DOI: https://doi.org/10.33103/uot.ijccce.22.2.1

Color Visual Cryptography Based on Three Dimensional Chaotic Map

Shaymaa A. Fadhil[1], Alaa K. Farhan[2]
[1,2]Department of Computer Science, University of Technology, Baghdad, Iraq
[1]shaymaaammar55@gmail.com, [2]Alaa.k.farhan@uotechnology.edu.iq

Abstract*— Cryptographic approaches based on chaos theory provide a several new and promising avenues for developing safe picture encryption solutions. This paper aims to complicate the process of decrypting images by adding encryption with keys, this was achieved by applying the principle of the 3D-chaotic system with the encryption algorithm, so we present an image encryption algorithm called black mask by using an efficient Multidimensional Chaotic Map represented by Lorenz system. For the confusion process, the suggested approach is based on a keys stream generator. The process of confusion is initiated by a 256-bit secret keys, which is produced by a logistic maps. To make the cipher more dynamic in the face of any threat. The suggested digital image encryption technique, as well as its security analysis and implementation, are discussed in depth. The experimental results suggest that the proposed method for image encryption and transmission is both efficient and safe.*

Index Terms*— Chaotic Maps, visual Cryptography, confusion, diffusion.*

I. INTRODUCTION

Visual cryptography is a cryptographic approach that encrypts visual data in such a way that decryption is a mechanical process that does not require the use of a computer [1]. The secret image is the first piece of information that needs to be encrypted. After encryption, ciphers are generated and referred to as shares. Sharing refers to the portion of confidentiality that has been jumbled. Visual cryptography is based on the concept of sharing a secret among groups of people [2].

Due to its complex features, pseudo unpredictability, and severe sensitivity to their initial values and settings, chaotic systems have been widely used in digital picture encryption [3]. Scrambling refers to the permutations of pixel values or permutation of bit values in a bit plane. Transforming a plain image into a meaningless noise and eliminate the high correlation between adjacent pixels are the objective of scrambling. Various image scrambling techniques are used in image and video encryption [4]. To make the method more complex and difficult to crack, we present a visual cryptography technique based on a multidimensional chaotic map in this study.

The following is how the paper will be organized: Section II deals with the related works in image encryption using chaos approach, Section III define the chaos approach and its types used in encryption, section IV describes the proposed digital picture encryption method based on the Lorenz system, discusses the proposed digital image encryption algorithm's experimental results in section V. Sections (VI and VII) offer the security analysis and conclusion, respectively.

II. RELATED WORK AND BACKGROUND IN CHAOTIC IMAGE ENCRYPTION

Low-dimensional chaotic sequences have a number of issues, for example, the password cycle is short and inaccurate, making the picture encryption algorithm's security

Received 24/August/2021; Accepted 4/December/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.2.1

impossible to ensure. When compared to a chaotic attractor, a hyper chaotic attractor can exhibit more dynamic phenomena and has a higher randomness. As a result, in recent years, encryption methods based on hyper chaotic systems have become a research focus [5]. In [3], S.C. Wang et al. presented An picture encryption technique based on the Knuth–Durstenfeld algorithm and a hidden attractor chaos system. To encrypt digital images, first a hidden attractor chaos system is used. Second, the Knuth–Durstenfeld algorithm is sufficiently random. Finally, image pixel values are diffused using DNA sequence procedures. Meanwhile, H. Liu et al. [6] devised a color image-based encryption technique in which bit-level permutation is utilized for scrambling and a piece-wise linear chaotic map is used for permutation. Some writers provided hyperchaotic chaotic maps and picture encryption techniques in addition to simple chaotic systems. As an instance, M. Zhou et al. [7] proposed an image encryption strategy based on a conservative hyper-chaotic system with closed-loop diffusion between blocks (for changing pixels in blocks process).

III. CHAOS THEORY

The mathematical investigation of nonlinear dynamic systems gave rise to chaos theory. When used in management, it allows for the resolution of problems including complex interconnections and unpredictability. Chaos theory, sometimes known as deterministic chaos, may be traced back to mathematician Henri Poincare, who worked at the end of the 19th century, and meteorologist Edward Lorenz, who worked more recently. They discovered that, starting from essentially similar conditions, the behavior of low-dimensional systems (systems that can be represented by a small number of variables, such as less than six) can diverge substantially [8].

A. Types of chaotic maps

Some chaotic systems are used in chaos theory-based picture encryption techniques. Classic Logistic map, ten map, Sin map, Chebyshev map, and others are examples of one-dimensional chaotic maps. Henon map is one example of a two-dimensional chaotic system. Lorenz map, for example, is a hyperchaotic system. Have spatiotemporal chaotic systems in various dimensions, as well [9]. For their comparatively simple structure and application, several academics focus on one-dimensional (1-D) chaotic maps. The parameter range for the Logistic map to exhibit chaotic behavior, on the other hand, is extremely limited. Most 1-D chaotic maps, despite their low processing cost, lack complicated parameter structure and hyperchaotic behavior. Many researchers are turning to multi-dimensional chaotic systems as an alternative [10]. Edward N. Lorenz published the first study of three-dimensional chaotic systems in 1963. Many other three-dimensional chaotic attractors have been proposed since then, including a system of three nonlinear ordinary differential equations first examined by Otto Rössler in 1976 [11].

IV. PROPOSED DIGITAL IMAGE ENCRYPTION ALGORITHM

The purpose of this research is to offer a new digital picture encryption technique that is based on black mask algorithm and Lorenz chaotic system as shown in *Fig. 1*. Unpredictability, confusion, and diffusion-like features, as well as sensitivity to initial circumstances and parameters, are all advantages of the Lorenz chaotic map. The suggested algorithm for digital picture encryption consists mainly of three phases: first: using the black mask algorithm presented by “Young-Chang Hou” in 2003 [12], apply scramble process on the share extracted from the black mask algorithm in the first phase, finally: generation of new secret keys from the logistic map, and encrypting the four shares

Received 24/August/2021; Accepted 4/December/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.2.1

generated from the past phases (C,M,Y,K) using chaotic sequences that generate from the Lorenz system.

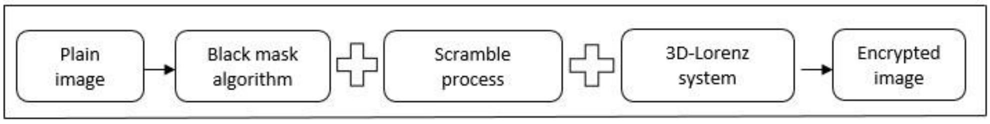


FIG. 1. BASIC SCHEMATIC CHART OF PROPOSED IMAGE ENCRYPTION SYSTEM.

Below, we will first recall the definitions of the basic phase's .Then, we will go into the specifics of putting the above encryption processes into action. The decryption process will also be detailed for completeness.

A. Black Mask Encryption Algorithm

The procedure shown in *Fig. 2* is used in this method .to convert a color hidden picture to three halftone images in Cyan, Magenta, and Yellow Then, using approach shown in *Fig. 3*, Each halftone pixel is enlarged to a block of 2*2 , from which a color is allocated. As a result, two blank pixels and two color pixels are present in each block of the sharing pictures, ensuring the entropy is maximized and the secret picture's contents is hidden. Moreover, create a mask with half (black and white) to shade unintended colors within the overlaying sharing pictures, ensuring that just an intended colors appear.

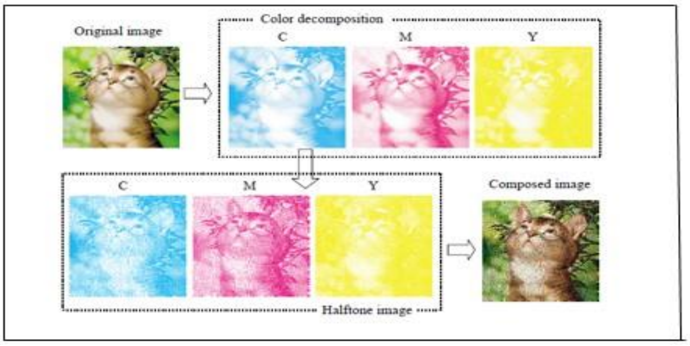


FIG. 2. COLOR IMAGE PRINTING [12].

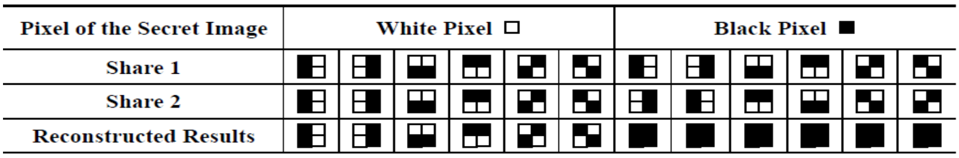
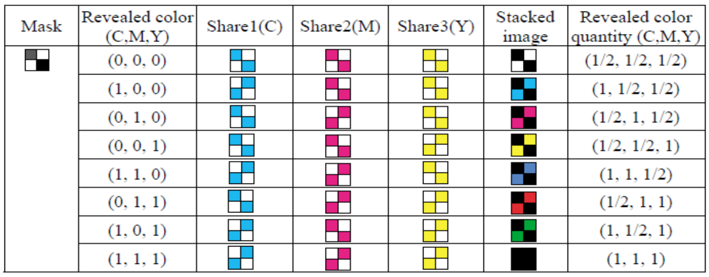


FIG. 3. BLACK AND WHITE PIXELS ARE SHARED AND STACKED IN THIS PATTERN [13].

Consider *Fig. 4* the distribution of color pixels in the three sharing images is attributed to the first row in *Fig. 4* whether pixel pij of the assembled picture is (0, 0, 0,). On the three sharing photos, black pixels shade all of the color pixels. After being layered via the mask picture, revealing only a white pixels, resulting in a white-like color, just C and M elements are visible when pixel Pij is (1; 1; 0), together with the Y element hidden behind the black mask. Thus, there are 6 (C= (4; 2)) alternative distributions of black pixels in the mask in this manner, each corresponding to a distinct distribution of Shares 1, 2, and 3. To increase the difficulty of cracking, we have the option of picking the mask and the share distribution at random [12].

Received 24/August/2021; Accepted 4/December/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.2.1



Mask	Revealed color (C,M,Y)	Share1(C)	Share2(M)	Share3(Y)	Stacked image	Revealed color quantity (C,M,Y)
	(0, 0, 0)					(1/2, 1/2, 1/2)
	(1, 0, 0)					(1, 1/2, 1/2)
	(0, 1, 0)					(1/2, 1, 1/2)
	(0, 0, 1)					(1/2, 1/2, 1)
	(1, 1, 0)					(1, 1, 1/2)
	(0, 1, 1)					(1/2, 1, 1)
	(1, 0, 1)					(1, 1/2, 1)
	(1, 1, 1)					(1, 1, 1)

FIG. 4. SCHEME OF COLOR CRYPTOGRAPHY [12].

B. Scrambling process

Image scrambling (a type of encryption) is an useful way to secure image data by rendering it visually unreadable and making it difficult to decrypt for unauthorized users , To make the visual content unreadable, many image scrambling techniques are used [14].

The image scrambling method is characterized as a reversible transformation that transforms an image into an entirely other, meaningless image. By scrambling a picture, the ability to withstand unwanted attacks and, as a result, enhance security can be efficiently acquired [15]. In our method we create an index table in random way and use it as index to scramble the position of the image pixels.

C. Lorenz chaotic system

Edward Lorenz introduced the Lorenz Chaotic system in 1960. This dynamical system's non-linear ordinary differential system is given as follows [16]:

$$\begin{aligned} \frac{dx}{dt} &= a\,(Y - X) \\ \frac{dy}{dt} &= (\sigma - Z)\,X - Y \qquad\qquad (1) \\ \frac{dz}{dt} &= XY - bZ \end{aligned}$$

Equation (1) above describe the 3D-Loranz system equation where X (0) = x0, Y (0) = y0, Z (0) = z0, are the initial values. When simulated on a computer, these equations, now known as the 3D-Lorenz system, looked to have difficult solutions. They describe fluid flow in atmospheric layers that is akin to convection and is utilized in weather forecasting. With the parameters a = 10, b = 28, and σ = 8/3, Lorenz discovered that the x, y, and z solution-curves circle around two equilibrium points. Following that, he demonstrated that even little changes in the parameters and/or initial conditions result in completely distinct solution-curves [17].

D. Encryption process

The encryption process of the proposed encryption method is described in this section. *Fig. 5* depicts the proposed encryption algorithm flow chart. Where first, apply a black mask algorithm on the original image in order to generate four shares. Second, perform a scrambling process on the pixels of shares (C, M, Y, K,) that generate from the black mask algorithm to making it difficult to decrypt for unauthorized users. Third, apply Lorenz system on the shares (C, M, Y, K,) that generated from the second phase (scrambling process) in order to make the encrypted image more complex and hence more secure. We receive four shares (C, M, Y, and K), which represent the final encrypted image, after performing three stages of the encryption system (black mask algorithm, scramble process,

Received 24/August/2021; Accepted 4/December/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.2.1

and Lorenz system) to encrypt the original image. These shares will be transferred to the intended recipient.

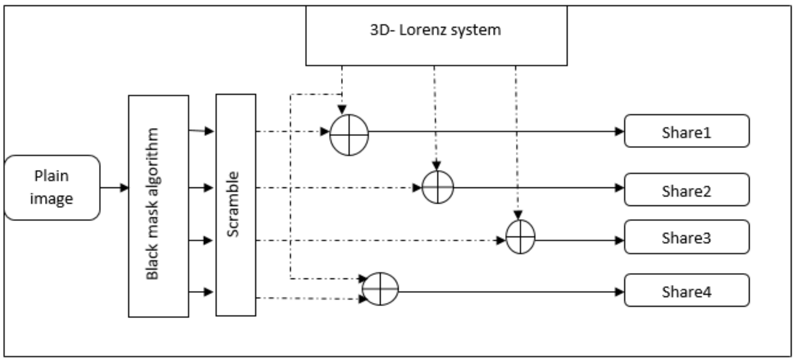


FIG.5. THE PROPOSED ENCRYPTION ALGORITHM FLOW CHART.

```
Algorithm(1): Key Generation Algorithm Using 3-D Lorenz Chaotic Map
Input: Three Equations (3.1), three initial values(x, y, z), initializing constants      (a, b, $\sigma$), Image Size
Output: Key 1, Key 2, Key 3
Begin
dt = 0.01
Step 1: Initializing three empty lists (xs, ys, zs)according to the size of the image, and assign three initial values (x, y, z) to the first location in each list
xs[0], ys[0], zs[0] = (x, y, z)
Step 2: Initializing constants:
a = 10, b = 28, $\sigma$ = 2.667
Step 3: Perform the system of equations (1) to generate three keys sequence in loop according to the image size
End
```

```
Algorithm(2): Encryption Algorithm of Black Mask Algorithm Using Scramble Process and 3-D Lorenz Chaotic Map
Input: Color Image As An Original Secret Image, Three initial values(x, y, z), Scrambled Share Size, Scrambled Share 1, Scrambled Share 2, Scrambled Share 3, Scrambled Share 4
Output: Final Share 1, Final Share 2, Final Share 3, Final Share 4
Begin
Step 1: Read Secret image Pixel by Pixel
    • Using the CMYK color model, an image broken down into its basic primary color channel components.
Step 2: Each primitive-color image is dithered, resulting in two color levels for each image, the presence or absence of the corresponding primitive color.
Step 3: There are eight possible combinations based on the pixel values of three halftone photos. As illustrated in FIG. (4), shares are constructed differently for each of these combinations.
    • Read halftone images
    • for x in range of number of rows
    • for y in range number of columns
    • pixel color = halftone image.getpixel((x, y))
    • if pixel color[C]+pixel color[M]+pixel color[Y] == 0 then
      DO
```

Received 24/August/2021; Accepted 4/December/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.2.1

```
    share.putpixel((x * 2, y * 2), (255,0,0,0))
    share.putpixel((x * 2 + 1, y * 2), (0,0,0,0))
    share.putpixel((x * 2, y * 2 + 1), (0,0,0,0))
    share.putpixel((x * 2 + 1, y * 2 + 1), (255,0,0,0))
else:
    share.putpixel((x * 2, y * 2), (0,0,0,0))
    share.putpixel((x * 2 + 1, y * 2), (255,0,0,0))
    share.putpixel((x * 2, y * 2 + 1), (255,0,0,0))
    share.putpixel((x * 2 + 1, y * 2 + 1), (0,0,0,0))
End if
    • Repeat Step 3 for each halftone image until complete, so generate four CMYK shares.
Step 4: In order to scramble a pixels of the shares do the following:
    • Store the pixels of the image in buffer (pxs).
    • Generate a list of random numbers according to the size of the image (idx).
    • Shuffling (idx) in random way.
    • out = []
      for i in idx:
          out.append(pxs[i])
      return out
    • Repeat step 4 for each shares.
Step 5: Apply XOR operation between the first key that generated from the first equation in
(1) with the first share (Cyan) pixel value to get a new pixels
Step 6: Apply XOR operation between the second key that generated from the second equation
in (1) with the second share (Magenta) pixel value to get a new pixels
Step 7: Apply XOR operation between the third key that generated from the third equation in
(1) with the third share (Yellow) pixel value to get a new pixels
Step 8: Apply XOR operation between the first key that generated from the first equation in
(1) with the fourth share (Black) pixel value to get a new pixels
End
```

E. Decryption Process

The proposed encryption strategy is reversed in the decryption scheme. *Fig*. 6 depicts the decoding of images. Where the four shares (C, M, Y, K,) that represent the cipher image undergo again to (3D-Lorenz system, unscramble).respectively and finally use stack process in black mask algorithm on the entire four share to Restore the original image.

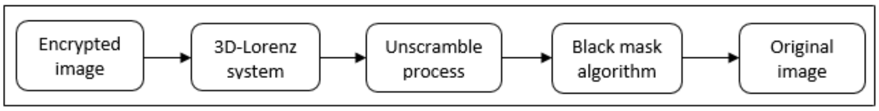


FIG. 6. DECRYPTION SCHEME OF THE PROPOSED IMAGE ENCRYPTION ALGORITHM.

V. EXPERIMENT RESULTS

Some experimental results are presented in this section. For evaluating the proposed image encryption's performance algorithm, the test image is used for the experimental analysis “happy faces” (1280*1145 pixel), as shown in *Fig*. 7 .The simulation is done in Python 3.8 to implement the entire encryption/decryption process. In *Fig*. 7, the matching encrypted image using the black mask algorithm is depicted in four shares (cyan, magenta, yellow, and black).

Received 24/August/2021; Accepted 4/December/2021

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.2.1

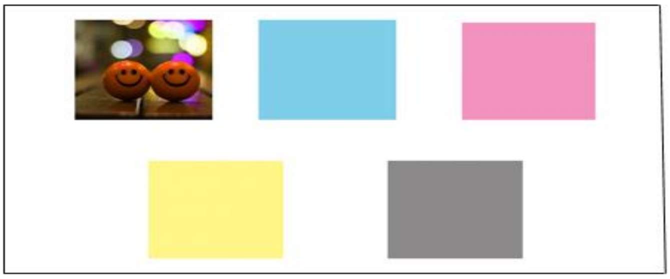


FIG. 7. ORIGINAL AND ENCRYPTED IMAGE REPRESENTED BY SHARES (C M Y K) RESPECTIVELY.

The result of applying scramble process on the pixels of these four share is represented in *Fig. 8*.

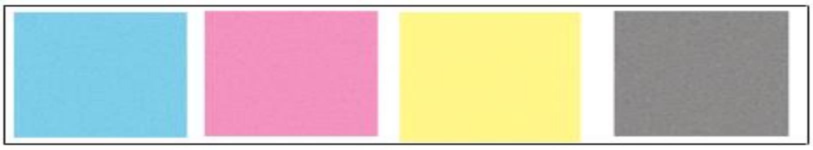


FIG. 8. SCRAMBLED SHARES (C M Y K).

Perform Lorenz system on the shares from previous scramble process by using the following initial values and parameters: a = 10, σ = 8/3, b = 28 and X0=0.01, Y0=0.02, Z0= 0.03. The shares are illustrated in *Fig*. 9 below:

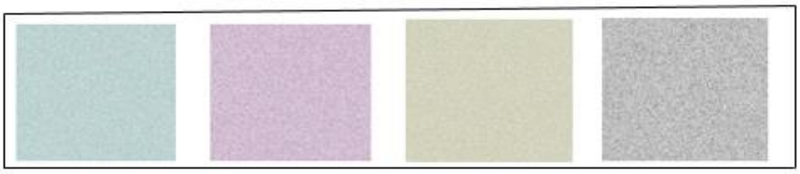


FIG. 9. SHARES AFTER PERFORM LORENZ SYSTEM.

Fig. 10 illustrate the decrypted image after apply a black mask algorithm on the original image only, whereas *Fig. 11* shows the decrypted image after performing the reverse process in each step of the proposed algorithm, where the size of decrypted images (2560*2290 pixel) is twice as original image because the effect of black mask algorithm where each pixel expanded to 2*2 block.

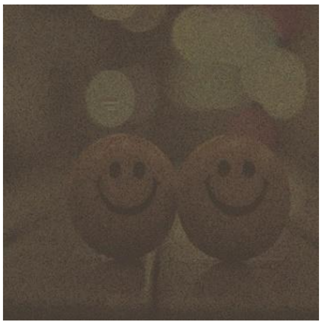


FIG. 10. DECRYPTED IMAGE FROM BLACK MASK ALGORITHM.

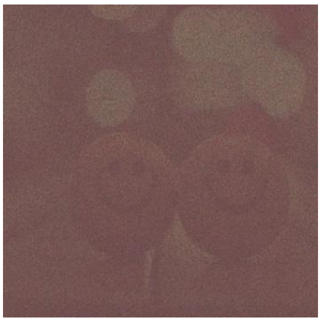


FIG. 11. FINAL DECRYPTED IMAGE.

Received 24/August/2021; Accepted 4/December/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.2.1

VI. SECURITY ANALYSIS

In this section, we look at the suggested digital image encryption algorithm's security and performance. Below are a series of standard tests and analyses.

F. Mean Square Error (MSE)

The mean-square error is a standard metric for assessing the quality of estimators (MSE). The goal is to estimate and/or minimize a version of the MSE in several fields (e.g., estimating, de-noising , modeling) [18]. MSE is simple to deal with mathematically, and it may provide insight into a related and significant class of generalized quantiles consistent scoring systems.

$$\frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}}(\mathrm{Xi}-\mathrm{Yi})^2 \qquad (2)$$

where (N) is a vector of predictions that produced from a sample of N data points, X is the vector of observed values and Y is the vector of predicted values [19]. MES computed between the original image and the final decrypted image from the proposed algorithm.

G. Peak signal to noise ratio (PSNR)

The geometric mean of individual image/frame mean square error (MSE) is used to calculate a single PSNR. The peak signal to noise ratio (PSNR) is a fidelity metric that is independent of image/video dynamic range. The arithmetic mean of the PSNR of each image/frame in the test set is frequently used to report technique performance.

$$-\frac{1}{N}\sum_{K=1}^{N} 10\ \log_{10}(mse_k) \qquad (3)$$

where N number of sample discoveries (test images) and MSE of the k'th sample realization is denoted by mse_k. The table below show MSE and PSNR metrics where each of these metrics compute between the original image and decoded image ,once in decode image after stack the shares in black mask algorithm and the second decoded image after apply the proposed encryption algorithm (scramble and 3D-Lorenz system) [20]. PSNR computed between the original image and the final decrypted image from the proposed algorithm. As illustrated in Table I below the result of MSE and PSNR are relatively good so the reconstructed image seems as possible like the original compared to other methods.

TABLE I. MSE AND PSNR ANALYSIS

Algorithm	MSE	PSNR
Proposed algorithm	0.09	58.39
Ref. [21]	0.11	57.63
Ref. [22]	0.06	60.17

H. Unified Average Changing Intensity (UACI)

(UACI) is the most used metric for assessing the security of image encryption techniques against differential attacks. UACI tests is extensively used in image encryption to assess cipher resilience to differential attacks. When the difference between plaintext images is subtle, UACI is developed to assess the number of changing pixels and the number of averaged altered intensity between ciphertext images (usually a single pixel). A high UACI score is usually interpreted as great differential attack resistance.

Received 24/August/2021; Accepted 4/December/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.2.1

$$\text{UACI: U (c1, c2)} = \sum_{ij} \frac{|C^1(i,j) - C^2(i,j)|}{F\ .\ T} \times 100\% \qquad (4)$$

where C1 and C2 are ciphertext images before and after one pixel change in a plaintext image, the pixel value at (i , j) are denoted as C1(i , j) and C2(i , j) ,symbol T signifies the total number of pixels in the ciphertext and symbol F denotes the ciphertext image format's largest supported pixel value [23]. UACI computed between the original image and the final decrypted image from the proposed algorithm. Our proposed algorithm reach a good result which is around 33.92 compared to other encryption algorithm. Table II below show the UACI analysis.

TABLE II. UACI ANALYSIS

Algorithm	**UACI**
Proposed algorithm	33.92
Ref. [3]	33.50
Ref. [16]	33.55
Ref. [7]	33.28
Ref. [24]	33.46
Ref. [25]	31.59

I. Information entropy

Entropy is a complexity metric. In the examination of biological signals, entropy can be employed [26]. In image processing applications, a measure of picture information is often utilized. This metric necessitates the estimation of a high-dimensional image probability density function, which is a realistic restriction [27].

The quantity of information in the growth of a scale can be measured using information entropy. Information entropy is characterized via the following:

$$\text{Hi (p)} = -\sum_{j=1}^{j} Pij \log_2(Pij) \qquad (5)$$

where Pij $\log_2(Pij)$ = 0 when Pij = 0, where the probability of each potential (ij) state is given by Pij [9]. Where information entropy computed for the final decrypted image from the proposed algorithm. Also here we can reach using our algorithm to a good result which is near to the optimal result in entropy metrics. Table III describe the Entropy analysis.

TABLE III. ENTROPY ANALYSIS

Algorithm	**Entropy**
Proposed algorithm	7.53
Ref. [21]	6.84
Ref. [3]	7.99
Ref. [16]	7.99
Ref. [7]	7.99
Ref. [24]	7.99

J. Quality encryption

The following factors can be used to assess picture encryption quality: Let F and F′ stand for the original and encrypted images, respectively. Each image has M*N pixels in size and has L grey levels. F(x, y), F′(x, y) are the images F and F″s grey levels at position (x, y) (0 ≤ x ≤ M −1, 0 ≤ y ≤ N −1). Let Hl (F) the number of times each grey level L appears in the original image F. Similarly, Hl (F’) in the encrypted image, the number of occurrences of each grey level L. The encryption quality is stated mathematically as the

Received 24/August/2021; Accepted 4/December/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.2.1

average number of modifications to each grey level L [28]. Quality encryption computed between the image decrypted from the black mask algorithm and final decrypted image from the proposed algorithm. The result of this metric illustrate that our algorithm has a good picture encryption quality with. Table IV illustrate the Quality encryption analysis.

$$\text{Encryption Quality} = \frac{\sum_{l=0}^{255} |H_L(F') - H_L(F)|}{256} \tag{6}$$

TABLE IV. QUALITY ENCRYPTION ANALYSIS

Algorithm	Quality encryption
Proposed algorithm	1168.943
Ref. [29]	283.648

K. Time Complexity

The system is worthless if it is inefficient. The suggested system must be computationally quick, with encrypting the channels and subsequently the entire image taking less than a second. The proposed approach examined on a testing image with a resolution of (1280*1145 pixels), and the time of execution is recorded when the 1280*1145 share is encrypted by the system after that, it encrypts all of the shares of 1280*1145* 4, where pixel expansion occurs during the black mask algorithm encrypt phase. On the core i7 system, the time complexity test is performed. *Fig. 12* below shows the calculated time complexity for six image with different size, the size tested for are (1280*1145, 500*405, 590*300, 532*521, 450*281, 1920*1080) the larger the image, the higher the time.

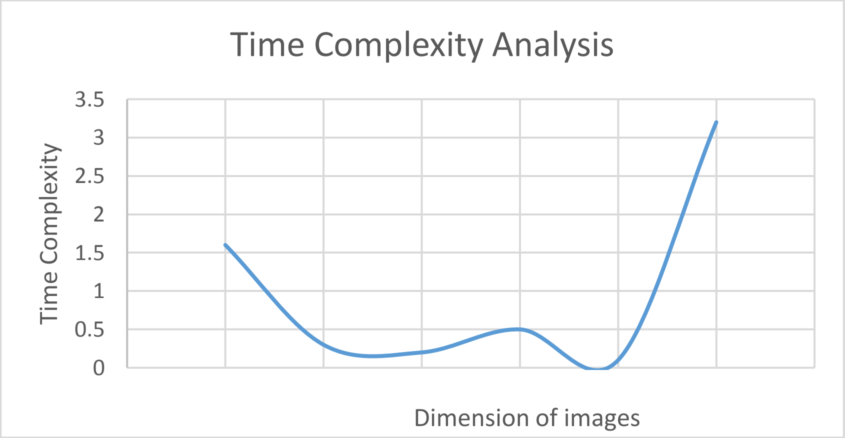


FIG. 12. TIME COMPLEXITY ANALYSIS.

L. Key Space Analysis

All chaotic systems have one thing in common: they are highly dependent on the starting values. In other words, if the initial values of the functions change slightly, the functions yield an altogether new outcome after a sufficiently enough time period. For the encryption algorithm designs to be reliable, the key space should be capable of neutralizing brute-force attacks. The encryption system key contains the starting values (x1, y1, and z1) as well as the initial parameter. In general, for chaotic systems, the precision of the beginning conditions should be as high as feasible, for example, 14 or 15 numbers just after commas. As a result of which the key space can exceed 1070. The key space is S = 1070 ≅ 2232 > 2100, which allows the cryptosystem to withstand brute-force attacks [30].

Received 24/August/2021; Accepted 4/December/2021
ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.2.1

M. Resistance to Known Plaintext and Chosen Plaintext Attacks

According to the suggested algorithm, the key is highly dependent on the chaotic system's initial values and initial parameters, with any little change yielding completely different results. As a result, different keys would be generated for various types of photos. Any attacker cannot decipher a specific image using a key from another image. To summarize, the provided system may be immune to both known—plaintext and chosen—plaintext threats.

N. Differential Attacks

Normally, in an image encryption mechanism, the encoded data is thought to vary from the unencrypted form. The UACI criteria were utilized to determine such a difference between the versions. In other terms, the crypto scheme described here should ensure that the encoded copies of two photos differ from each other when one bit is changed in one of them. The UACI test is shown in Table II. The outcome is acceptable, and the program has been found to be resistant to differential attacks.

O. Resisting Noise Attack Analysis

When data flows through an actual communication channel, the encoded picture version is necessarily subjected to various sorts of noise. This noise can cause issues while acquiring the original image. As a result, the algorithm must be noise resistant in order for the encryption scheme to be legitimate. As illustrated in Table I, the Peak Signal-to-Noise Ratio (PSNR) is used to measure the quality of the decoded image after the attacks. We can see that the original image is completely retrieved again, which is significant. Which indicates that the deciphered pictures are nearly identical to the originals. As a result, the suggested algorithm can be regarded to be somewhat robust to noise attacks.

VII. CONCLUSIONS

A chaos-based color image encryption algorithm is proposed in this paper. The generated sequences of keys from the Lorenz map are used to scramble the color input image sub pixels for the goal of creating confusion. Then, in the diffusion stage, scrambled images are used to replace pixels using a random shuffling mechanism. An detailed security analysis, including Mean Square Error, Unified Average Changing Intensity, and Quality encryption has been performed, demonstrating the recommended scheme's competent security. The predicted encryption strategy performs better according to the computational proficiency results. The proposed technique is resistant to traditional sorts of assaults. The proposed innovative technique provides a secure encryption/decryption file, according to statistical simulations.

REFERENCES

[1] A. Pandey and S. Som, "Applications and usage of visual cryptography: A review," *2016 5th Int. Conf. Reliab. Infocom Technol. Optim. ICRITO 2016 Trends Futur. Dir.*, pp. 375–381, 2016, doi: 10.1109/ICRITO.2016.7784984.

[2] A. Kadhim and R. M. Mohamed, "Visual cryptography for image depend on RSA & AlGamal algorithms," *Al-Sadiq Int. Conf. Multidiscip. IT Commun. Tech. Sci. Appl. AIC-MITCSA 2016*, pp. 195–200, 2016, doi: 10.1109/AIC-MITCSA.2016.7759935.

[3] S. C. Wang, C. H. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm," *Opt. Lasers Eng.*, vol. 128, no. December, p. 105995, 2020, doi: 10.1016/j.optlaseng.2019.105995.

[4] B. Mondal, "Cryptographic Image Scrambling Techniques," *Cryptogr. Inf. Secur.*, no. February, pp. 37–65, 2019, doi: 10.1201/9780429435461-2.

[5] X. Huang, T. Sun, Y. Li, and J. Liang, "A color image encryption algorithm based on a fractional-order hyperchaotic

Received 24/August/2021; Accepted 4/December/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.2.1

system," *Entropy*, vol. 17, no. 1, pp. 28–38, 2015, doi: 10.3390/e17010028.

[6] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, no. 16–17, pp. 3895–3903, 2011, doi: 10.1016/j.optcom.2011.04.001.

[7] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, no. February, 2020, doi: 10.1016/j.sigpro.2020.107484.

[8] B. Forgues, "The Palgrave Encyclopedia of Strategic Management," *Palgrave Encycl. Strateg. Manag.*, no. January, 2016, doi: 10.1057/978-1-349-94848-2.

[9] X. Wang, Y. Li, and J. Jin, "A new one-dimensional chaotic system with applications in image encryption," *Chaos, Solitons and Fractals*, vol. 139, p. 110102, 2020, doi: 10.1016/j.chaos.2020.110102.

[10] A. Mansouri and X. Wang, "A novel one-dimensional chaotic map generator and its application in a new index representation-based image encryption scheme," *Inf. Sci. (Ny).*, vol. 563, pp. 91–110, Jul. 2021, doi: 10.1016/j.ins.2021.02.022.

[11] P. Gholamin and A. H. R. Sheikhani, "A new three-dimensional chaotic system: Dynamical properties and simulation," *Chinese J. Phys.*, vol. 55, no. 4, pp. 1300–1309, 2017, doi: 10.1016/j.cjph.2017.07.002.

[12] Y. C. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 36, no. 7, pp. 1619–1629, 2003, doi: 10.1016/S0031-3203(02)00258-3.

[13] A. Jaafar and A. Samsudin, "A survey of black-and-white visual cryptography models," *Int. J. Digit. Content Technol. its Appl.*, vol. 6, no. 15, pp. 237–249, 2012, doi: 10.4156/jdcta.vol6.issue15.28.

[14] P. M. Modak and V. Pawar, "A comprehensive survey on image binarization techniques," *Stud. Comput. Intell.*, vol. 560, no. 12, pp. 5–15, 2014, doi: 10.1007/978-81-322-1907-1_2.

[15] S. Heidari, M. Vafaei, M. Houshmand, and N. Tabatabaey-Mashadi, "A dual quantum image scrambling method," *Quantum Inf. Process.*, vol. 18, no. 1, pp. 1–23, 2019, doi: 10.1007/s11128-018-2122-4.

[16] D. S. Malik and T. Shah, "Color multiple image encryption scheme based on 3D-chaotic maps," *Math. Comput. Simul.*, vol. 178, pp. 646–666, 2020, doi: 10.1016/j.matcom.2020.07.007.

[17] N. Sharma, I. Saini, A. Yadav, and P. Singh, "Phase-Image Encryption Based on 3D-Lorenz Chaotic System and Double Random Phase Encoding," *3D Res.*, vol. 8, no. 4, 2017, doi: 10.1007/s13319-017-0149-4.

[18] S. Beheshti, M. Hashemi, E. Sejdić, and T. Chau, "Mean square error estimation in thresholding," *IEEE Signal Process. Lett.*, vol. 18, no. 2, pp. 103–106, 2011, doi: 10.1109/LSP.2010.2097590.

[19] E. Y. Ovcharov and S. Wahl, "Bias-Corrected Decomposition of Mean Squared Error," no. December 2015, pp. 0–7, 2015.

[20] O. Keleş, M. A. Yılmaz, A. M. Tekalp, C. Korkmaz, and Z. Dogan, "On the Computation of PSNR for a Set of Images or Video," 2021, [Online]. Available: http://arxiv.org/abs/2104.14868.

[21] D. Pandey, U. S. Rawat, and A. Kumar, "Robust progressive block based visual cryptography with chaotic map," *J. Discret. Math. Sci. Cryptogr.*, vol. 19, no. 5–6, pp. 1025–1040, 2016, doi: 10.1080/09720529.2015.1132040.

[22] M. T. Elkandoz, W. Alexan, and H. H. Hussein, "3D Image Steganography Using Sine Logistic Map and 2D Hyperchaotic Map," *2019 Int. Conf. Electr. Comput. Technol. Appl. ICECTA 2019*, pp. 3–8, 2019, doi: 10.1109/ICECTA48151.2019.8959700.

[23] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," *Cyberjournals.Com*, no. April 2011, 2011, [Online]. Available: http://www.cyberjournals.com/Papers/Apr2011/05.pdf.

[24] C. Wang, X. Zhang, and Z. Zheng, "An efficient image encryption algorithm based on a novel chaotic map," *Multimed. Tools Appl.*, vol. 76, no. 22, pp. 24251–24280, 2017, doi: 10.1007/s11042-016-4102-y.

[25] V. Sankaradass, P. Murali, and M. Tholkapiyan, *Region of interest (ROI) based image encryption with sine map and lorenz system*, vol. 30. Springer International Publishing, 2019.

[26] A. K. Farhan, N. M. G. Al-Saidi, A. T. Maolood, F. Nazarimehr, and I. Hussain, "Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder," *Entropy*, vol. 21, no. 10, pp. 1–14, 2019, doi: 10.3390/e21100958.

[27] Q. R. Razlighi and N. Kehtarnavaz, "A comparison study of image spatial entropy," *Vis. Commun. Image Process. 2009*, vol. 7257, no. January 2009, p. 72571X, 2009, doi: 10.1117/12.814439.

[28] G. N. Krishnamurthy, "Encryption Quality Analysis and Security Evaluation of CAST-128 Algorithm and its Modified Version using Digital Images," *Netw. Secur.*, vol. 1, no. 1, pp. 28–33, 2009.

[29] H. E. H. Ahmed, "Image Encryption Using Development of Chaotic Logistic Map Based on Feedback Stream Cipher," *Recent Adv. Telecomunication, Informatics Educ. Technol.*, pp. 274–283, 2014.

[30] B. Arpacı, E. Kurt, K. Çelik, and B. Ciylan, "Colored Image Encryption and Decryption with a New Algorithm and a Hyperchaotic Electrical Circuit," *J. Electr. Eng. Technol.*, vol. 15, no. 3, pp. 1413–1429, 2020, doi: 10.1007/s42835-020-00393-x.

Received 24/August/2021; Accepted 4/December/2021