Received: May 20, 2023. Revised: June 20, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A High-Security Image Utilizing Triple Generators for the Rabinovitch System

Noor Haider Witwit[1] **Ali Yakoob Al-Sultan**[1]*

[1]*Department of Computer, College of Science for Women, University of Babylon, Babylon, Iraq*
* Corresponding author's Email: *wsci.ali.yakoob@uobabylon.edu.iq

Abstract: Chaotic encryption offers a higher level of security than traditional ciphers. This research provides an encryption system using chaotic sequences to encrypt digital images using three hyperchaotic methods. The first system generates a random integer number sequence between (0 - 255), while the second and third hyper-chaotic generators use a chaotic random selector from the random number generated from the first hyperchaotic generator and the image pixels. The third system is used to chaotic select the pixel from the image. Then the pixel value is changed using the XOR operation to encrypt the pixels. The number of keys depends on 33 dimensions (each hyper-chaos has 11 dimensions, four initial values, five parameters, and two big and mod numbers), and all available keys at less than 2^{1644}. This number represents a massive key space.

Keywords: Chaotic scrambling, Image encryption, Testing quality of image.

1 Introduction

Everyone has the right to privacy protection, particularly on the Internet, which is tied to information security. Digital images have emerged as one of the most popular internet content types because they contain important information and are characterized by solid pixel correlation and redundancy [1]. A famous study area deals with how to encrypt images and guard against improperly decoded information. Traditional encryption techniques are complicated since image encryption standards are becoming more stringent [2].

Chaos theory, which has its roots in physics and mathematics, examines the behavior of nonlinear dynamical systems that show a high sensitivity to their starting circumstances. In the context of image encryption, chaos-based algorithms utilize the unpredictable nature of chaotic systems to provide a high level of security. These algorithms leverage the inherent randomness and complex dynamics of chaotic maps or systems, making it extremely difficult for adversaries to decipher the encrypted images without the correct decryption key. In contrast to traditional methods, chaos-based image encryption offers several notable advantages [3, 4]. Chaos-based encryption techniques provide a higher security level than traditional methods. The complex and unpredictable nature of chaotic systems makes it challenging for attackers to reverse-engineer the encryption process and retrieve the original image [5]. Key sensitivity: Chaos-based encryption algorithms exhibit key sensitivity, indicating that even a slight alteration to the encryption key results in a significantly altered encrypted picture. This characteristic improves the system's security and resilience to brute-force assaults [6].

This study offers a solution for encrypting digital images that use three hyperchaotic generators to create chaotic sequences. While the second and third hyper-chaotic generators employ a chaotic random selection from the random number obtained by the first hyper-chaotic generator and the picture pixels, the first system creates a random integer number sequence between (0 - 255). The third system is employed to choose a pixel from the picture randomly. Then, the pixel value is modified using the XOR technique to encrypt the pixels.

2 Literature review

In 2023, Alexan, Wassim, et al. The KAA map combines several chaotic maps in the proposed color picture encryption technique employing Shannon's security concepts. Two encryption keys are used to

create confusion, the other from the 2D Logistic Sine map and a linear congruential generator, one from the tent map and the Bernoulli map. To accomplish diffusion, the KAA map is employed [7]. In 2023, Q. Liang and C. Zhu claimed that SCCMs in one dimension might be corrected using information from SCCMs in higher dimensions. They also provide SCCM and random DNA-based image encryption services. The method takes its cues from random DNA coding by randomly selecting encoding, decoding, and computation rules using chaotic sequences and the assumption of one pixel per rule [8]. A color image encryption method based on a random phase mask and structural chaotic measurement matrix was presented in 2020 by X. Wang and Y. Su. The Chebyshev chaotic sequence generates the chaotic cyclic matrix, the sampling subset, and the fip permutation matrix. A two-dimensional fractional Fourier transform is used to re-encrypt the original image after it has been concurrently compressed and encrypted using compressed sensing. Simulation experiments show how effective and reliable the method is [9]. In 2021, Long, Min, and Li Tan. The Chebyshev map, logistic map, and nonlinear chaotic algorithm (NCA) are used to encrypt and decode pictures and other data. The approach is very sensitive to the plaintext and keys, and it can survive existing attacks such as information entropy attacks, statistics attacks, and chosen/known plaintext attacks, according to the method's security analysis published in total [10].

In 2020, Yasser, Ibrahim, et al. For highly secure data transfer, novel chaotic-based multimedia encryption techniques are presented. It is suggested to use a hybrid chutnification structure in which several maps are integrated to produce control parameters for diffusion and permutation structures. Control parameters are produced using blended chaotic maps [11]. In 2018, Hreshee, et al. presented a highly secure communication system built on chaotic systems with two degrees of encryption. Chaos is present at two levels: scrambling and masking [12]. In 2020, Song et al. produced multi-layer quantum video encrypting using controlled XOR operations on a qubit plane and a refined logistical road map. The proposed technique employs three fundamental cryptographic operations: permutation between frames, geometric alteration of pixel positions within frames, and scrambling on four planes inside each frame. The inter-frame positions of a quantum movie can be juggled with the use of keys generated by a revised logistic map. Secondly, a geometric transformation and a logistic map are used to encrypt the pixel coordinates used inside a single frame. Quantum controlled XOR operations and an improved logistic map jumble the high-order 4-intra-frame qubit planes[13]. In 2022, Alibraheemi, et al., A stream cipher-based picture encryption technique employing multi-dimensional hyperchaotic generators is designed and implemented on FPGAs. XORing three hyperchaotic generators creates a new pseudo-random bit generator for picture pixels masking (encryption). Forward euler integration solves the hyperchaotic dynamical equations and combines binary streams to yield encryption-ready random bits. [14]. In 2020, Hussein, E. et al. A voice signal-encrypted communication system is presented. Two layers of chaotic masking on the signal were used to accomplish the security approach: Lorenz and Rossler chaotic flow systems. This two-chaotic masking strategy aims to boost keyspace and data security. To minimize noise, the recommended strategy uses immunity. This system was tested with AWGN channel noise for practical use [15].

3 Hyper chaotic rabinovitch system (HCRS)

Nonlinear processes generate non-periodic and chaotic signals and have noise characteristics. Interactional systems have a predetermined number of state variables governed by a system of differential equations. Chaotic state variables in dynamical systems are characterized by limited, non-periodic sensitivity to initial conditions and parameters and seemingly random fluctuations[16-18].

Additionally, they possess a trait called a sensitive dependency on the beginning—conditions, meaning that any two close starting conditions will result in the same result. Lead to two state variable motions or trajectories that are easily entirely uncorrelated. This characteristic enables the creation of an endless number of chaotic signals from the same system with various beginning values [12]. The types of chaos are chaotic map and chaotic flow. The chaotic flow model is a continuous-time system generated from differential equations:

$$\dot{x} = dx/dt = \dot{x}(t) \tag{1}$$

where $dx/dt \; and \; \dot{x}$ the system's state vector at the time (t) in a dynamic system, Rossler systems, Lorenz systems, Chen's systems, Chua systems, and Lü systems are all well-known examples of chaotic flows for which f(.) is a function[13, 19, 20].

The chaotic map is a function of evolution that shows chaotic behavior. A discrete-time can be used as a parameter for chaotic maps. Typically, discrete mappings have the shape of kth-iterated functions. The study of dynamical systems typically involves chaotic maps.[20].

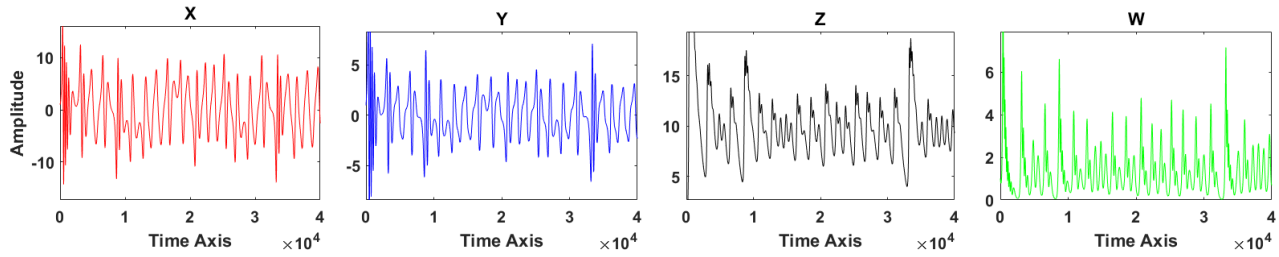


Figure. 1 All vectors to the Rabinovitch system's time series

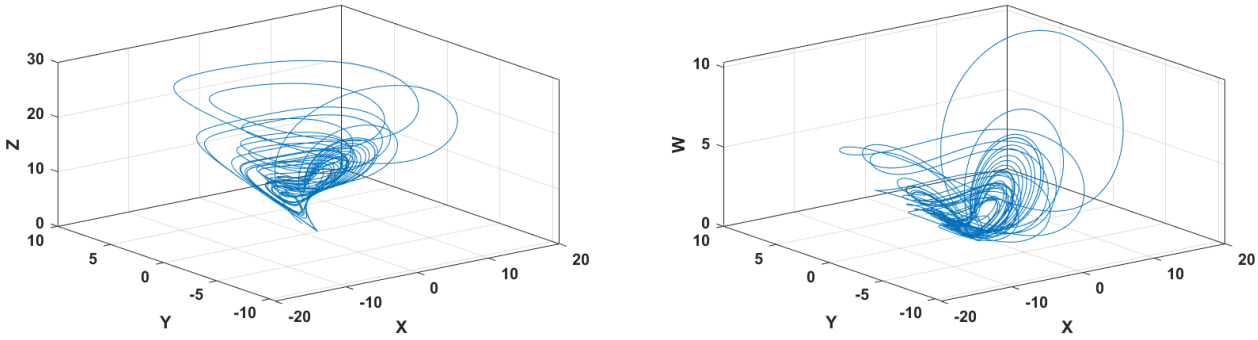


Figure. 2 Portraits in three dimensions of the Rabinovitch system

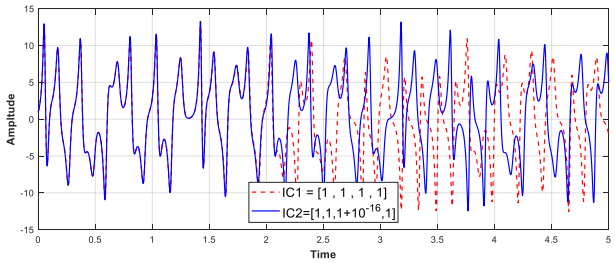


Figure. 3 Sensitive to initial conditions

$$X_{k+1} = g(X_k) \quad (2)$$

X_k represents the state vector, and g(.) represents the chaotic map's iterative function. Famous maps include the following: Cat map, Hénon map, Standard map, and Logistic map.

Continuous-time hyper-chaotic autonomous systems must have four dimensions and two positive Lyapunov exponents. Thus, randomizing the system helps.; both are essential for safe communication. The HCRS consists of Eq. (3), shown below.[8, 21, 22]:

$$\begin{aligned} \dot{x} &= hy - ax + yz \\ \dot{y} &= hx - by - xz \\ \dot{z} &= -dz + xy + w^2 \\ \dot{w} &= xy + cw \end{aligned} \quad (3)$$

Fig. 1 shows the time series for each vector, with the form of the chaotic attractor limited by the system parameters.

Fig. 2 shows the irregular hyper-attractors of the studied chaotic system, which may be seen at a glance.

The Rabinovitch model indicates that despite different characteristics, one trajectory is closely connected. It is sensitive to the starting settings and parameters of the system. In Fig. 3, the state's time-domain waveform x(t) is shown, with the blue line representing starting conditions (x_0, y_0, z_0, w_0) equal to (1,2,3,4) and the red line indicating initial conditions (1, 2, $3+10^{-16}$, 4) correspondingly. Due to the changing initial circumstances, the system's activities are fundamentally different. Similar to how little changes to machine settings may completely alter a time series.[23], as shown in Fig. 3.

4 The proposed encryption and decryption system

The proposed system uses three hyperchaotic system generators of the Rabinovitch model, Then, the first system is used to generate a random sequence, the second is used to select a random index from the sequence first system, and the third is used to choose the pixel from the image. Then the pixel value is changed using the XOR operation by multiplying the index generated from system 1&3. Applying the first encryption system is done randomly instead of in the serial fashion (in other words, pixels number 1, then 2, then 3, etc.) typically used in traditional systems.

Algorithm 1: The proposed chaotic random number generators

Input: initial values X_0, Y_0, Z_0 & W_0, and Rabinovitch hyper Chaotic System parameters.

Output: Pseudo random sequence.
Initial values:
X_0, Y_0, Z_0, W_0: Initial values for Hyper Chaotic Rabinovitch System.
r, a, b, c, d: Parameters for Hyper Chaotic Rabinovitch System.
Generate a pseudo-random sequence*:*
Step 1: Set the initial values X_0, Y_0, Z_0 & W_0, and Rabinovitch hyper chaotic parameters (r, a, b, c, d).
Step 2: Create a chaotic sequence (X, Y, Z, and W) using the Rabinovitch system given in Eq. (1). This equation will generate a number with low randomness.
Step 3: To get high randomness, multiply the result from step 2 by a significant number such as (10^{12}), divide by a small number (255), and take the remainder number.
Generate a random index:

$$\text{RandVal} = \left(10^{12}.\text{Chaotic}_{\text{Sequence}}\right) \bmod 255 \quad (4)$$

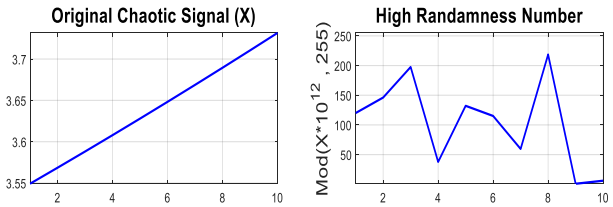
$$\text{CRNG} = \text{round}(\text{RandVal}) \quad (5)$$

Where CRNG represent the chaotic random number generator for the first hyperchaotic system.

Algorithm 2: The proposed scrambling algorithm is described in the following steps:

Input: Pseudo random sequence.
Output: Encrypted image.
Step 1: Sorted ascendingly the results from Eq. (4) RandVal that were generated from the 2nd and 3rd Hyperchaotic system. Concerning the third-step produced sequence.
Step 2: A new index is assigned to each element after step 4, which involves sorting the chaotic vector. The updated image permutation (encryption) scrambler index is shown here. In step 4, we have N=10 in our sequence. Thus, the new index representation is:

The proposed system algorithm can be explained in the following steps where the Rabinovitch system is used as:



(a) (b)

Figure. 4: (a) Generating chaotic signal (steps 1 & 2) and (b) High randomness numbers (step 3)

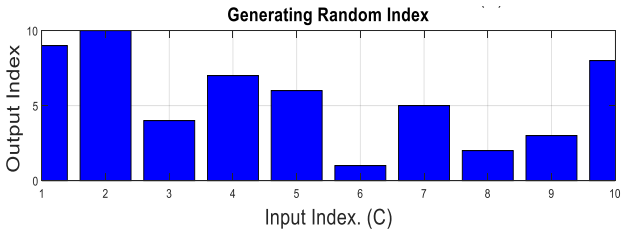


Figure. 5 Generate random location (steps 4 & 5)

Applying the proposed algorithms to encrypt the sub-image:

Step 1: Initialize the three Chaos functions by entering initial values and parameters.
Step 2: Enter the original image (m, n, d) and convert it from two dimensions (for the Gray image) or three dimensions (for the color image) into a single row image of pixels with dimensions (1, (n)(m)(d)). For example, the figure below is a sub-image (3, 4) converted to a single-row sub-image (1, 12) where the dimensions of a clear image are m, n, and d.
Step 3: From the **First chaos**, we generate pseudo-random integer values between (0 to 255) with the number of image vector elements.
Step 4: From the **Second Chaos**, generate an integer and semi-random value between 1 and the size of the single-row image. This value is a selector to choose the random value from the third step. (Such as select location 11)
Step 5: From the **Third Chaos**, generate a location (also confined between the one and the single row image length) to randomly and non-sequentially select pixels from the single row image based on step 2.
Step 6: Perform the XOR operation between the pixel that chose (from the fifth step) and the random value from the first chaotic generator (from step 3), which we randomly chose using the second chaotic generator (from step 4).
Step 7: Repeat the process from step 4 to step 6 (n*m*d) times. So that all pixels are encrypted, and we get a vector of encrypted pixels.
Step 8: After all the pixels have been encrypted, create an image with the exact dimensions as the original image by converting the vector of the encrypted pixels. **Note**: The first and second selectors cannot generate the location more than once.

5 System performance and security analysis

In this section, seven different statistical tests with three different image sizes will be implemented to analyses the security of the proposed cryptographic method and determine the overall performance of the

Table 1. MSE, PSNR, correlation, and entropy results for encryption and decryption images

Images	Entropy of Images	Encryption Results				Decryption Results			
		MSE	PSNR	Correlation	Entropy	MSE	PSNR	Correlation	Entropy
Cameraman	7.0097	9474.5	8.2968	-0.0006	7.9974	0	Inf	1	7.0097
Peppers	7.3785	11259	7.6156	0.0022	7.9997	0	Inf	1	7.3785
Babylon Unv.	7.7108	12025	7.33	-0.0038	7.9989	0	Inf	1	7.7108

entire system. Peak signal to noise ratio (PSNR), mean squared error (MSE), correlation, and entropy.

5.1 Lyapunov exponent

This test is based on calculating the natural algorithm of the divergence rate of two orbits in phase space for the same system but with a tiny difference in the initial conditions. In other words, it measures system sensitivity to the initial conditions. There are three general cases when calculating the Lyapunov exponent result where:

All Lyapunov exponents are smaller than zero, indicating that the system is not chaotic and that its orbit is being attracted to a fixed point.

All Lyapunov exponents are equal to zero. Stability is maintained with continual separation (not chaotic).

If at least one Lyapunov exponent is more significant than zero, the system behaves chaotically (positive).

The system exhibits hyperchaotic behavior if at least two Lyapunov exponents are more significant than zero (positive).

The Lyapunov exponent could be used to evaluate the system behavior for both continuous and discrete systems where, for the discrete system, it could be obtained from the following Eq. (6):

$$\lambda_i = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} log \frac{\sigma x_i(n+1)^n}{\sigma x_i(n)} \quad (6)$$

While the continuous system is calculated by Eq. (7):

$$\lambda_i = lim_{\sigma x_i(0)\to 0} lim_{t\to\infty} \frac{1}{t} log \frac{\sigma x_i(t)}{\sigma x_i(0)} \quad (7)$$

where $x_i(t)$ is the i^{th} state of the state vector, λ is the Lyapunov exponent of the system are $\lambda_1 = 6.8, \lambda_2 = 1.85, \lambda_3 = -2.912, and\ \lambda_4 = -12.3$ [24, 25]. There are two positive exponents for Rabinovitch System and two exponents less than zero. This makes the system hyper-chaos.

5.2 Mean squared error (MSE) and peak signal to noise ratio (PSNR)

To withstand differential and statistical assaults, every cryptography method seeks to maximize the difference between encrypted and unencrypted data. This study employs MSE and PSNR to discriminate between the original and encrypted pictures [26, 27]. Eqs. 8 and 9 provide a mathematical explanation of the MSE and PSNR, respectively:

$$MSE = \frac{\sum_{i,j}|I_1(i,j) - I_2(i,j)|}{m*n} \quad (8)$$

$$\mathrm{PSNR_{dB}} = 10 \log\left(\frac{255^2}{\mathrm{MSE}}\right) \quad (9)$$

5.3 Correlation coefficients

The correlation coefficient is used to obtain the similarity between the two images:

$$\mathrm{corr} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}((x_i - E(x)))^2}\sqrt{\sum_{i=1}^{N}((y_i - E(y)))^2}} \quad (10)$$

where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x(i)$, x and y are the pixel value of the original and the encrypted image, respectively. When lowered to 0, the images seem different (the original and the encrypted images). If the value is 1, the image's original details remain visible after encryption [25].

5.4 Entropy

Information entropy analysis measures randomness and encryption quality. The entropy of plain and cipher images could be compared to measure encryption quality. The image's entropy is calculated as follows:

$$\mathrm{E} = \sum_{i=0}^{2^n-1}\left[p(i) * \log_2\left(\frac{1}{p(i)}\right)\right] \quad (11)$$

where p(i) is the bit-valued I probability. For images with 256 Gray levels (0 to 255), the maximum entropy equals 8, and it has considered optimum randomness. Practical image entropy is lower than maximal entropy [28, 29]. See Table 1.

Table 1 shows the results of comparing the encrypted and recovered images in terms of all testing measurements.

The simulation results from Table 1, The encryption in the method proposed in this paper

Table 2. The simulation results for other research

References	Image	MSE	PSNR (dB)	Corr	Entropy
Ref. [7]	Peppers	10033	8.1624	0.00175	7.9968
Ref. [9]	Peppers	-	-	0.0035	7.9959
Ref. [8]	Cameraman	-	8.9311	0.5879	7.9973
	Peppers	-	8.6262	0.4917	7.9997
Ref. [10]	Peppers	-	-	0.0017	7.9976
Ref. [11]	Cameraman	9445	8.38	-	7.9991
	Peppers	8413	8.88	-	7.9994

Table 3. The decryption process if change any parameter or initial value

Image		Change Value	MSE	PSNR (dB)	Corr	Entropy
Cameraman	First HCRS	$a=a-10^{-15}$	6089.1	10.217	0.313	7.874
Peppers		$X=x-10^{-15}$	11264	7.613	0.0006	7.999
Babylon Univ.		$W=w+10^{-15}$	10140	8.070	0.165	7.988
Cameraman	Second HCRS	$Y=Y-10^{-15}$	9471.2	8.298	-0.0007	7.997
Peppers		$b=b-10^{-15}$	11255	7.617	0.001	7.999
Babylon Univ.		$d=d+10^{-15}$	11986	7.343	-0.001	7.998
Cameraman	Third HCRS	$a=a-10^{-14}$	9455.3	8.305	8.947	7.997
Peppers		$d=d-10^{-15}$	11244	7.621	0.002	7.999
Babylon Univ.		$c=c-10^{-15}$	11952	7.356	0.001	7.998

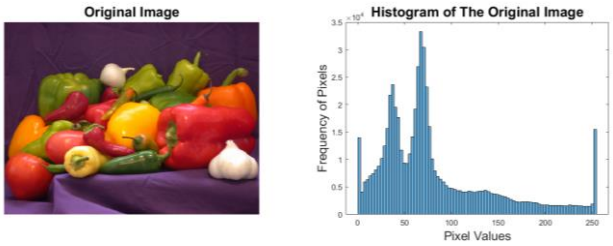


Figure. 6 Original image

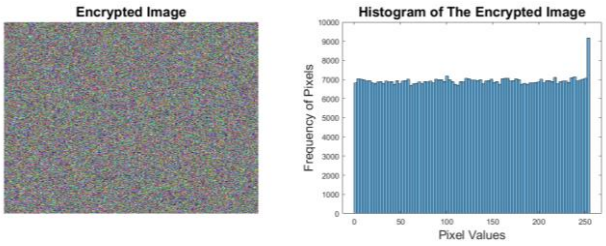


Figure. 7 Encrypted image

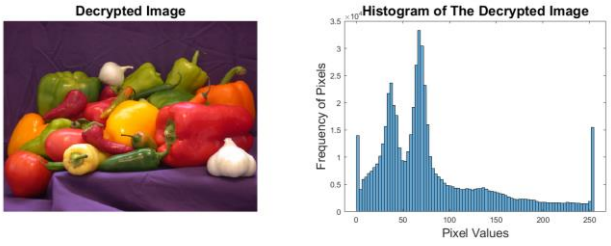


Figure. 8 Recovered image

showed that the testing measurements used to evaluate the encryption performance are complete (PNNR about 8 dB, Correlation near to 0, and entropy very close to 8).

The results based on images and histograms are shown in Figs. 6, 7, and 8.

From Fig. 6, the simulation results show that the histogram of the encrypted image is flat, indicating that nearly every possible pixel value occurred. A situation like this is unquestionably necessary regarding the security of the communication. In most statistical tests, the encryption of several pictures is acceptable.

5.5 Comparison of the proposed system with other research

Here, we will look at simulation results from the proposed system that uses modulo addition and multiplication to encrypt images. We will compare them to prior research that employed the XOR operation between the key and the original image to produce the encrypted image. As shown in Table 2.

Table 2, it is clear that the results of the proposed system (from Table 1 and from Fig. 6 to Fig. 8) are equal to or better than the results of previous studies.

5.6 Cryptoanalysis (Key Sensitivity and Space)

If there is even the slightest difference in the encryption and decryption keys, the encrypted signal will no longer be reliably decoded. Sensitivity is crucial for all safe cryptosystems. This means the Attacker cannot obtain any information by changing even a single element of the key—the starting state of X0, Y0, Z0, or W0—by a small amount, as shown in Table 3.

Table 3 shows that when we make a tiny change in the first & second hyper-chaos generators, the histogram of the decryption image will remain encrypted. In contrast, when we make a slight change

$$\begin{pmatrix} x_1, y_1, z_1, w_1, r_1, a_1, b_1, c_1, d_1, BigNum_1, ModNum_1 \\ x_2, y_2, z_2, w_2, r_2, a_2, b_2, c_2, d_2, BigNum_2, ModNum_2 \\ x_3, y_3, z_3, w_3, r_3, a_3, b_3, c_3, d_3, BigNum_3, ModNum_3 \end{pmatrix} All\ Keys = \prod_{1}^{3D} \frac{1}{10^{-15}} = \left(\frac{1}{10^{-15}}\right)^{3*11} = 10^{495} \quad (12)$$

Table 4. Comparison of key space in the proposed system with other studies

References	Key Space
Mazin H., et al. [14]	2^{1088}
Alsaabri HH., and et al. [8]	2^{956}
Hreshee SS., and et al.[12]	2^{266}
Abdullah HN., [13]	2^{319}
Hussein EA, [15]	2^{319}
Proposed System	2^{1644}

in the third hyper-chaos, the histogram of the decrypted image will be returned as before encryption, but the image will not be recovered and will remain encrypted. The reason for this is that the pixels of the image are recovered but not in their correct locations. The keyspace of the image encryption system employed in this paper is primarily determined by the five parameters [r, a, b, c, and d] and four initial conditions utilized to generate the chaotic sequence presented in this paper. (x_0 , y_0 , z_0, and w_0) and the two big and small numbers are used in the mod process. There are 11 coefficients used in only one system, while in the proposed system, we use three. There are 33 coefficients used in the proposed method. The key space of this article is at least:

$$All\ Keys = 2^{1644} \quad (13)$$

Validate the article's key space against the algorithms, as illustrated in Table 4.

6 Conclusions

In this paper, an efficient system for digital image encryption is proposed. Three Rabinovitch chaos sequences are used in this system. The first system generates a random integer number sequence between (0 - 255), the second selects a random index from the sequence first system, and the third is used for chaotic pixel selection from the image. Then changing the pixel value using the XOR operation to encrypt the pixels. The simulation results give good results regarding encryption and obtained massive key space of about 2^{1644}.

Acknowledgment

We want to express our sincere gratitude to the University of Babylon, College of Science for Women, Department of Computer Science, for supporting this research paper.

References

[1] M. J. M. Ameen and S. S. Hreshee, "Securing Physical Layer of 5G Wireless Network System over GFDM Using Linear Precoding Algorithm for Massive MIMO and Hyperchaotic QR-Decomposition", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 5, pp. 579-591, 2022, doi: 10.22266/ijies2022.1031.50.

[2] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding", *Expert Syst. Appl.*, Vol. 213, p. 118845, 2023, doi: 10.1016/j.eswa.2022.118845.

[3] Y. Zhang, A. Chen, Y. Tang, J. Dang, and G. Wang, "Plaintext-related image encryption algorithm based on perceptron-like network", *Inf. Sci. (Ny).*, Vol. 526, pp. 180–202, 2020.

[4] R. Wang, G. Q. Deng, and X. F. Duan, "An image encryption scheme based on double chaotic cyclic shift and Josephus problem", *J. Inf. Secur. Appl.*, Vol. 58, p. 102699, 2021.

[5] R. G. Zhou and Y. B. Li, "Quantum image encryption based on Lorenz hyper-chaotic system", *Int. J. Quantum Inf.*, Vol. 18, No. 05, p. 2050022, 2020.

[6] Y. Shi, R. Chen, D. Liu, and B. Wang, "A visually secure image encryption scheme based on adaptive block compressed sensing and non-negative matrix factorization", *Opt. Laser Technol.*, Vol. 163, p. 109345, 2023.

[7] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color Image Encryption Through Chaos and KAA Map", *IEEE Access*, Vol. 11, pp. 11541–11554, 2023.

[8] H. H. Alsaabri and S. S. Hreshee, "Robust Image Encryption Based on Double Hyper Chaotic Rabinovich System", In: *Proc. of 7th Int. Conf. Contemp. Inf. Technol. Math. ICCITM 2021*, pp. 146–152, 2021, doi: 10.1109/ICCITM53167.2021.9677722.

[9] X. Wang and Y. Su, "Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform", *Sci. Rep.*, Vol. 10, No. 1, pp. 1–19, 2020.

[10] M. Long and L. Tan, "A chaos-based data

encryption algorithm for image/video", In: *Proc. of 2010 Second International Conference on Multimedia and Information Technology*, Vol. 1, pp. 172–175, 2010.

[11] I. Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A chaotic-based encryption/decryption framework for secure multimedia communications", *Entropy*, Vol. 22, No. 11, p. 1253, 2020.

[12] S. S. Hreshee, H. N. Abdullah, and A. K. Jawad, "A High Security Communication System Based on Chaotic Scrambling and Chaotic Masking", *Int. J. Commun. Antenna Propag.*, Vol. 8, No. 3, p. 257, 2018, doi: 10.15866/irecap.v8i3.13541.

[13] X.-H. Song, H.-Q. Wang, S. E. Venegas-Andraca, and A. A. Abd El-Latif, "Quantum video encryption based on qubit-planes controlled-XOR operations and improved logistic map", *Phys. A Stat. Mech. its Appl.*, Vol. 537, p. 122660, 2020, doi: 10.1016/j.physa.2019.122660.

[14] H. Mazin, M. Alibraheemi, Q. Al-gayem, and E. A. Hussein, "Design and FPGA Implementation of High-Speed Cryptographic System for Wireless Communications Based on Multi-Dimensional Hyperchaotic Generator", *Neuro Quantology*, Vol. 20, No. 7, pp. 559–573, 2022, doi: 10.14704/nq.2022.20.7.NQ33073.

[15] E. A. R. Hussein, M. K. Khashan, and A. K. Jawad, "A high security and noise immunity of speech based on double chaotic masking", *Int. J. Electr. Comput. Eng.*, Vol. 10, No. 4, pp. 4270-4278, 2020, doi: 10.11591/ijece.v10i4.

[16] L. Ren, M. H. Lin, A. Abdulwahab, J. Ma, and H. S. Nik, "Global dynamical analysis of the integer and fractional 4D hyperchaotic Rabinovich system", *Chaos, Solitons & Fractals*, Vol. 169, p. 113275, Apr. 2023, doi: 10.1016/j.chaos.2023.113275.

[17] Y. B. Huang, S. H. Wang, Y. Wang, and H. Li, "A New Four-Dimensional Chaotic System and Its Application in Speech Encryption", In: *Proc. of 2020 Information Communication Technologies Conference (ICTC)*, May 2020, pp. 171–175. doi: 10.1109/ICTC49638.2020.9123294.

[18] F. Min and L. Xue, "Routes toward chaos in a memristor-based Shinriki circuit", *Chaos An Interdiscip. J. Nonlinear Sci.*, Vol. 33, No. 2, p. 023122, Feb. 2023, doi: 10.1063/5.0126900.

[19] D. Xu, G. Li, W. Xu, and C. Wei, "Design of artificial intelligence image encryption algorithm based on hyperchaos", *Ain Shams Eng. J.*, Vol. 14, No. 3, p. 101891, Apr. 2023, doi: 10.1016/j.asej.2022.101891.

[20] Y. Yang, M. Cheng, Y. Ding, and W. Zhang, "A Visually Meaningful Image Encryption Scheme Based on Lossless Compression SPIHT Coding", *IEEE Trans. Serv. Comput.*, pp. 1–15, 2023, doi: 10.1109/TSC.2023.3258144.

[21] R. D. Ene, N. Pop, and M. Lapadat, "Approximate Closed-Form Solutions for the Rabinovich System via the Optimal Auxiliary Functions Method", *Symmetry (Basel).*, Vol. 14, No. 10, p. 2185, 2022, doi: 10.3390/sym14102185.

[22] S. Kuznetsov and L. Turukina, "Generalized Rabinovich–Fabrikant system: equations and its dynamics", *Izv. VUZ. Appl. Nonlinear Dyn.*, Vol. 30, No. 1, pp. 7–29, Jan. 2022, doi: 10.18500/0869-6632-2022-30-1-7-29.

[23] R. K. Ghaziani, Z. Eskandari, and M. Gholami, "Three-dimensional fractional system with the stability condition and chaos control", *Math. Model. Numer. Simul. with Appl.*, Vol. 2, No. 1, pp. 41–47, Feb. 2022, doi: 10.53391/mmnsa.2022.01.004.

[24] J. B. Dingwell, *Lyapunov Exponents*, Wiley Encyclopedia of Biomedical Engineering, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2006. doi: 10.1002/9780471740360.ebs0702.

[25] N. N. Gbo and J. Tang, "On the Bounds of Lyapunov Exponents for Fractional Differential Systems with an Exponential Kernel", *Int. J. Bifurc. Chaos*, Vol. 32, No. 12, 2022, doi: 10.1142/S0218127422501887.

[26] S. Halagowda, S. K. Lakshminarayana, and S. Lakshminarayana, "Image encryption method based on hybrid fractal-chaos algorithm", *Int. J. Intell. Eng. Syst.*, Vol. 10, No. 6, pp. 221–229, 2017.

[27] A. J. Parsaoran, S. Mandala, and M. Pramudyo, "Study of Denoising Algorithms on Photoplethysmograph (PPG) Signals", In: *Proc. of 2022 International Conference on Data Science and Its Applications (ICoDSA)*, Jul. 2022, pp. 289–293. doi: 10.1109/ICoDSA55874.2022.9862918.

[28] H. A. H. A. Delfi and F. S. Hasan, "Hybrid Ciphering and Frequency Domain Scrambling for Secure Speech Transmission through MIMO-OFDM System", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 6, 2022, doi: 10.22266/ijies2022.1231.50.

[29] U. Sara, M. Akter, and M. S. Uddin, "Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study", *J. Comput. Commun.*, Vol. 7, No. 3, pp. 8–18, 2019.