INTERNATIONAL JOURNAL OF Telecommunications
AIR DEFENSE COLLEGE

Survey Image Cryptanalysis Using a Substitution Box Based Chaotic Map

Ahmed Rabea [1], Mohamed G. Abdelfattah [2], Ali E. Takieldeen [3], Abeer T. Khalil[4]

Citation: Rabea , A.; Mohamed , G.; Takieldeen , T.; Abeer , T. *Inter. Jour. of Telecommunications,* ***IJT'2023***, *Vol. 03, Issue 02, pp. 1-12, 2023.*

Editor-in-Chief: Youssef Fayed.

Received: 10/07/2023.

Accepted: date 02/09/2023.
Published: date 02/09/2023.

Publisher's Note: The International Journal of Telecommunications, IJT, stays neutral regarding jurisdictional claims in published maps and institutional affiliations.

[1] Air Defense College Military Academy Egypt; rabeaahmed701@std.mans.edu.eg.
[2] Department of Electronics and Communications Engineering, Faculty of Engineering, Mansoura University, Egypt; eng.mo.gamal@mans.edu.eg.
[3] IEEE Senior Member, Faculty of Artificial Intelligence, Delta University for Science and Technology Air Defense College Military Academy, Egypt; a_takieldeen@yahoo.com.
[4] Associate Professor at Electronics and communications department Faculty of Engineering, Mansoura University, Egypt; abeer.twakol@mans.edu.eg.

Abstract: Providing a new framework for chaotic image encryption is becoming increasingly important and more significant in various applications, such as the transmission of medical and military photographs. Substitution boxes based on chaos have received a lot of attention lately. Recently, a method of picture encryption based on numerous chaotic Substitution boxes was proposed. Many chaos map-based encryption methods have been proposed, taking advantage of their superior properties such as sensibility to the initial state and controlling factors. This encryption technique was founded on the idea of the confusion that the S-implementation boxes alone may generate. The technique involves incorporating replacement box encryption, working with a chaotic map to extract the output data, encrypting that data using a well-known encryption algorithm, and then having the other party decrypt it. And then to ensure the accuracy of the recovered data, certain statistical analysis is performed on it, including correlation, charts, and entropy.

Keywords: Encryption; S- boxes; Cryptography; Chaotic Maps.

1. Introduction

A crucial challenge for security and confidentiality is color picture encryption. Many chaotic map-based encryption techniques [1,2] have been presented with other great qualities including severity and sensitivity to the starting situation and the control variables. The fragility of popular chaotic cryptography techniques based on the permutation-based approach has been confirmed by a few cryptanalysis publications [3,4]. structure for diffusion. As a result, the introduction of chaotic picture cryptography algorithms [5] in combination with other unique techniques, such as genetic material, The sensitivity mechanism is constructed [6] using the ordinary mage's information entropy. As a result, cipher analysis research has been put out [7] to evaluate the security of picture data. It could make the current cryptosystems more secure. Li et al., for instance, attacked the information entropy-based chaotic picture encryption technique [8]. Latin Square's cryptography property has recently led to the construction of other more chaotic picture encryption methods[9].To strengthen the security and privacy required by using variable keys, the proposed method integrates various chaotic maps (such as logistic, tent, quadratic, cubic, and Bernoulli) to produce more reliable chaotic maps. The chaotic maps used in our system are created using the latter, which is created by computing the sine square logistic map. To get the ideal period for each chaotic map during which it performed the best encryption, we carried out numerous experiments. Here, various chaotic maps are combined to create a new map that performs well when X [0, 1].
It was important to figure out how to select the top chaotic maps to use in the encryption procedure.

However, Hu and co. identified a mathematical flaw in [10]. The chaotic picture cipher is broken using the chosen-plaintext attack combined with the chosen-ciphertext assault. Ge et al. also found a weakness in the A compound chaotic stream cryptography based on perturbation is used as a reverse picture encryption method.. in [11], who then attacked the algorithm. However, the majority of chaotic maps used to generate the encryption security key are multi-dimensional, which increases the computational complexity. There have recently been some 1D chaotic map encryption techniques developed in [12,13] that are simpler to implement in software or hardware. In [14], a novel 1D chaotic map model is suggested. Following is an outline for this essay: Part 2 Review of the Original Plan. Part 3 Cryptanalysis of Image. Part 4 Proposed Algorithm. Part 5 Metrics of performance. part 6 Summary OF Experimental tests. The conclusion is in the final section.

2. Literature review

For the past 20 years, chaos-based encryption techniques have been employed. The peculiar behavior of chaotic systems is what has sparked interest in the chaos theory in the construction of cryptographic systems. Chaos is an unpredictable, deterministic process that occurs in nonlinear dynamic systems. Despite being finite, chaotic systems are not periodic and do not converge to a particular value. The fact that chaotic systems rely heavily on their beginning conditions and control settings is their most crucial trait. Chaos appears to have a random and unpredictable nature. These chaotic system characteristics are linked to confusion and diffusion, two fundamental requirements for cryptographic systems. What kind of chaotic system should be chosen during the encryption process is one of the most crucial factors to consider when creating encryption systems based on chaotic systems. However, during this selection, it is important to consider and maintain the balance between encryption system characteristics like security (the encryption system should be as sophisticated as possible) and efficacy (the simplicity of the encryption system's practical applicability). The complexity of the chaos-based encryption scheme is improved by continuous-time chaotic systems. However, due to issues with the implementation of continuous-time chaotic systems (such as computational difficulty and digital deterioration), a significant portion of chaos-based encryption systems are based on discrete-time chaotic systems (chaotic maps). Therefore, it is important to research the relevance of the higher and more complicated chaotic system[15-16].

According to the trichromatic theory, the color image of size M×N must be divided into three photos in grayscale before cryptography. Link the two grayscale images together to create a new grayscale image of size M×3N. By reshaping the final grey image, the sequence S = {s1, s2, . . . sM×3N} is created, and its length is M×3N [17].

Fig 1 displays the schematic for the 1D chaotic image encryption technique. The chaotic sequence X is acquired during the permutation phase by repeatedly applying the new chaotic system M3(N+N0) and removing the previous N0 elements. The following equation describes the new chaotic map in [18]:

$$x_{n+1} = F_{\text{chaos}}(u, x_n) \times 2^{k} - floor\ F_{\text{chaos}}(u, x_n) \times 2^{k} \quad (1)$$

where a chaotic one-dimensional map, like the logistic, sine, and Chebyshev maps, is Fchaos (u, xn). the chaotic sequence produced is xn. u ∈ (0, 10] and k ∈ [8, 20] are the initial values. The particulars of u, k, and N0 are utilized as the security key. The ascending order sorting of vector S yields the permutation position vector Xj = {xj1, xj2, ... xjM×3N}. The permuted picture pixel vector P is obtained using the equation P(i) = S(Xj(i)).

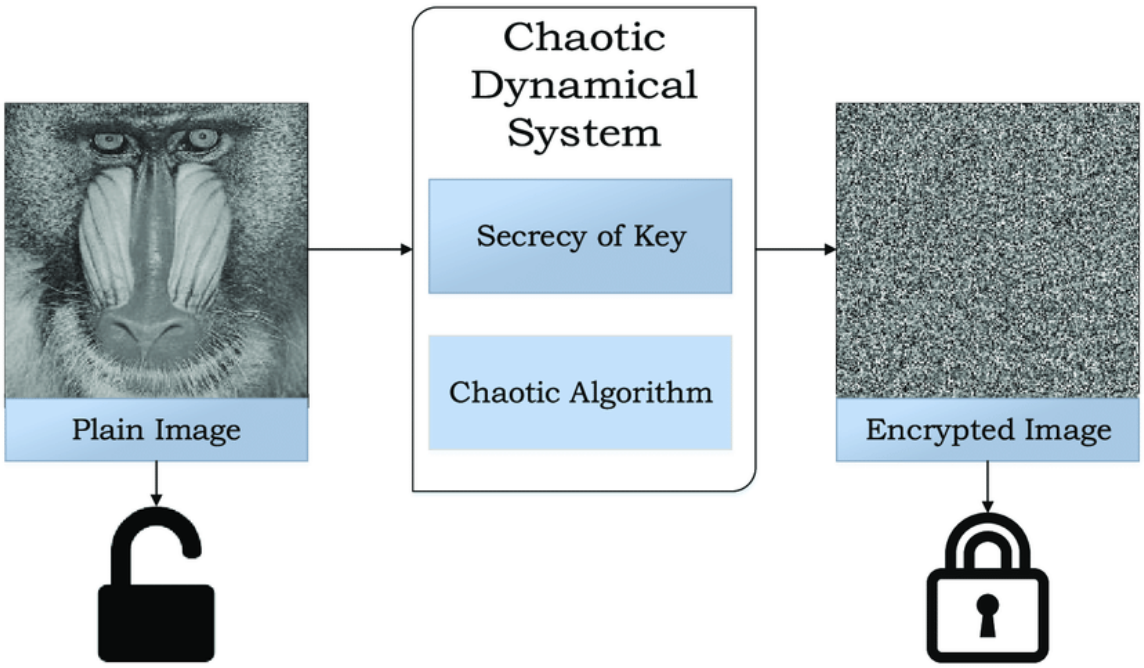

Figure 1. The schematic for 1D chaotic image encryption

2.1. With s-box

An essential component of a symmetric algorithm used for substitution is the s- box. Block ciphers frequently employ them to hide the connection between the key and the ciphertext. A table-driven non-linear substitution procedure is called an S-box. They can be produced either randomly or algorithmically, and they differ in both input and output sizes. S-boxes were initially utilized in Lucifer, followed by DES, and then in most encryption algorithms.

An S-box is a crucial component of algorithms with symmetric keys that do substitution (S-box) in cryptography. Block ciphers frequently employ them to hide the connection between the key and the ciphertext, or Shannon's property of confusion. The S-Boxes are frequently carefully selected to be resistant to cryptanalysis.

2.2. With chaotic map

A map (specifically, how progress works) that displays several types of chaotic conduct is referred to as a chaotic map in mathematics. A discrete-time or continuous-time parameter can be used to parameterize maps. Discrete maps are typically represented by iterated functions. Chaotic mapping is helpful in analyzing dynamic structures that frequently appear.

2.3. Chaotic map type

1. Logistic map

It is a simple discrete nonlinear chaotic system, which exhibits chaotic behavior (DCS) [19]. It is 1DCS, and it fits the following description:

$$X_{n+1} = \mu X_n (1 - X_n) \quad (2)$$

Where n is the number of iterations [0, 4], X [0, 1] in which the chaotic conduct is recognized when [3.57, 4] and is the chaotic factor X= 0.5555, μ= 3.9999999.

2. Tent map

One of the important maps in our study .it [1-2.24] is a repeating function that takes the form of a tent in mathematics and forms a discrete-time dynamical system. A genuine line's Xn is extracted and mapped to a different point [20].

$$X_{n+1} = \begin{cases} \mu' X_n & X_n < 0.5 \\ \mu'(1 - X_n)0 & .5 \leq X_n \end{cases} \quad (3)$$

n is the number of repetitions, *X* is [0, 1] and the new real chaotic factor is [3, 4].

3. Bernoulli map

Another well-liked map that is widely employed in encryption is the Bernoulli map, sometimes known as the 2 mod 1 map. 8,9 A discrete-time random process called a Bernoulli process is made up of a limitless or limited series of autonomous random factors, such as X1, X2, and X3…. such that the value of Xi for each value of I is either 1 or 0; the probability that Xi = 1 is the same for all values of i. The Bernoulli method includes a future trial from any point in time that is separate from the prior trials. Bernoulli's map [8,9,17] is typically described as

$$X_{n+1} = \begin{cases} 2X_n 0 & \leq X_n < 0.5 \\ 2X_n - 0 & 1.5 \leq X_n < 1 \end{cases} \quad (4)$$

4. Cubic map

One of the system's simple nonlinear process and chaotic maps that exemplifies the chaotic method is the cubic map. 1–5,17 It's outlined by

$$X_{n+1} = f(X_n) = \mu' {X_n}^3 + (1 - \mu')X_n \quad (5)$$

where μ' is the number of iterations and is the new chaotic factor. When $x \in [0,1]$ and $\mu' \in [3, 4]$.

5. Quadratic map

The quadratic map is a type that exhibits chaotic behavior since it is a 2nd equation. In Refs, the explanation of the standard formula for the quadratic map was presented

$$X_{n+1} = f_c(X_n) = {X_n}^2 + c \quad (6)$$

where n represents the number of repetitions. Were $x \in [0,1]$.

3. Cryptanalysis and Encryption Algorithm of Image

3.1.Cryptanalysis

1. Chosen-plaintext attack

The attacker chooses one or more plaintexts to be encrypted in this attack type and then gets the related ciphertexts. The primary goal of the assault is to gather more information that will weaken the encryption system's security. One of the probable classic assaults is this one.

2. Chosen-ciphertext attack

In this attack technique, the cryptanalyst picks the ciphertext deciphered and obtains the plaintext that goes with it.

3. Ciphertext-only attack

In this instance, the attacker has less information because they only have access to a collection of ciphertexts that were created from several plaintexts. The key is attempted to be inferred by the cryptanalyst by analyzing them, and if the key is determined using this inadequate amount of information, the cryptographic procedure is rather insecure.

4. Known-plaintext attack

The cryptanalyst in this instance has access to both the plaintext and the ciphertext of those plaintexts. The attacker is free to use the pairings of plaintext and ciphertext to determine the key.

3.2. Encryption Algorithm

3.2.1 Elliptic Curve Cryptography

Data encryption uses elliptic curve cryptography (ECC), which is dependent on keys. ECC concentrates on pairs of public and private keys for online traffic encryption and decryption.

With RSA and ECC encryption keys, there is a significant size to security yield discrepancy. The table below lists the key sizes required to offer the same level of security. In other words, a 384-bit elliptic curve cryptography key delivers the same level of security as an RSA key with 7680 bits.

1. Advantages of Elliptic Curve

Algorithms that are simple to process in one direction and challenging to process in the opposite are used in public-key cryptography. For instance, RSA depends on the ease with which prime numbers can be multiplied to get larger numbers, However, RSA requires keys with 2048 bits or more in order to stay secure. This slows down the process and emphasizes the significance of crucial size.

The same degree of security as ECC may be used with smaller keys. In a world where mobile devices must perform increasing amounts of encryption while using less computational resources, ECC offers stronger security with quicker, shorter keys than RSA.

2. The Equation of an Elliptic Curve

It is defined by the equation

$$E: y2 = f(x) \quad (7)$$

When a polynomial is cubic or quartic, f is referred to as an elliptic curve (x). Moreover, we demand that its polynomial f(x) has no double roots. This ensures that the curve is nonsingular. When one of the equation's variables is changed, the equation takes on a more straightforward form.

$$E: y2 = x3 + A\,x + B \quad (8)$$

Lastly, we add an extra point O "at infinity," so that E is the set, for reasons that will be described in a moment.

$$E = \{(x, y): y2 = x3 + A\,x + B\} \cup \{O\} \quad (9)$$

4.Proposed Algorithm

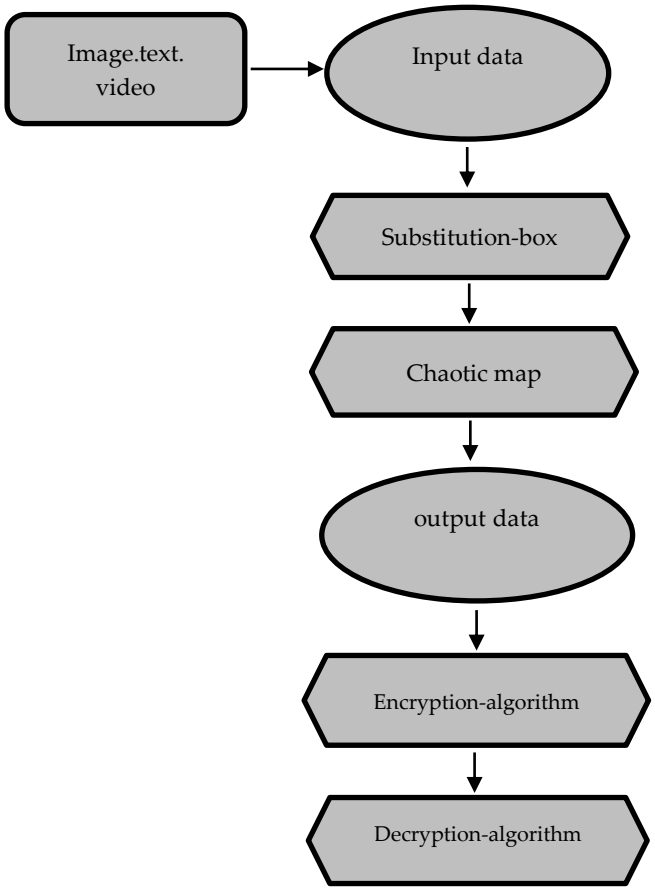

Figure 2. Flow Chart for Proposed Algorithm

We present the proposed algorithm in Figure 2 based on data entries such as (Image. text. video), then the substitution box is used to hide the relationship between the key and the ciphertext, and to secure the plain text against data analysis attacks and key spacing attacks. S-box, which is a portion of the block cipher's nonlinear component, is important for secure communication. Shannon initially presented the Substitution box's design in 1949[20]. S-box carries out a few crucial functions. Inherent Nonlinearity, Differential Uniformity, Strict Avalanche Criterion (SAC), Linear Approximation, and Algebraic Complexity Bit independence criterion for fixed (Fp) and opposite fixed points (OFp) [21]. Then using a Chaotic map to confusion and diffusion, two fundamental requirements for cryptographic systems. to obtain the output data, use appropriate chaotic maps for blocking ciphers that maintain key characteristics throughout discretization, or for stream ciphers, use a balanced combining function and an appropriate key stream generator [22]. the desired data is entered in a cryptographic format. Cryptography is regulated via a chaotic system, which results in a random pattern, to retrieve the information in a random and disorganized way so that it is challenging to recognize it by Shannon's theory of security. Chaos flows are produced using a variety of chaos maps (CMs). to increase safety and effectiveness. One of the encryption techniques is used to get the data once it has been obtained, keeping it encrypted until it is sent to the location to which it is to be delivered in total secrecy. The data is then decrypted on the receiving side using one of the encryption techniques until it is read, and its content is known.

5. Metrics of Performance

To assess the effectiveness of our strategy, used sensitivity examination of plaintext as the average net pixel change rate and changing intensity. also used various assaults such as Analysis of the correlation coefficient, the mean percentage error, and the peak signal to noise ratio to make our system appear flawless:

1. Sensitivity testing in plaintext

A useful relationship between the cipher image and the plain image is produced by comparing cipher images with the plain image after changing, which defines the secret key, using the other part. The cryptography tool uses the selected plaintext attack and known-plaintext attack to attempt and change one bit, or normally one pixel, in the plain image. Two of the most used metrics, net pixel changes rate (NPCR) and unified average changing intensity (UACI) are used to examine the effects of a single-pixel change on the entire cipher picture [16]

$$NPCR = \frac{\sum_{i,j} Diff(i,j)}{W \times H} \times 100\% \quad (10)$$

where the pictures' relative height and width are defined by H and W. The UACI, on the other hand, entails altering the necessary pixels' strength in both the plain picture & the cipher image. Its UACI resistance to a differential attack on the encryption system increases with size. The UACI is defined by

$$UCAI = \frac{1}{W \times H} \sum_{i,j} \left[\frac{CI1(i,j) - CI2(i,j)}{255} \right] \times 100\% \quad (11)$$

The UACI is 33.4653, and the value of NPCR for two random images is 99.69, which is a reasonable estimate for a reliable encryption method. The UCAI and NPCR values for the suggested technique, respectively, range from 32.82 to 40.23 and 98.698 to 100. Due to its exceptional sensitivity on the plaintext, the suggested image encryption approach is immune to a differentiating assault.

2. Mean absolute error (MAE)

The pictures' grey levels (GLs) are specified and represented by the function C (i, j) [16–18]. Additionally, the GLs that each pixel at a certain place gets are shown as P (i, j). The cypher has the following measurements: W×H. Two photos are used to calculate the total of subtraction, and the resulting MAE is defined as follows:

$$\mathrm{MAE} = \frac{1}{\mathrm{WxH}} \sum_{i=1}^{w} \sum_{i=1}^{H} |C(i,j) - P(i,j)| \quad (12)$$

3. Peak signal to noise ratio (PSNR)

The peak signal to noise ratio (PSNR) [9,15] of the original picture and the encrypted image is calculated as follows:

$$PSNR = 10\log_{10}\frac{h_{w\left[\max_{1<i\le m,1<j\le n}\{pi,j\}\right]^2}}{\sum_{j=1}^{W}\sum_{i=1}^{H}(Pi\cdot j-P\prime,j)^2} \quad (13)$$

4. Correlation coefficient analysis

Probability analysis and histogram equalization both reveal the overall unpredictability of an image. 22 To find the attributes shown by the local location of the nearby pixels, to design both before and after encrypted. Calculated is the relationship between two pixels in various orientations as

$$r_{xy} = \frac{COV(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} \quad (14)$$

where:

$$COV(X,Y) = \frac{1}{N}\sum_{j=1}^{N}(Xj\ -\ -E(X))(Yj\ -\ -E(Y)) \quad (15)$$

cov (x, y) denotes the covariance between the Random elements X and Y, as well as E(y) and E(x) denote the anticipated values of X and Y, correspondingly, and N is the number of selected nearby pixels calculated as W H, where H and W are the dimensions of the encrypting image to experience the entire image. A decreased correlation between adjacent pixels should be attained for good encryption and impedance qualities. The correlation coefficient is defined as

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(X_j\ -\ -E(X)^2 \quad (16)$$

$$D(y) = \frac{1}{N}\sum_{j=1}^{N}(Y_j\ -\ -E(y)^2 \quad (17)$$

$$E(X) = \frac{1}{N}\sum_{j=1}^{N}X_j \quad (18)$$

$$D(Y) = \frac{1}{N}\sum_{j=1}^{N}Y_j \quad (19)$$

The deviations from the mean are expressed as ((D(x)) and (D(y)) for random variables X and Y, where x and y are the intensity values of the adjacent pixels, and N is the number of neighbors that were randomly selected; in the trials, all nearby pixels are chosen to calculate the correlation. The deviations from the mean are expressed as ((D(x)) and (D(y)) for random variables X and Y, where x and y are the intensity values of the adjacent pixels, and N is the number of neighbors that were randomly selected; in the trials, all nearby pixels are chosen to calculate the correlation.

6.Summary OF Experimental Test

The MATLAB / Simulink framework uses the specified encryption algorithm. Lena, Cameraman, Baboon, Bridge, and the Airplane are among the 256 x 256 grayscale photos that are taken into consideration to validate and evaluate the robustness of the suggested approach. utilized the suggested workflow to encrypt these photos. The robustness against the impact of picture noise has also been validated. The suggested method has been compared to the other algorithms, and that is all there is to it. The histogram of the fruit picture is shown in Figure 3. After cryptography, the structure of pixel or intensity values is dissected to determine the degree of homogeneity in all sections of the altered image. The primary image of the example Lena's picture in various sizes, together with its histogram, is shown in 3(a). The encrypted form of this image and its graph are displayed in 3(b), and as can be seen, the texture of the image is widely dispersed. Fig 3(c). displays Lena's decryption picture and histogram for the noise transmitted/received channel using a 2% salt and pepper noise effect was used. Even though noise is added prior to transmission via the sending and receiving channels and after cryptography, Figure 3 also depicts the decryption of the original picture. Fig. 4 displays a further example of how to use the bird image to demonstrate a point. We demonstrate the impact of our technique on

various fruit sizes in Table I utilizing the results of a plaintext sensitivity analysis and a differential attack. The findings and the size of the image seem to be related in some way. It is obvious that the better the correlation coefficient value, UACI, PSNR, and entropy findings are, the greater the picture size. Figure 4 displays the bird's picture in various sizes together with its graph following the application of the suggested technique. The picture and its graph are displayed in Figure 4(a).

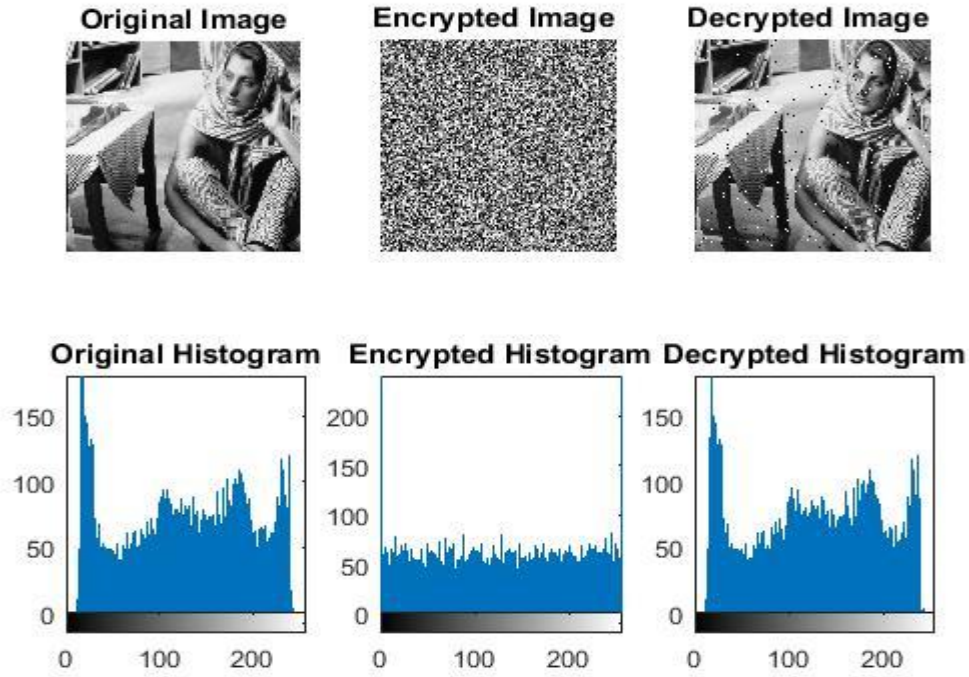

Figure 3. The original picture of the Lena graph and its salt-and-pepper noises.

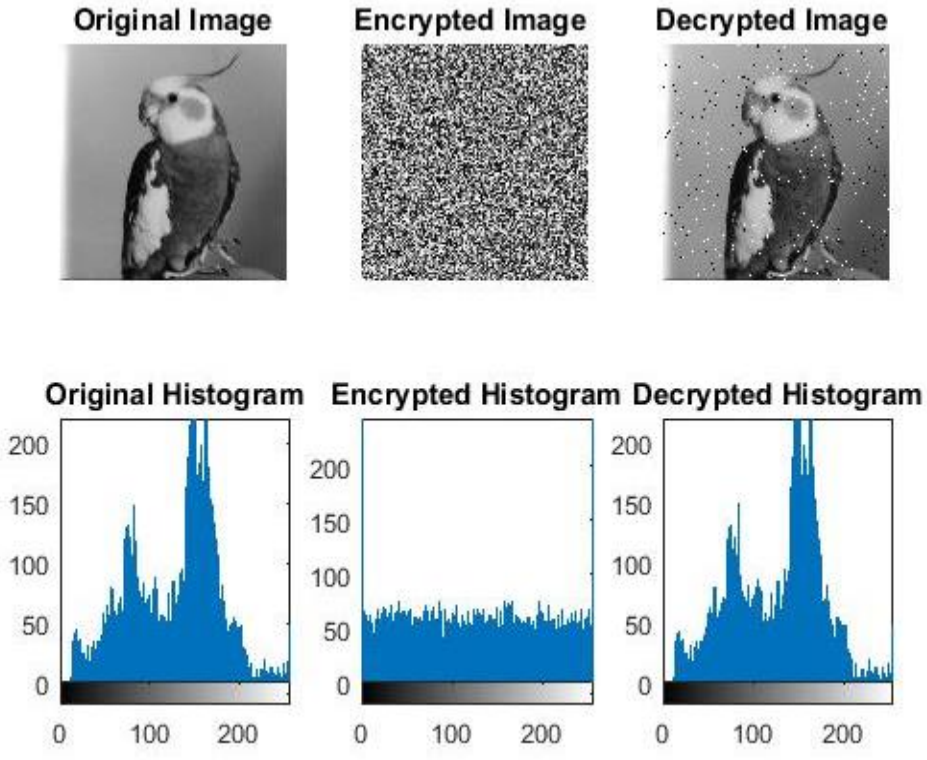

Figure 4. The bird's picture and its graph with salt-and-pepper noises.

In Table 1 confirms the correlation between the encoded picture's size and the outcomes of the differential attack and plaintext sensitivity analysis. After using the suggested approach, we provide a huge size of 1024× 1024 for the original airplane picture in Fig.5 and its graph. Figure 5(displays the histogram for the original picture, Fig 5(b) displays the graph for the encrypted image, and Figure 5(c) displays the histogram for the decrypted image after applying Together, pepper and salt make up 2%.

TABLE 1. Outcomes of the sample fruit image with various sizes.

Analysis	CORR	UACI	PSNR	MAE	PNCR	Time	Entropy
128 × 128	0.000 07	33.23	8.87	8072	99.64	11.1	7.72
256 × 256	0.000 05	33.45	8.63	8544	99.85	6.23	7.72
512 × 512	0.000 03	33.84	8.43	8792	99.94	5.39	7.71

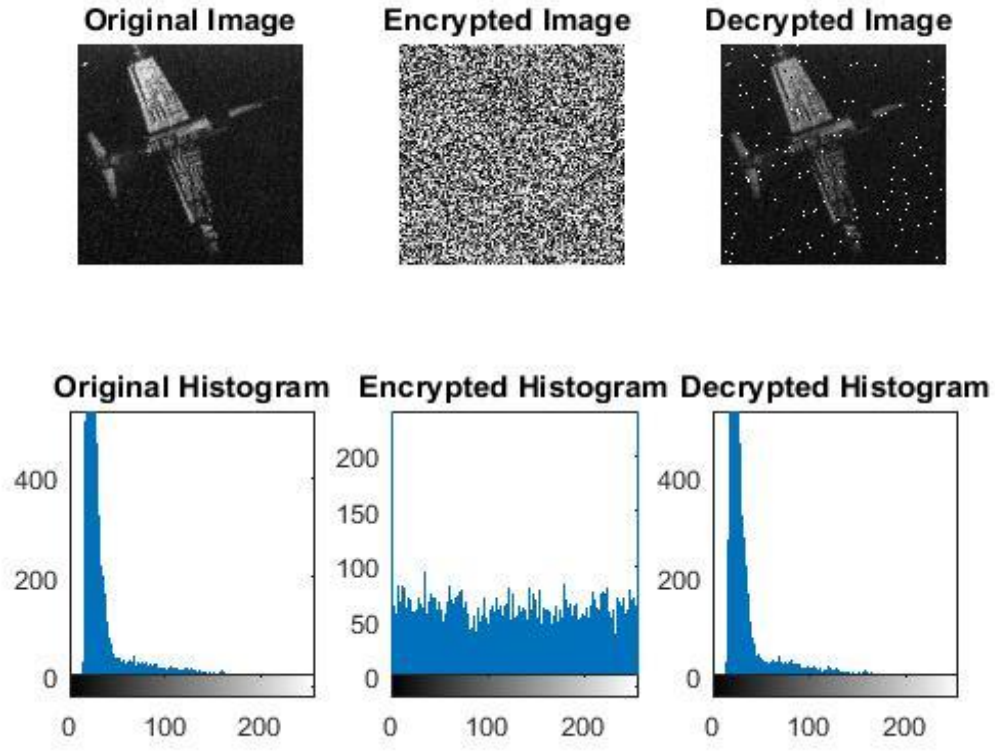

Figure 5. the airplane's picture and its graph with salt-and-pepper noise

When we employed a bigger picture with a resolution of 1024×1024, the analysis's findings for both the differential attack and text sensitivity showed a significant rise. Table II presents the findings. We found that the values of UACI, MAE, and PSNR were significantly improved, based on the CORR metric, and the outcomes of our technique and other encryption schemes are compared. One of the signs of greater safety and preference for the suggested algorithm is the demonstrably large increase in the CORR value. Additionally, Table 2 compares the image results utilizing the findings of NPCR, UACI, CORR, MAE, And PSNR using the

pictures of Lena, Baboon and the airplane Take note of the results of UACI, and NPCR. MAE, PSNR, and "CORR" in a definite and apparent way. This demonstrates the benefit of our encryption.

TABLE 2. results of the UACI, NPCR. MAE, PSNR, and "CORR" for images

Analysis	UACI	NPCR	MAE	CORR	PSNR
Lena	33.06	99.46	9395	0.000 01	8.31
Baboon	33.2	99.46	7131	0.000 17	9.31
airplane	40.19	98.87	15900	0.000 041	6.2

7. Conclusions

Recent research has shown that chosen and well-known plaintext assaults can be used to crack chaos-based encryption systems. New chaotic systems and practical design algorithms should therefore be researched. We presented a proposed technique for picture encryption and decryption by various chaotic maps and substitution boxes, that strengthened the security required to protect privacy by utilizing a substitution box, chaotic maps, and an encryption algorithm. Which increased the security needed to protect privacy. It is done to compare the outcomes with cutting-edge algorithms. Based on assessment criteria including PSNR, CORR, MAE, UACI, and NPCR, the suggested methodology has been shown to perform better than the compared approaches. The approach combines chaotic maps and substitution boxes to provide an extremely safe cryptography picture level with a minimal amount of computation cost, and Which makes the system completely secure for data transmission and communication making it ideal for actual-time video communication implementation that desired a high plane of security. Future studies will focus on enhancing such outcomes by utilizing new techniques for picture encryption and security.

REFERENCES

1. Zhang, Yushu, et al. "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.
2. Zhang, Yushu, and Di Xiao. "Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform." Optics and Lasers in Engineering 51.4 (2013): 472-480.
3. Ye, Guodong, and Kwok-Wo Wong. "An efficient chaotic image encryption algorithm based on a generalized Arnold map." Nonlinear dynamics 69 (2012): 2079-2087.
4. Mirzaei, Omid, Mahdi Yaghoobi, and Hassan Irani. "A new image encryption method: parallel sub-image encryption with hyper chaos." Nonlinear Dynamics 67.1 (2012): 557-566.
5. Liu, Yanbing, et al. "Design and statistical analysis of a new chaotic block cipher for wireless sensor networks." Communications in Nonlinear Science and Numerical Simulation 17.8 (2012): 3267-3278.
6. Zhang, Yushu, and Di Xiao. "Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform." Optics and Lasers in Engineering 51.4 (2013): 472-480.
7. Wong, Kwok-Wo, Bernie Sin-Hung Kwok, and Wing-Shing Law. "A fast image encryption scheme based on chaotic standard map." Physics Letters A 372.15 (2008): 2645-2652.
8. Norouzi, Benyamin, et al. "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process." Multimedia tools and applications 71 (2014): 1469-1497.

9. Arroyo, David, Jesus Diaz, and F. B. Rodriguez. "Cryptanalysis of a one round chaos-based substitution permutation network." Signal Processing 93.5 (2013): 1358-1364.
10. Zhang, Yushu, and Di Xiao. "Cryptanalysis of S-box-only chaotic image ciphers against chosen plaintext attack." Nonlinear Dynamics 72 (2013): 751-756.
11. Arroyo, David, Jesus Diaz, and F. B. Rodriguez. "Cryptanalysis of a one round chaos-based substitution permutation network." Signal Processing 93.5 (2013): 1358-1364.
12. Ahmed, Makram, et al. "A novel image encryption/decryption scheme based on integrating multiple chaotic maps." AIP Advances 10.7 (2020): 075220.
13. Zhang, Yu, et al. "Breaking a chaotic image encryption algorithm based on perceptron model." Nonlinear Dynamics 69 (2012): 1091-1096.
14. Zhang, Yushu, et al. "Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process." Nonlinear Dynamics 76 (2014): 1645-1650.
15. Özkaynak, Fatih, and Sırma Yavuz. "Designing chaotic S-boxes based on time-delay chaotic system." Nonlinear Dynamics 74 (2013): 551-557.
16. Ye, Guodong, et al. "A chaotic image encryption algorithm based on information entropy." International Journal of Bifurcation and Chaos 28.01 (2018): 1850010.
17. Dou, Yuqiang, et al. "Cryptanalysis of a DNA and chaos-based image encryption algorithm." Optik 145 (2017): 456-464.
18. Ye, Guodong, et al. "A chaotic image encryption algorithm based on information entropy." International Journal of Bifurcation and Chaos 28.01 (2018): 1850010.
19. Alanazi, Ammar S., et al. "Cryptanalysis of novel image encryption scheme based on multiple chaotic substitution boxes." IEEE Access 9 (2021): 93795-93802.
20. Mohamed, Kamsiah, et al. "Study of S-box properties in block cipher." 2014 International Conference on Computer, Communications, and Control Technology (I4CT). IEEE, 2014.
21. Pisarchik, Alexander N., and Massimiliano Zanin. "Chaotic map cryptography and security." Encryption: Methods, Software and Security (2010): 1-28.
22. Behnia, Sohrab, et al. "A novel algorithm for image encryption based on mixture of chaotic maps." Chaos, Solitons & Fractals 35.2 (2008): 408-419.
23. Li, Ming, et al. "Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata." IEEE access 6 (2018): 47102-47111.
24. [2Khan, Majid. "A novel image encryption scheme based on multiple chaotic S-boxes." Nonlinear Dynamics 82.1-2 (2015): 527-533.
25. Farwa, Shabieh, et al. "An image encryption technique based on chaotic S-box and Arnold transform." International Journal of Advanced Computer Science and Applications 8.6 (2017).
26. Kanafchian, Mohadeseh, and Behrouz Fathi-Vajargah. "A novel image encryption scheme based on clifford attractor and noisy logistic map for secure transferring images in navy." International Journal of e-Navigation and Maritime Economy 6 (2017): 53-63.
27. Farwa, Shabieh, et al. "An image encryption technique based on chaotic S-box and Arnold transform." International Journal of Advanced Computer Science and Applications 8.6 (2017).
28. Wang, Xingyuan, Xiaoqiang Zhu, and Yingqian Zhang. "An image encryption algorithm based on Josephus traversing and mixed chaotic map." IEEE Access 6 (2018): 23733-23746.
29. Liu, Xingbin, Di Xiao, and Yanping Xiang. "Quantum image encryption using intra and inter bit permutation based on logistic map." IEEE Access 7 (2018): 6937-6946.

30. Gopalakrishnan, T., and S. Ramakrishnan. " Image encryption in block-wise with multiple chaotic maps for permutation and diffusion." ICTACT Journal on Image & Video Processing 6.3 (2016).
31. Zhu, Congxu, and Kehui Sun. "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps." Ieee Access 6 (2018): 18759-18770.
32. Munir, Noor, et al. "Cryptanalysis of nonlinear confusion component-based encryption algorithm." Integration 79 (2021): 41-47.
33. Alanazi, Ammar S., et al. "Cryptanalysis of novel image encryption scheme based on multiple chaotic substitution boxes." IEEE Access 9 (2021): 93795-93802.
34. Alanazi, Ammar S., et al. "Cryptanalysis of novel image encryption scheme based on multiple chaotic substitution boxes." IEEE Access 9 (2021): 93795-93802.
35. Shafique, Arslan. "A new algorithm for the construction of substitution box by using chaotic map." The European Physical Journal Plus 135.2 (2020): 194.