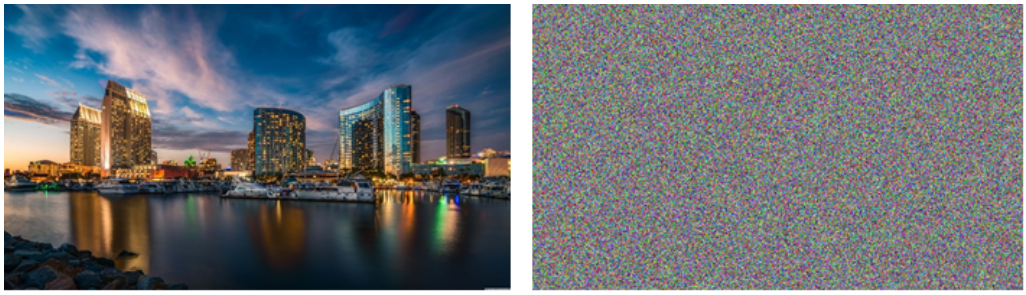

Figure 8: The pre-substitution encryption on a color image with size $1920 \times 1200$

image called $w_1$ to $w_k$. In this respect, the amount of k is gained with the relation $k = [m/n]$. In Figure 9, the division of the three-dimensional image into k window is shown, the value of k includes the following two cases:

1. If $m = n$, the amount becomes $k = 1$, and we have only one $w_1$ window, which occurs when the relation $M = n^3$ is established. For instance, the amount for a $512 \times 512$ image is $n = 64$, and the amount of m is gained by the relation (4.2).

2. If $m > n$, in this case, we have more than two windows, the last two windows $w_{k-1}$ and $w_k$. May overlap under the images. For example, for a $680 \times 480$ image, by selecting the optimal amounts of $n = 40$ and $m = 192$, the relations (4.1) and (4.2) are gained in this number $k = \lceil \frac{192}{40} \rceil = 5$ below the image with windows $W_1$ to $W_5$. The $W_1$ to $W_5$ windows cover the sub-images 1 to 40, 41 to 80, 81 to 120, 121 to 160, and 153 to 192, respectively. The W4 and W5 windows overlap with the 8 sub-images 153 to 160.

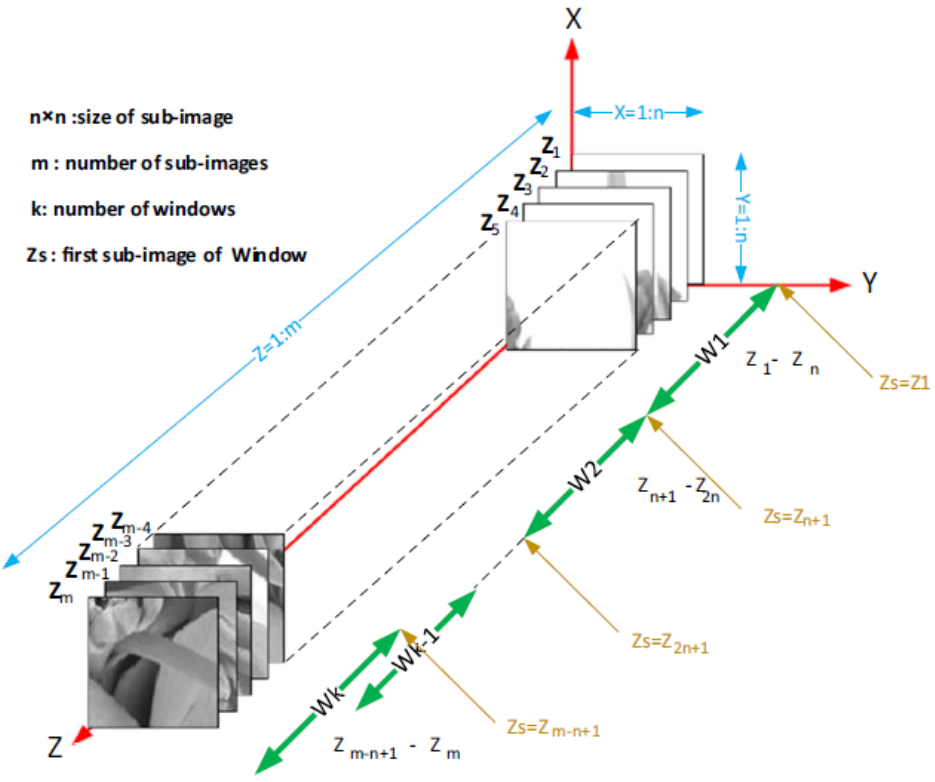


Figure 9: Divide m sub-images to k windows with n sub-images

A three-dimensional chaotic mapping operation is performed on each window using Equation (3.2)

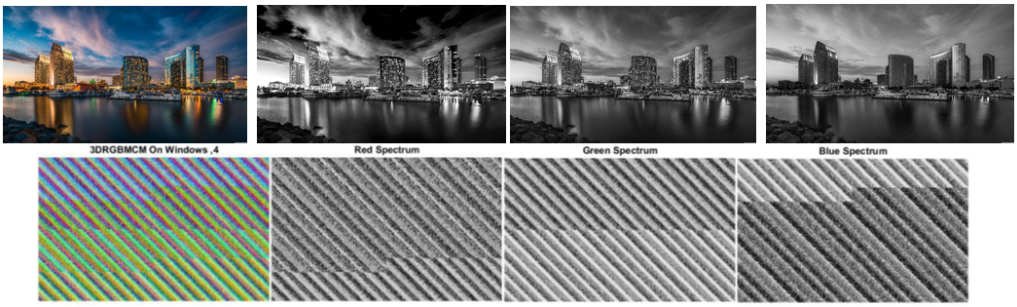


Figure 10: The stages of the 3D modular chaotic map

after the following images have been converted to k windows of n module size. Chaotic mapping parameters used as a key window can be selected differently; after dividing the sub-images into k windows with size modulo n, on each window with n sub-images, a 3DMCM operation is carried out using equation (3.1). The 3DMCM parameters are used as keys, and the 3DMCM operations on each window can be done with different keys. So, selecting the various keys in the 3DMCM on each window will increase the space of the key.

Figure 10 shows the different steps of encryption and decryption of the 3DMCM on a $1920 \times 1200$ image with four steps on windows $W_1$ and $W_4$. With aid size of image ($M = 1920$ and $N = 1200$) SI3DMCM parameters are calculated as follows: $n = 120, m = 480, k = 3, Zs = [1, 76, 118]$.

### *4.4. Post-substitution operations*

In the next step, replacing the contents for each pixel or group of pixels with a circular shift operation to the right or left will change. In this case, the pixels of the color spectrum of the image are verified as a 24-bit number with the help of a suitable key of the circular shift.

For post-replacement and reverse operations, Equations (4.8) and (4.9) are used, respectively, through a circular shift on the following $Z_1$ to $Z_m$ images.

$$Z_i^{'} = ROR\left(Z_i \middle| Z_{\left(\frac{m}{3}+i\right)} \middle| Z_{\left(\frac{2\times m}{3}+i\right)}, KeyPostD(i)\right) \quad (4.8)$$

$$Z_i = ROL\left(Z_i^{'} \middle| Z_{\left(\frac{m}{3}+i\right)} \middle| Z_{\left(\frac{2\times m}{3}+i\right)}^{'}, KeyPostD(i)\right) \quad (4.9)$$

In the above ROR equations, the array keys with the length m by integer amounts between 1 and 24 include the right-hand circular shift function, the left-hand circular shift ROL, and the keyPostD. In each sub-image, the KeyPostD array represents the number of circular bits.

Figure 11 represents the various stages of encryption and decryption of the proposed method according to Figure 3 on a color image with a size of $1920 \times 1200$ step by step.

## 5. Performance evaluation and experimental results

### *5.1. Histogram analysis*

The brightness distribution of the pixels of a digital image is indicated by a histogram. An attacker uses an encrypted image histogram in a statistical attack, and frequency analysis is used to detect the key to encrypt or decrypt image pixels. To prevent statistical attacks, the original

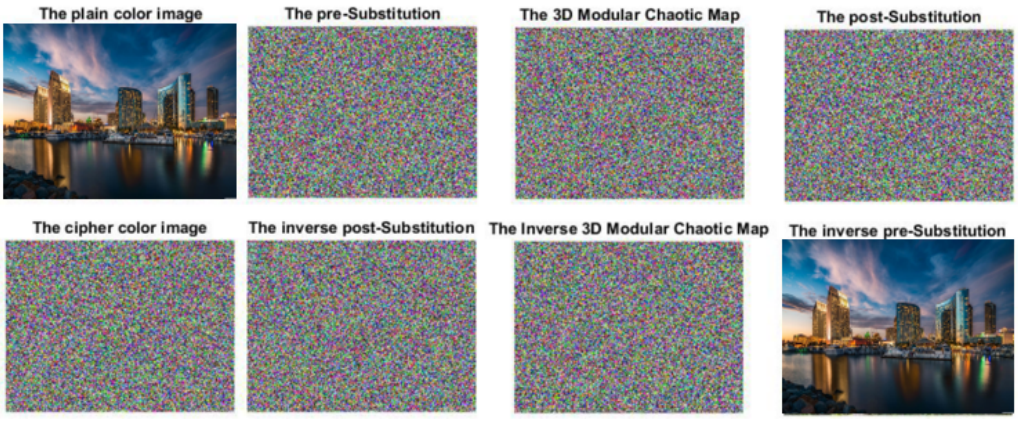


Figure 11: The proposed encryption and decryption on color image $1920 \times 1200$ with 6 windows and sub-images $100 \times 100$

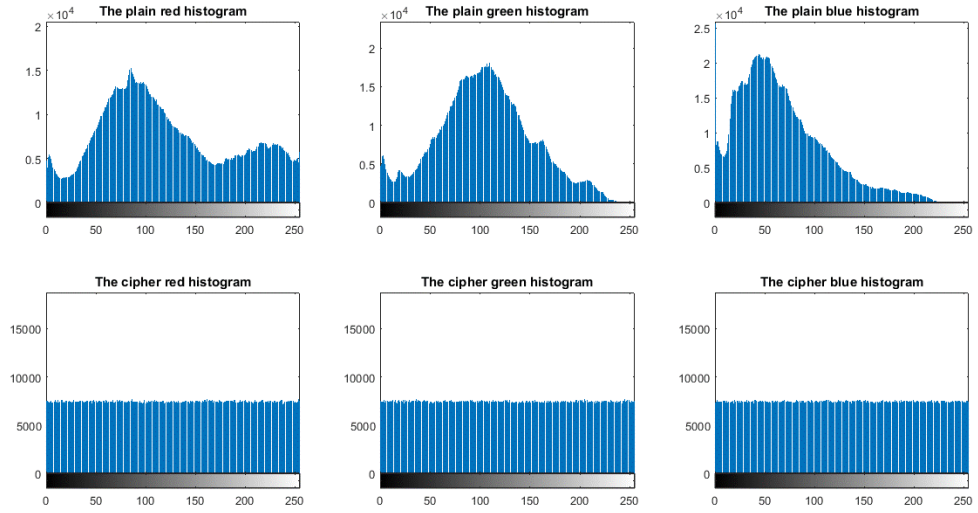


Figure 12: The red, green, and blue components histograms of plain and cipher color images in Figure 11

image histogram and the encrypted image should not be statistically similar to one another. For this purpose, the encoded image histogram should be relatively flat or statistically uniformly distributed [11]. One of the important points in image encryption is that the operation of moving and shifting the pixels will not change the histogram. Therefore, only the operation of publishing and replacing the pixels will make a worthy variety between the histogram of the original image and the encrypted one. The high quality of publication and replacement operations in digital image encryption is reflected by the relatively uniform distribution of encrypted image pixels.

Figure 12 ($1600 \times 1200$ color image) represents Figure 11 before and after encryption with the proposed method. Figure 10 also shows that the pre-replacement and post-replacement operations in the proposed method performed very well in standardizing the encoded image histogram.

### *5.2. Statistical analysis*

The entropy of an image is calculated from the gray surface L by Equation (4.7) [19].

$$H\left(l_i\right) = -\sum_{i=0}^{L-1} P\left(l_i\right) \times \log_2 P\left(l_i\right) \tag{5.1}$$

In the above relation $P(I_i)$, there is a possibility of the occurrence of the i-gray surface that is easily gained from the gray image histogram. The encrypted image can be regarded as an image with completely random amounts; therefore, if the number of gray surfaces is $L = 256$, this value should be close to 8. The entropy of the original image is 7.755, and the red, green, and blue components of the encrypted image of Figure 9 are equivalent to 7.999, which is very close to the ideal value of 8.

Overall, sensitivity to minor changes in the original image and the key is an ideal property for an encrypted image. Produce the initial encryption. An optimal cryptographic system has another important property, which is key sensitivity. In other words, a completely different decoding image is the result of a slight change in the private key.

Very high key sensitivity to some extent ensures the security of the cryptographic system contrary to a comprehensive search attack. To test the sensitivity to the key of the cryptographic design understudy, the test image is encrypted once with the original secret key and once with a bit changed private key.

If it is impossible to visually compare the two cryptocurrencies, then the cryptographic design under study is highly sensitive to the key. Owing to diffusion and clutter, if a minor change in the original image occurs in the image sensitivity process that causes a significant change in the password image, the differential attack loses its effect and is practically useless. This attack may causes a moderate change in the original image and compares the decoded image to it and identifies a significant relationship between them. Sensitivity to minor changes to the key and the initial image is a feature of a good encryption system.

To evaluate the resistance of the procedure to this attack and test the effect of changing one input pixel on the full image encrypted by the proposed algorithm, two integrated averages of change rate, namely UACI, and pixel change rate value, i.e. NCPR, are used. Modified and UACI means the measurement of changes in brightness in an integrated manner, in which the average brightness difference between the two original images and the coded image is calculated [19]. Standard functions of UACI and NCPR evaluation criteria are used to calculate the similarity of the two images. The values of NCPR close to 100 and UACI close to 37 indicate the higher sensitivity of the method than changes to the original image and indicate that the cryptographic algorithm performs better than another method. These two indices are defined according to equations (5.2 (to) 5.4):

$$NCPR = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} D\left(i,j\right) \times 100 \tag{5.2}$$

$$D\left(i,j\right) = \begin{cases} 1 & I_p\left(i,j\right) = I_{enc}\left(i,j\right) \\ 0 & I_p\left(i,j\right) \neq I_{enc}\left(i,j\right) \end{cases} \tag{5.3}$$

$$UACI = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\left|I_p\left(i,j\right) - I_{enc}\left(i,j\right)\right|}{255} \times 100 \tag{5.4}$$

In the above relations, $I_p$ and $I_enc$ specify the original and encrypted image, and M and N specify the size of the original and encrypted image. In Table 1, the performance of both NCPR and UACI methods is compared to that of other algorithms.

### *5.3. Correlation analysis of adjacent pixels Period behavior*

This scale measures in an image the value of dependence or correlation in adjacent pixels The value of the correlation is a number between 1 and -1.

Correlation value 1 indicates a high positive correlation and -1 indicates a low negative correlation. For a good cryptographic algorithm, the correlation amounts are expected to be near zero [19]. In

Table 1: The NCPR and UACI measures

| 2*Encryption method | Red spectrum | | Green spectrum | | Blue spectrum | |
|---|---|---|---|---|---|---|
| | NCPR | UACI | NCPR | UACI | NCPR | UACI |
| Proposed method | 99.58 | 32.4 | 99.52 | 30.25 | 99.28 | 33.79 |
| [18] | 99.62 | 33.42 | 99.6 | 33.43 | 99.61 | 33.4 |
| [4] | 99.59 | 33.28 | 99.61 | 33.53 | 99.58 | 33.33 |
| [16] | 99.6 | 31.55 | 99.61 | 29.29 | 99.61 | 33.69 |

the original image, each pixel strongly correlates with its neighboring pixels, and the dependence of adjacent pixels is usually high. An ideal cryptographic algorithm should produce decrypted images with a low correlation between pixels. To calculate the correlation of adjacent pixels (N), in this paper, 3000 is selected (adjacent pixel pairs are randomly selected from the location of the main image or the encrypted image in horizontal, vertical, or diagonal directions).

We denote these two sets of pixels by the vectors x and y, which we represent as $(x_i, y_i), i = 1, 2, 3 \ldots, N$ with the labels $x = \{x_i\}$ and $y = \{y_i\}$ In this case, the correlations of adjacent peaks are calculated using relations (5.5) to (5.8). To extract the adjacent vectors $x$ and $y$ in the horizontal direction, we select a random number $N$ of the rows of odd and even pairs of the image, respectively. The horizontal direction is randomly extracted from the individual and even columns of the image.

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{5.5}$$

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{j=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{5.6}$$

$$E(x) = \frac{1}{N}\sum_{j=1}^{N} x_i \qquad E(y) = \frac{1}{N}\sum_{j=1}^{N} y_i \tag{5.7}$$

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(x_i - E(x)) \qquad D(y) = \frac{1}{N}\sum_{j=1}^{N}(y_i - E(y)) \tag{5.8}$$

In the above relations, $cov(x, y)$ represents the covariance of the pixel vectors adjacent to $x$ and $y$ from the original or encrypted image, $D(x)$ and $D(y)$ show the variance of the vectors $x$ and $E(x)$, $y$ and $E(y)$, respectively. The average of the vectors $x$ and $y$, and $N$ are the lengths of the vectors. Figure 13 shows the correlation analysis of the original image and the image shown for the three spectra of red, green, and blue. As can be observed, the correlation between adjacent pixels in the original image is very high, and the graph is almost a line with $a + 1$ slope; however, the correlation between adjacent pixels in the encrypted image is reduced, indicating a greater scatter of adjacent pixels in the encrypted image.

*5.3.1. Period behavior of chaotic maps:*

One of the problems associated with the Arnold Cat map is related to points that have zero-period. These points will not be displaced in permutation operations and will have security problems against attacks. With the values of matrix $A$ and modulo(n) of the below table, the period and frequency of points and the points which have zero-period are shown in the next table for the Arnold cat map and

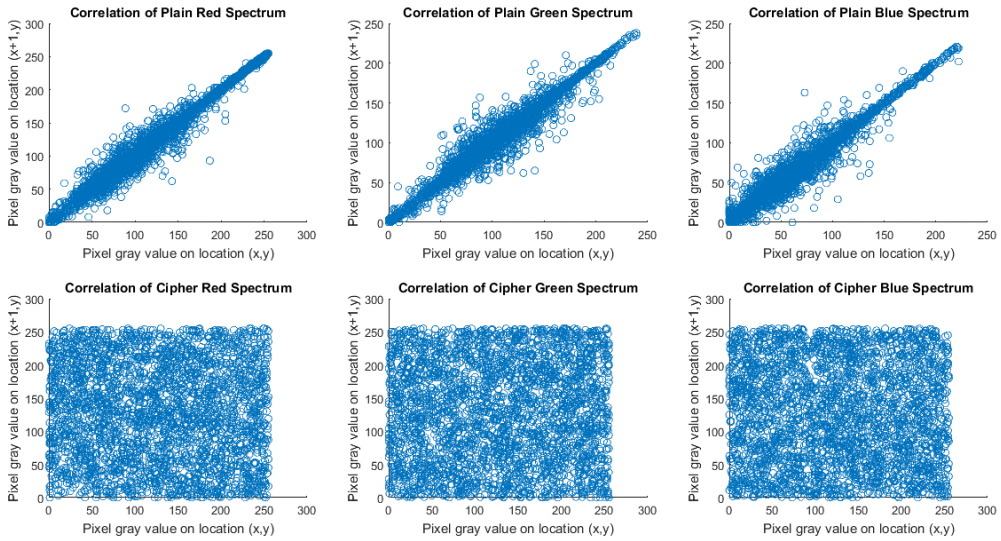


Figure 13: The pixels adjacency correlation of red, green, and blue spectrums of plain and cipher images Figure 8

3DMCM. As shown in the table, the Arnold cat map has 8 points with zero-period, the 3DMCM has zero-period only at the starting point. As a result, the periodic behavior of modular chaotic maps has outperformed the Arnold cat map. These points can be permuted before or after mapping by a suitable key for solving the problem with points with zero-period.

Table 2: Chaotic maps period

| Modulo ( n ) | Chaotic map | Matrix A | Average period |
|---|---|---|---|
| 64 | Arnold cat | $\begin{bmatrix} 1 & 7 \\ 8 & 57 \end{bmatrix}$ | 41.8574 |
| 64 | 3D modular chaotic map | $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 56 & 21 & 19 \end{bmatrix}$ | 208.0667 |

Table 3: Period of points, frequency of them, and zero period points

| Modulo ( n ) | Chaotic map | Period | Freq. | Zero-period points |
|---|---|---|---|---|
| 64 | Arnold cat | 0 | 8 | (0.0)(8.0)(16.0)(24.0)(32.0) (40.0)(48.0)(56.0) |
| 64 | 3D modular chaotic map | 0 | 1 | (0.0.0) |

### *5.4. Keyspace Analysis*

The keyspace of cryptographic steps and n, m three-dimensional parameters is one of the things that keyspace depends on as the presented cryptographic method.

The keyspace of the pre-replacement stage depends on the number of keyPreD key states, and the starting point in the relation (4.3), in this case, the keyspace as a relation (5.9), is obtained.

$$KeySpacePreD = (256)^n \times n^2 \times m = 2^{8n} \times n^2 \times m \tag{5.9}$$

In the above relation, $2^{8n}$ specifies the number of $KeyPreD$ key modes and n2m as the number of starting point modes.

The number of shiftable bits that can be changed and the following number of images m are some of the things that the key processing space of the post-processing stage depends on, which is gained through the relation (5.10):

$$KeySpacePreD = 23 \times \frac{m}{3} \cong 8 \times m \tag{5.10}$$

The key space of the permutation phase with the aid of three-dimensional chaos maps depends on the three-dimensional chaos key space and the number of windows k. If the parameter n is a three-dimensional chaotic mapping of the number (if it is not the first, the keyspace will be less than the value and its exact calculation is complex in terms of n (the three-dimensional chaotic mapping keyspace of the module is obtained by relation (5.8).

$$KeySpaceMCM = (n)^9 \times n^2 \times m = n^{11} \times m \tag{5.11}$$

In the above relation, $n^9$ indicates the number of states of the residual matrix $A$, and $n2m$ determines the number of states of the mapping point.

The total keyspace of the proposed method is obtained by the relation (5.9) to (5.11) (according to the number of k windows used in chaos mapping) and the relation (5.12):

$$\begin{aligned} KeySpace &= KeySpacePreD \times (KeySpaceMCM)^k \times KeySpacePostD \\ &= 2^{8n} \times n^2 \times \left(m \times n^{11}\right)^k \times m \times 8 \times m = 8 \times 2^{8n} \times n^{11+k+2} \times m^{k+2} \end{aligned} \tag{5.12}$$

The keyspace for an image is $1920 \times 1200$ with the parameters $n = 120, m = 480$, and $k = 4$ The keyspace is equal to $4.15 \times 10^{401}$ . Table 4 compares the keyspace of the presented method to that of other methods. Owing to the dependence of the keyspace of the proposed method on $m, n$, and $k$ parameters in this table, the average amount measured from some images is given.

Table 4: Evaluation and comparison of a keyspace

| | |
|---|---|
| The proposed method | $4.15 \times 10^{401}$ |
| Maximum review reference keyspace [11] | $7.2 \times 10^{218}$ |
| [35] | $8.3 \times 10^{54}$ |
| [25] | $3.9 \times 10^{341}$ |
| [16] | $2.3 \times 10^{218}$ |

## 6. Conclusion

A scale Invariant image encryption and decryption scheme based on a 3D modular chaotic map is investigated. The proposed method contains three main steps: pre substitution, scale-invariant

3D chaotic map, and post substitution that reached optimal parameters such as NPCR, UACI, and entropy with at least one rounds repetition. Also, it's good pass histogram uniformity analysis tests and has suitable results adjacency pixels correlation. The simulation results and performance evaluations demonstrate that the proposed scale-invariant image encryption and decryption scheme is secure with high key and plaintext sensitivity, high keyspace, and suitable periodic behavior by reducing zero-point periods to one point. As a result of that its resists and is robust against to brute-force attack, chosen-plaintext attack, and statistical analysis attack

## References


[1] Sh. Agarwal, *A Review of Image Scrambling Technique Using Chaotic Maps*, International Journal of Engineering and Technology Innovation, 8 (2) (2018) 77-98.

[2] X. Chai, X. Fu, Zh. Gan, Y. Lu and Y. Chen, *A color image cryptosystem based on dynamic DNA encryption and chaos*, 155 (2019) 44-62.

[3] 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*, 142 (2018) 340-353.

[4] B. Chen, M. Yu, Y. Tian, L. Li4, D. Wang, X. Sun, *Multiple-parameter fractional quaternion Fourier transform and its application in color image encryption*, IET Image Process., 12 (12) (2018) 2238-2249.

[5] R. Enayatifar, H.J. Sadaei, A.H. Abdullah, M. Lee and I.F. Isnin, *A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata*, 71 (2015) 33-41.

[6] C. Fu, J. Chen, H. Zou, W. Meng, Y. Zhan and Y. Yu, *A chaos-based digital image encryption scheme with an improved diffusion strategy*, Opt. Express 20 (3) (2012) 2363-2378.

[7] Zh. Hua, F. Jin, B. Xu and H. Huang, *2D Logistic-Sine-coupling map for image encryption*, Elsevier, Signal Processing 149 (2018) 148-161.

[8] Z. Hua and Y. Zhou, *Design of image cipher using block-based scrambling and image filtering*, 396 (2017) 97-113.

[9] D. Jiang, Y. Chen, X. GU, L. Xie and L. Chen, *Efficient and universal quantum key distribution based on chaos and middleware*, 31 (2) (2017)1650264.

[10] A. Jolfaei and A. Mirghadri, *An Image Encryption Approach using Chaos and Stream Cipher*, Journal of Theoretical and Applied Information Technology, 117-123.

[11] M. Kumari, Sh. Gupta and P. Sardana, *A Survey of Image Encryption Algorithms*, Springer, 3D Research 8 (37) (2017).

[12] A. R. Lan, J. He, Sh. Wang, T. Gu and X. Luo, *Integrated chaotic systems for image encryption*, 147 (2018) 133-145.

[13] C. Li, Y. Liu, T. Xie and M.Z.Q. Chen, *Breaking a novel image encryption scheme based on improved hyperchaotic sequences*, 73 (3) (2013) 2083-2089.

[14] C. Li, *Cracking a hierarchical chaotic image encryption algorithm based on permutation*, 118 (2016) 203–210. https://doi.org/10.1016/j.sigpro.2015.07.008.

[15] M. Liu, S. Zhang, Z. Fan, M. Qiu, *H∞ state estimation for discrete-time chaotic systems based on a unified model*, IEEE Trans. Syst. Man Cybern, Part B 42 (4) (2012) 1053-1063.

[16] A. Momeni Asl, A. Broumandnia and S. J. Mirabedini, *Scale-Invariant Digital Color Image Encryption Using a 3D Modular Chaotic Map*, in IEEE Access, 9 (2021) 102433-102449, DOI: 10.1109/ACCESS.2021.3096224.

[17] M.A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gutiérrez and O.R. Acosta Del Campo, *A RGB image encryption algorithm based on total plain image characteristics and chaos*, 109 (2015) 119-131.

[18] X. Wang and Zh. Li, *A color image encryption algorithm based on Hopfield chaotic neural network*, Optics and Lasers in Engineering 115 (2019) 107-118.

[19] X. Wang, P. Li, Y. ZhangLi, Y. Liu, H. Zhang and X. Wang, *A novel color image encryption scheme using DNA permutation based on the Lorenz system*, Multimedia Tools and Applications, 77 (5) (2018) 6243-6265.

[20] X. Wang, Y. Zhang and Xue-Mei Bao, *A Colour Image Encryption Scheme Using Permutation-Substitution Based on Chaos*, 17 (2015) 3877-3897.

[21] E.Y. Xie, C. Li, S. Yu and J. Lü, *on the cryptanalysis of Fridrich's chaotic image encryption scheme*, 132 (2017) 150-154.

[22] L. Xu, Z. Li, J. Li and W. Hua, *A novel bit-level image encryption algorithm based on chaotic maps*, 78 (2016) 17-25.

[23] P. PING, J. YANG FAN, Y. CHI MAO, F. XU and Z. GAO *A chaos-based image encryption scheme using digit-level permutation and block diffusion*, IEEE Access, 2019.

[24] P. R. Sankpal and P. A. Vijaya, *Image Encryption Using Chaotic Maps: A Survey*, 2014.
[25] L. Skanderova and I. Zelinka, *Arnold cat map and Sinai as chaotic numbers generators in evolutionary algorithms*, In: AETA 2013, Recent Advances in Electrical Engineering and Related Sciences, (2014) 381-9.
[26] B. Yang and X. Liao, *A new color image encryption scheme based on the logistic map over the finite field ZN*, Multimedia Tools and Applications, 77 (16) (2018) 21803–21821.
[27] G. Ye and X. Huang, *Spatial image encryption algorithm based on chaotic map and pixel frequency*, Sci. China-Inf. Sci. 61 (5) (2018) 058104.
[28] Y. Zhang and D. Xiao, *An image encryption scheme based on rotation matrix bit-level permutation and block diffusion*, Communication Nonlinear Science Numer. Simul. 19 (1) (2014) 74-82.
[29] Y. Zhang, D. Xiao, Y. Shu and J. Li, *A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations*, Signal Processing Image Communication. 28 (3) (2013) 292-300.
[30] Y.Q. Zhang and X.Y. Wang, *A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice*, Inf. Sci. 273 (2014) 329-351.
[31] Y.Q. Zhang and X.Y. Wang, *A new image encryption algorithm based on non-adjacent coupled map lattices*, Appl. Soft Comput. 26 (2015) 10-20.
[32] N. Zhou, Y. Hu, L. Gong and G. Li, *Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations*, Quantum Inf. Process. 16 (6) (2017) 164.
[33] Y. Zhou, K. Panetta, S. Agaian and C.L.P. Chen, *Image encryption using P-Fibonacci transform and decomposition*, 285 (5) (2012) 594-608.
[34] Y. Zhou, L. Bao and C.L.P. Chen, *Image encryption using a new parametric switching chaotic system*, 93 (11) (2013) 3039-3052
[35] H. Zhu, Y. Zhao and Y. Song, *2D logistic-modulated-sine-coupling logistic chaotic map for image encryption*, IEEE Access, 7 (2019) 14081-14098.