Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 5, pp. 1507–1522
DOI : 10.47974/JDMSC-1934

An efficient hybrid chaotic map-based encryption technique for multiple image security systems

Mohanad J. Jaber *
Department of Basic Science
College of Dentistry
Kufa University
Najaf
Iraq

Zahraa Jasim Jaber †
Ahmed J. Obaid §
Department of Computer Science
Faculty of Computer Science and Mathematics
Kufa University
Najaf
Iraq

Abstract

Researchers are increasingly interested in image encryption in the modern technological era. Their goal is to improve the security of image data from unauthorized sources. Due to its randomness and unpredictable behavior, chaos theory is considered the most suitable method for encrypting images. An image encryption algorithm based on diffusion maps is presented in this paper. An element of nonlinearity is generated by modifying the pixel values with a chaotic map first. Three chaotic maps are used in the proposed image encryption scheme. In an efficient encryption algorithm based on the improved three chaotic maps, the permuted image is subjected to a diffusion process using the key from the original image. This scheme has the advantage of a large key space and is resistant to various attacks. Real-time applications are suitable for the proposed scheme because of their high-security level and low computational complexity.

Subject Classification: *68P25, 94A60.*

Keywords: *Encryption, Map-based, Image security, Chaotic map.*

* *E-mail:* **mohanad.altalqani@uokufa.edu.iq (Corresponding Author)**
† *E-mail:* **zahraaj.altalakany@uokufa.edu.iq**
§ *E-mail:* **ahmedj.aljanaby@uokufa.edu.iq**

© Taru Publications

1. Introduction

Multimedia content is protected from unauthorized access with security measures. The data in an image differs from the data in text; it contains more data, more redundancy, and a higher correlation between pixels than text. In addition to the lack of standard encryption algorithms like RSA, AES, and DES, traditional encryption algorithms cannot directly encrypt images [1]. Traditional cryptosystems take a lot of time to encrypt image data directly due to their larger size than text. Decrypted texts must also be equivalent to original texts. However, this is not necessary for images because human perception allows for small distortions in a decrypted image [2]. In the practical world, chaotic signals are highly useful because of their characteristics, such as their high sensitivity to initial conditions and system parameters, their pseudorandom properties, and their non-periodic nature since chaotic signals are usually noise in nature. Information security benefits from the combination of chaotic theory and cryptography. Since chaotic signals resist statistical attacks, chaos systems are excellent cryptosystems. Chaotic systems have been used in a variety of image encryption algorithms [3]. Several algorithms have been developed based on chaotic maps, including the logistic, Baker, and cat maps. Image encryption algorithms use shuffled pixels to enhance security performance using plain images. A proposed encryption process is secured through the use of two chaotic maps.

Digital documents are often protected by scrambling their contents to hide their true message. For example, compression, digital watermarking, steganography, and cryptography are some methods of achieving this [4]. Our paper focuses on the encryption and chaos mapping methods used to protect digital images. The authors propose an image encryption algorithm with chaos mapping by rearranging pixels based on their location and performing a Boolean XOR operation to transform gray scale values into an encrypted image. Mathematicians study chaos theory, a branch of nonlinear systems highly susceptible to initial conditions. It is a branch of science that deals with continuous and nonlinear systems with properties similar to random behavior. Chaos has the following properties: [5]:

(i) A deterministic system is one in which mathematical equations decide their behavior.

(ii) The initial conditions do not predict their behavior, making them nonlinear and unpredictable. The results can significantly differ

from one starting point to another, even if the starting point is very slight.

(iii) Despite appearing random and disorderly, they are well organized. Order and pattern lie beneath random behavior. Among the most attractive features of deterministic chaotic systems is their highly unpredictable and random-looking output, which could be used for a wide range of unconventional applications [6].

2. Related Work

Since the last decade, researchers have been researching chaos encryption. This topic has been discussed in several papers, most of which discuss how chaos encryption can be used in optical data transmission and secure communication [7]–[16]. There have, however, been several proposals for chaotic image encryption algorithms over the past five years. Using some chaotic function, these algorithms scatter pixels. The authors [17], [18] proposed two chaotic image encryption algorithms based on a chaotic system generating random binary sequences. Due to the vulnerability of [19], the author improved the chaotic encryption scheme.

In contrast, [1] and [17] proposed an alternative chaotic image encryption algorithm without requiring a chaotic generator. Rather, Baker's map transformation permutes the pixel's position. According to [2], all algorithms propose a square image as the object to be encrypted [20].

There is an algorithm called Rivest–Shamir–Adleman (RSA) that combines topological image protection with Rivest–Shamir–Adleman (RSA) component components [21], [22]. A functional fluctuation intensity image is the main advantage of the suggested approaches [21]. An earlier study examined how noise-adding functions and the number of simple numbers in the RSA scheme affected the results. Due to these results, an encrypted image was not supposed to have contours [23]. There are also other approaches to decrypting and encrypting images, such as linear and quadratic fractal algorithms [24], [25], as well as linear-quadratic transformations [26] and binary linear-quadratic transformations[27]. An image encryption model has been proposed based on a customized advanced encryption standard and a chaos-based pseudorandom number generator [28]. Altera Cyclone III was used to create the entire system. Cryptography algorithm was found to be faster and able to resist attacks [28], [29]. In [30], chaotic hybrid maps were used to introduce a grayscale image cryptosystem. More dynamic chaotic behavior and a broader chaotic range are among the benefits of the proposed scheme [30, 31].

Confusion and diffusion are the two main phases of the proposed encryption process. The proposed image encryption algorithm and cryptanalysis have been tested. Also, we measure the proposed algorithm with various analysis experiments, including histograms, entropies, average changing intensities (UACI), mean square errors (MSE), peak signal-to-noise ratios (PSNRs), and Key Space analysis.

3. Proposed Cryptosystem Model

This paper adopted two chaotic maps (Arnold's cat map, Henon Map and logistic map) to encrypt the image. We first introduce Arnold's cat map, Henon map, and logistic map before illustrating the suggested encryption and decryption mechanism.

Before running the algorithm, $\alpha, \beta,$ and (x_0, y_0) must be initialized, as well as some other variables. As shown in Figure 1, the encrypted architecture is proposed. A bit- and pixel-level permutation step is used in this scheme based on two secret images. Unlike bitwise permutations, pixel permutations shuffle pixels without altering their values or histograms.

Encryption and decryption processes require the creation of secret images and *P* and *Q* parameters for Arnold cat maps. Henon maps produce coordinates *x* and *y* for secret images that are pseudo-random-like in terms of pixel distributions. The plain and secret images determine the number of iterations in Hernon maps. A gray-level image of $m \times m$ is used in this study for experiments. Thus, Henon maps should have at least m^2 iterations. There seems to be a fairly close correlation between the first few iterations. To ensure higher randomness, the first 100 points are discarded to make the total number of iterations $m^2 + 100$. Based on the x- and y-coordinates of the Henon map, these pseudorandom pixel values $(0 \le pixX_i,\ pixY_i \le 255)$ represent *pixX* and *pixY*, respectively. The 2D *secImgX* and *secImgY* secret image is created by applying (2) and (4) to the one-dimensional pixel values. On the corresponding pixels, apply the XOR operation. The final secret image is formed from *secImgX* and *secImgY*. Deliberate

$$pixX_i = abs(x_{100+i} \times \gamma) \bmod 256, \quad i = 1, \ldots, m^2, \tag{1}$$

$$secImgX = reshape(pixX, m, m), \tag{2}$$

$$pixY_i = abs(x_{100+i} \times \gamma) \bmod 256, \quad i = 1, \ldots, m^2, \tag{3}$$

$$secImgY = reshape(pixY, m, m), \tag{4}$$

$$secImg = xor(secImgX, secImagY), \tag{5}$$

Arnold cat map is constructed by permuting P and Q parameters. The Henon map's x-ordinates and y-ordinates are applied to generate parameters for the ACM. Arnold cat maps return pixels to their preliminary positions after a finite number of iterations. The periodicity of this image may enable attackers to recover the original image. A different value for the parameters P and Q is used in each $q$round to prevent such reconstruction of the input image. As a result of equations (6) and (7), the Arnold cat map parameters can be calculated. As the permutation rounds increase, so do the generated parameters:

$$P_i = abs(x_{100+i} \times 10^{14}) \bmod \delta, \quad i = 1, \ldots, p*(q+r), \tag{6}$$

$$Q_i = abs(y_{100+i} \times 10^{14}) \bmod \delta, \quad i = 1, \ldots, p*(q+r), \tag{7}$$

3.1 *Encryption Process*

In Figure 1, you can see the encryption scheme proposed. Encrypted images are created by combining inputs and outputs. For this model, three inputs are required: plain image, *secImgX*, and *secImgY*. Permuting bits, modifying pixels, and permuting pixels are three of the most important functions. To generate secImg, *secImgX* and *secImgY* are *XORed* pixel by pixel as shown in Figure 1. Afterwards, q rounds of permutation are performed on the secret image. The plain image is permuted r times simultaneously. The outputs of these phases modify this sequence of pixels. Rather than feeding back the plain image to the bit permutation function, secImg is permuted with new parameters at each iteration. In the following sections, we describe the functions in more detail.

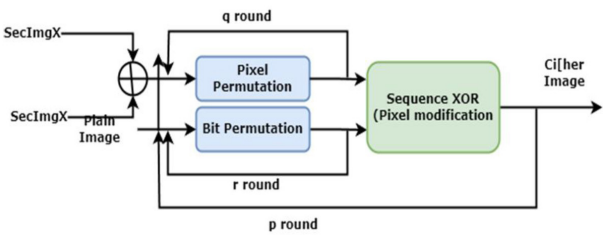

Figure 1

Proposed encryption scheme architecture

A. Bit Permutation

$m \times m \times 8$ bits are needed for a gray-level image having $m \times m$ pixels. Eight sub-images are created before bit permutation occurs. According to Figure 2, each subimage measures $m \times \frac{m}{8}$ pixels high and $m \times m$ pixels wide. The KTH subimage creation process is illustrated in the matrix (8). The subimage would be created by replacing the input image pixel values with their corresponding matrix values. Using binary representation, (i, j) represents nine pixels, with $b(8)$ representing the most significant bit. In the bit-plane, each row has m elements, each with a bit of value 0 or 1. An example of a bit-plane matrix can be seen in matrix (10). There are two types of bit-planes: $m \times m$ bit-planes and subimage bit-planes. Permutations and conversions of each bit-plane to their $m \times m$ equivalents are conducted independently:

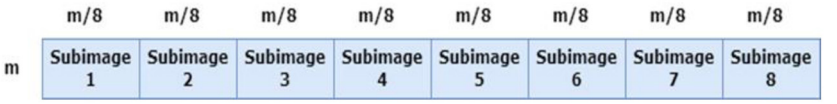

Figure 2

Splitting an image to 8 subimages

$$subImage_k = \begin{bmatrix} img\left(1,(k-1)*\frac{m}{8}+1\right) & \cdots & img\left(1,k*\frac{m}{8}+1\right) \\ img\left(2,(k-1)*\frac{m}{8}+1\right) & \cdots & img\left(2,k*\frac{m}{8}+1\right) \\ \vdots & & \\ \vdots & & \\ img\left(m,(k-1)*\frac{m}{8}+1\right) & \cdots & img\left(m,k*\frac{m}{8}+1\right) \end{bmatrix}, k = 1,.,8, \tag{8}$$

$$img)i, j) = b(8)b(7)\ldots.b(1), \tag{9}$$

$$bitPlane_k = \begin{bmatrix} b_{\left(1,(k-1)*\frac{m}{8}+1\right)}(8) & b_{\left(1,(k-1)*\frac{m}{8}+1\right)}(7) & \cdots & b_{\left(1,k*\frac{m}{8}\right)}(1) \\ b_{\left(2,(k-1)*\frac{m}{8}+1\right)}(8) & b_{\left(2,(k-1)*\frac{m}{8}+1\right)}(7) & \cdots & b_{\left(2,k*\frac{m}{8}\right)}(1) \\ & \vdots & & \\ & \vdots & & \\ b_{\left(m,(k-1)*\frac{m}{8}+1\right)}(8) & b_{\left(m,(k-1)*\frac{m}{8}+1\right)}(7) & \cdots & b_{\left(m,k*\frac{m}{8}\right)}(1) \end{bmatrix} \tag{10}$$

We permuted the bits using the Arnold cat map after creating the *bitplane* matrices. As a result of the permutation, each bit is moved to a new location by (11). As (x,y) moves to $(x, y),$ the pair of (x′, y′) becomes more significant. To start with, $i=1,\ldots,r$ uses different parameters *P* and *Q*. for permuting the input image r times. Consider

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & P_i \\ Q_i & P_iQ_i+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod m \tag{11}$$

When the *bitplane* matrixes are complete, the image pixels are reconstructed using decimal values.

B. Pixel Permutation

A secret image is randomly generated for q rounds while the plain image's bits are permuted. The pixel values are not affected by pixel permutation, unlike bit permutation. Thus, the histogram of a plain and shuffled image is identical. P and Q are permuted times with $j=1,\ldots,q,$ each time with a different parameter *P* and *Q*. Consider

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & P_j \\ Q_j & P_jQ_j+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod m \tag{12}$$

C. Pixel Modification

Pixel values are modified in the concluding phase. The cipher image pixels will be drastically altered if even one bit is changed in this step. For this step, we use the plain image permuted at bit levels and the shuffled secret image. Pixels are changed consecutively using equations (13) and (14). A modified image is the result of this step. This step will be repeated for *p* rounds to create more confusion and modification. Rounds are permuted based on a secret image replaced with an input plain image after each *q* round. An image of the cipher is created after *p* rounds have been completed. Consider

$$img(1) = xor(img(1), secImg(1)), \tag{13}$$

$$img(i) = xor(img(i-1), secImg(i)), \tag{14}$$

3.2 *Decryption Process*

The decryption process is shown in Figure 3. A private parameter is used to recreate the secret image on the receiving end by using *XORing,*

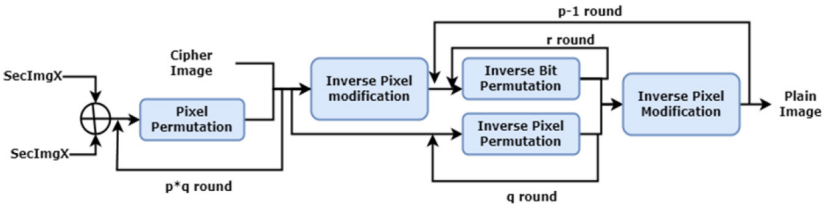

Figure 3

Decryption model architecture

secImgX, and *secImgY*. As a result of $p \times q$ rounds of pixel permutations, during the inverse pixel modification process, both the cipher image and the secret image are altered. In the first step, we perform a secret pixel permutation and save it for later use. It is then applied to the function for inverse pixel modification for q rounds each time. Inverse bit permutation output is the additional input after the inverse pixel modification function.

4. Result Analysis

Image encryption is strong when it is not vulnerable to attack. The encryption image can be tested for robustness against various attacks through many performance tests. Various security measurement metrics were used to assess the security of the proposed method. As shown in Figure 4, Lena images were used for color and gray 512 x 512 image encryption simulations. The experimental analysis was achieved using MATLAB R2020a. We have used three analyses to measure the effectiveness and security of the encryption algorithms: Intensity histogram analysis, Adjacent pixel autocorrelation test and key sensitivity tests.

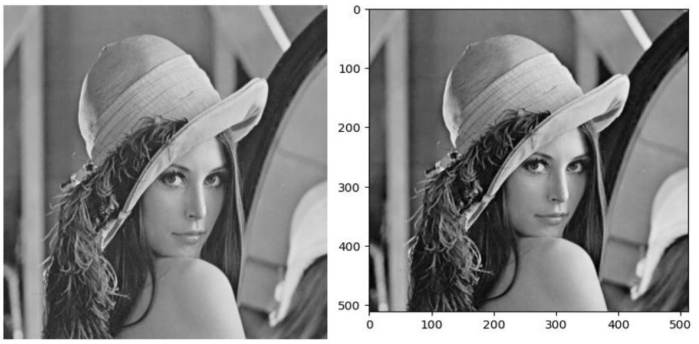

Figure 4

Original Image

4.1 *Histogram Analysis*

A histogram is a graphic representation of the frequency of an image. Each pixel value is plotted across all possible pixel values to calculate the frequency. Histograms of plain images show uneven pixel frequency distributions, while histograms of well-encrypted images show equal pixel frequency distributions. The figure illustrates the histogram of ciphered and original images. A histogram of ciphered images shows a consistent distribution across the area from the figures. This design approach creates ciphered images that do not release any analytical data to fraudsters. The histograms of the plane and cipher images are shown in Figure 5. Arnold cat encryption has the same intensity histogram as the original image. Arnold Cat shuffles the pixels and does not change any pixel values. A logistic map-based encryption system has the most uniform histogram, indicating a highly effective encryption system.

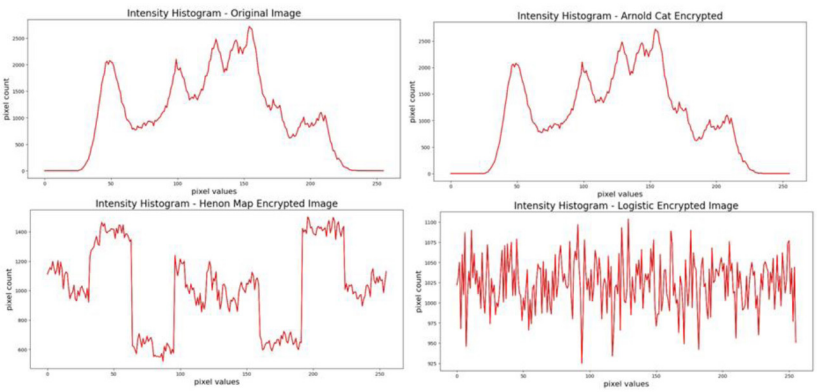

Figure 5

Intensity histogram

4.2 *Adjacent Pixel Autocorrelation Test*

There is a strong relationship between the horizontal and vertical neighbors of pixels in digital photographs. It is feasible to reliably ascertain pixel values by statistical analysis of photos with inadequate encryption. A correlation between the original and encrypted image can be seen by signal autocorrelation. A ciphered image is tested for vertical and horizontal correlation between neighboring pixels. An encryption algorithm that breaks images' information redundancy is desirable since

images exhibit high information redundancy. Therefore, we consider the correlation between adjacent pixels in a given direction (Horizontal, Vertical, or Diagonal) as a metric of encryption performance. The correlation between 1024 random pixels of an image is found and plotted for its rightmost neighbours in this test.

An image consists of elements that are extremely connected crosswise, vertically, and horizontally. An attacker uses this relation to crack encryption algorithms. However, a connection between adjacent elements should be reduced for an encrypted image. This paper calculates the connection between adjacent elements using an autocorrelation coefficient. Figures 6-8 show the graphical evaluation of the autocorrelation coefficient for Arnold Cat, Henon, and logistic maps. As a result of the proposed technique, adjoining elements of encrypted images are loosely correlated. Thus, the proposed technique protects from statistical attacks. This cipher image has less obvious patterns than the Arnold cat map. Autocorrelation

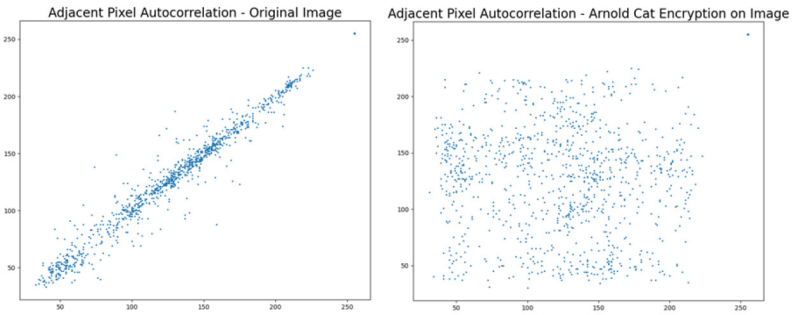

Figure 6

Graphical view of adjacent pixel autocorrelation evaluation for Arnold Cat Map

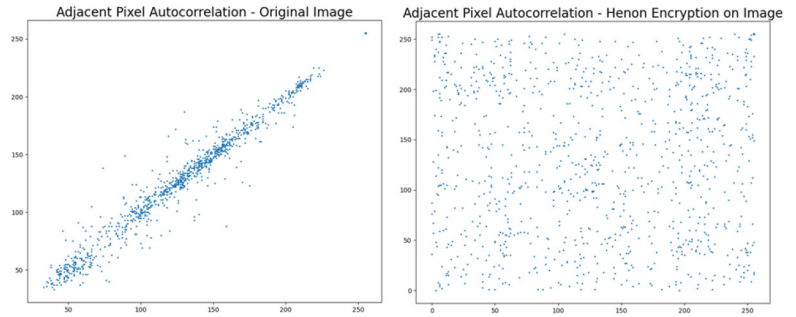

Figure 7

Graphical view of adjacent pixel autocorrelation evaluation for Henon Map

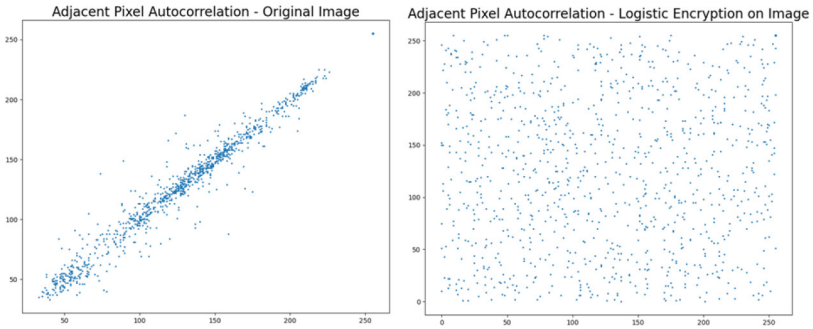

Figure 8

Graphical view of adjacent pixel autocorrelation evaluation for Logistic Map

graphs for encrypted images based on logistic chaos maps have a higher degree of randomness than for encrypted images based on Henon encrypting schemes, once again demonstrating the superiority of logistic chaos maps based on key mixing.

4.3 *Key sensitivity*

The highly sensitive behavior of the secret key is another essential requirement for an image encryption scheme. A single-bit change in the secret key can result in a completely different encrypted result for a good encryption system. There is a high degree of sensitivity to these chaotic maps' initial conditions and control parameters. The generated random sequence will completely change if we make a very insignificant key or control parameter change. The result is an entirely different encryption/decryption process. Therefore, the suggested image encryption system must be extremely sensitive to the initial key if an incorrect key is generated with little variation from the initial key. A plaintext image encrypted with two keys that differ by one bit can be decoded using each key. As a result, an effective encryption method should prevent the original picture data from being recovered during decryption.

Our test involves encrypting a plain image with the three algorithms to measure their key sensitivity. A slightly modified key is then used to decrypt them. Figure 9-11 shows that the Arnold cat map, the Henon map, and the logistic map algorithms are not affected by a change in key. Compared to the plain image, the resultant image has discernible features. The Arnold cat algorithm cannot be used in practice because of its periodicity. The encryption of both Henon maps and Logistic maps

appears sensitive to key changes. Two keys are used to encrypt and decrypt the same plaintext image. It is possible to decrypt the original image using the same key, but it is impossible to decrypt the original image with another key.

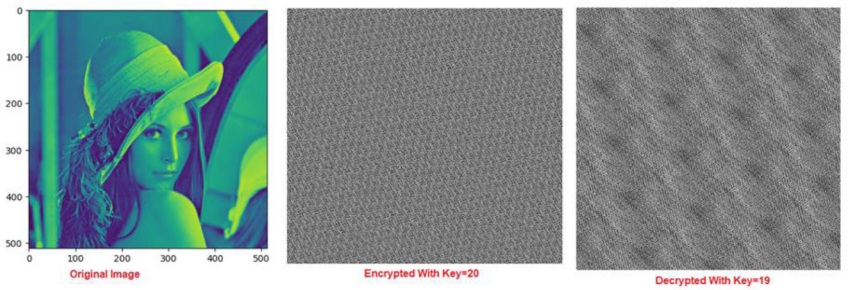

Figure 9

Key sensitivity for Arnold Cat Map

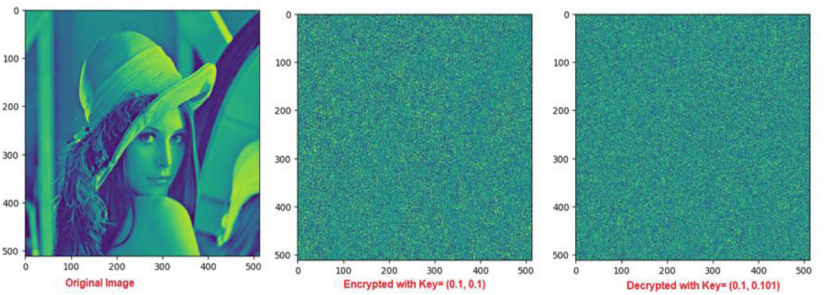

Figure 10

Key sensitivity for Henon Map

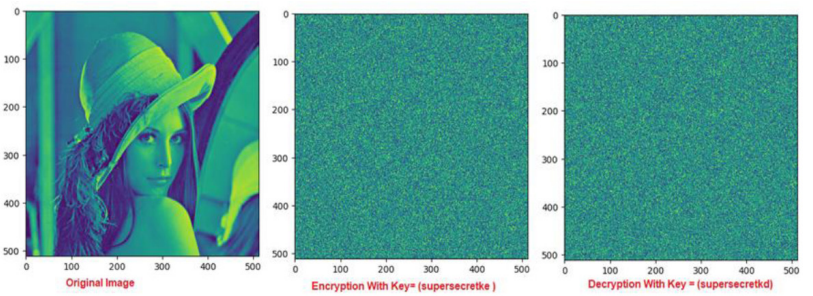

Figure 11

Key sensitivity for Logistic Maps

5. Conclusion

Security is one of the most important issues of the modern world, and encryption is one of the best ways to ensure security. Several image encryption schemes have also been proposed, each with strengths and weaknesses. An image encryption/decryption scheme is presented in this paper. Multiple chaotic-based circular mapping is used in this paper to provide a secure image encryption technique. As a result, we propose an image cipher that encrypts color images using the Henon map, Logistic map, and Arnold's cat map. Various security analyses and experimental results show that this system exhibits good security characteristics, is robust against noise, data loss, and cryptanalysis attacks, and can be implemented in real-time.

References

[1] P. Rani, P. N. Singh, S. Verma, N. Ali, P. K. Shukla, and M. Alhassan, "An implementation of modified blowfish technique with honey bee behavior optimization for load balancing in cloud system environment," *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. 1–14 (2022).

[2] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurc. Chaos*, vol. 8, no. 06, pp. 1259–1284 (1998).

[3] P. Rani, S. Verma, S. P. Yadav, B. K. Rai, M. S. Naruka, and D. Kumar, "Simulation of the Lightweight Blockchain Technique Based on Privacy and Security for Healthcare Data for the Cloud System," *Int. J. E-Health Med. Commun. IJEHMC*, vol. 13, no. 4, pp. 1–15 (2022).

[4] S. P. Yadav, M. Jindal, P. Rani, V. H. C. De Albuquerque, C. Dos Santos Nascimento, and M. Kumar, "An improved deep learning-based optimal object detection system from images," *Multimed. Tools Appl.*, Sep. (2023), doi: 10.1007/s11042-023-16736-5.

[5] M. Salleh, S. Ibrahim, and I. F. Isnin, *Ciphering key of chaos image encryption*. Universiti Teknologi Malaysia (2002).

[6] G. Jakimoski and L. Kocarev, "Chaos and cryptography: block encryption ciphers based on chaotic maps," *Ieee Trans. Circuits Syst. Fundam. Theory Appl.*, vol. 48, no. 2, pp. 163–169 (2001).

[7] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, "A secret key cryptosystem by iterating a chaotic map," in Advances in Cryptology—EUROCRYPT'91: Workshop on the Theory and Application of Crypto-

graphic Techniques Brighton, UK, April 8–11, 1991 Proceedings 10, Springer, pp. 127–140 (1991).

[8] Z. Kotulski and J. Szczepański, "Discrete chaotic cryptography," *Ann. Phys.*, vol. 509, no. 5, pp. 381–394 (1997).

[9] B. Fraser, P. Yu, and T. Lookman, "Secure communications using chaos synchronization," *Phys Can. Spec. Issue Non-Linear Dynam*, vol. 57, no. 2, pp. 155–61 92001).

[10] J. Scharinger, "Secure and fast encryption using chaotic Kolmogorov flows," in *1998 Information Theory Workshop (Cat. No. 98EX131)*, IEEE, pp. 124–125 (1998).

[11] M. Svensson and J.-E. Malmquist, "A simple secure communications system utilizing chaotic functions to control the encryption and decryption of messages," Proj. Rep. Course 'Chaosinscienceandtechnology' Lund Inst. Technol. Dept Phys. Sub-Dept Math. Phys., (1996).

[12] K. L. Shore, "Infrastructure for Chaotic Optical Data Encryption," EPSRC Proj. GRK78799 (2000).

[13] M. Salleh, S. Ibrahim, and I. F. Isnin, "Image encryption algorithm based on chaotic mapping," *J. Teknol.*, vol. 39, no. D, pp. 1–12 (2003).

[14] M. I. Sobhy and A.-E. Shehata, "Chaotic algorithms for data encryption," in 2001 IEEE international conference on acoustics, speech, and signal processing. Proceedings (Cat. No. 01CH37221), IEEE, pp. 997–1000 (2001).

[15] S. Li, X. Zheng, X. Mou, and Y. Cai, "Chaotic encryption scheme for real-time digital video," in *Real-Time Imaging VI*, SPIE, pp. 149–160 (2002).

[16] N. Hussain and P. Rani, "Comparative studied based on attack resilient and efficient protocol with intrusion detection system based on deep neural network for vehicular system security," in *Distributed Artificial Intelligence*, CRC Press, pp. 217–236 (2020). Accessed: Oct. 19, 2023. [Online].Available: https://www.taylorfrancis.com/chapters/edit/10.1201/9781003038467-13/comparative-studied-based-attack-resilient-efficient-protocol-intrusion-detection-system-based-deep-neural-network-vehicular-system-security-naziya-hussain-preeti-rani.

[17] J.-C. Yen and J.-I. Guo, "A new chaotic mirror-like image encryption algorithm and its VLSI architecture," *Pattern Recognit. Image Anal. Adv. Math. Theory Appl.*, vol. 10, no. 2, pp. 236–247 (2000).

[18] N. Hussain, P. Rani, H. Chouhan, and U. S. Gaur, "Cyber Security and Privacy of Connected and Automated Vehicles (CAVs)-Based Federated Learning: Challenges, Opportunities, and Open Issues," in *Federated Learning for IoT Applications*, S. P. Yadav, B. S. Bhati, D. P. Mahato, and S. Kumar, Eds., in EAI/Springer Innovations in Communication and Computing. , Cham: Springer International Publishing, pp. 169–183 (2022). doi: 10.1007/978-3-030-85559-8_11.

[19] S. Li, X. Mou, and Y. Cai, "Improving security of a chaotic encryption approach," *Phys. Lett. A*, vol. 290, no. 3–4, pp. 127–133 (2001).

[20] J. Fridrich, "Image encryption based on chaotic maps," in 1997 IEEE international conference on systems, man, and cybernetics. Computational cybernetics and simulation, IEEE, pp. 1105–1110 (1997).

[21] A. Kovalchuk, I. Izonin, M. Gregush Ml., and N. Kustra, "Information Protection Service using Topological Image Coverage," *Procedia Comput. Sci.*, vol. 160, pp. 503–508 (2019), doi: 10.1016/j.procs.2019.11.057.

[22] S. Verma *et al.*, "An automated face mask detection system using transfer learning based neural network to preventing viral infection," *Expert Syst.*, p. e13507, Nov. (2023), doi: 10.1111/exsy.13507.

[23] A. Kovalchuk, N. Lotoshynska, M. G. Ml., I. Izonin, and L. Berezko, "An Approach towards an Efficient Encryption-Decryption of Grayscale and Color Images," *Procedia Comput. Sci.*, vol. 155, pp. 630–635 (2019), doi: 10.1016/j.procs.2019.08.089.

[24] A. Kovalchuk, I. Izonin, M. Gregush Ml., and N. Lotoshynska, "An Approach Towards Image Encryption and Decryption using Quaternary Fractional-Linear Operations," *Procedia Comput. Sci.*, vol. 160, pp. 491–496 (2019), doi: 10.1016/j.procs.2019.11.059.

[25] A. Kovalchuk, I. Izonin, C. Strauss, M. Podavalkina, N. Lotoshynska, and N. Kustra, "Image Encryption and Decryption Schemes Using Linear and Quadratic Fractal Algorithms and Their Systems.," in *DCSMart*, pp. 139–150 (2019).

[26] A. Kovalchuk, I. Izonin, M. Gregush Ml., and O. Riznyk, "An Efficient Image Encryption Scheme using Projective Transformations," *Procedia Comput. Sci.*, vol. 160, pp. 584–589 (2019), doi: 10.1016/j.procs.2019.11.043.

[27] A. Kovalchuk and N. Lotoshynska, "Elements of RSA algorithm and extra noising in a binary linear-quadratic transformations during encryption and decryption of images," in *2018 IEEE Second International*

Conference on Data Stream Mining & Processing (DSMP), IEEE, pp. 542–544 (2018).

[28] A. Hafsa, M. Gafsi, J. Malek, and M. Machhout, "FPGA implementation of improved security approach for medical image encryption and decryption," *Sci. Program.*, vol. 2021, pp. 1–20 (2021).

[29] P. Rani *et al.*, "Federated Learning-Based Misbehaviour Detection for the 5G-Enabled Internet of Vehicles," *IEEE Trans. Consum. Electron.*, pp. 1–1 (2023), doi: 10.1109/TCE.2023.3328020.

[30] A. Pourjabbar Kari, A. Habibizad Navin, A. M. Bidgoli, and M. Mirnia, "A new image encryption scheme based on hybrid chaotic maps," *Multimed. Tools Appl.*, vol. 80, no. 2, pp. 2753–2772, Jan. (2021), doi: 10.1007/s11042-020-09648-1.

[31] Azmi Shawkat Abdulbaqi, Ahmed J. Obaid & Maysaa Hameed Abdulameer. Smartphone-based E.C.G. signals encryption for transmission and analyzing via IoMTs, *Journal of Discrete Mathematical Sciences and Cryptography* (2021), DOI: 10.1080/09720529.2021.1958996.

Received November, 2023