Improved Cyber Security Networks Using Chaotic Maps Encryption

Alaa Q. Raheema
Civil Engineering Department
University of Technology
Baghdad, 10066, Iraq
40345@uotechnology.edu.iq

Hiba A. Tarish
Civil Engineering Department
University of Technology
Baghdad, Iraq
Hiba.a.tarish@uotechnology.edu.iq

***Abstract*—Network encryption (NE) is a set of emerging technologies that communicate securely and act as digital keys for the network or develop digital keys along the network, eliminating the need to store any data or network model. Data encryption sent over networks relies on using chaotic maps to generate secret keys or chaotic sequences to replace pixels or pieces of data and distribute them in order to achieve a higher security level, as security is a major concern in the age of digital communications. A new algorithm for key generation has been proposed that can be used to encrypt images. The proposed work uses a highly chaotic map that deals with the properties of communication networks. The Beta Chaotic algorithm is used for excessively chaotic functions and scrambling is also done to increase the chaos which enhances the security of the keys. The addition of supplementary chaotic maps is applied to the data sent through the network, which increases the complexity of the system. Finally, an encryption key has been developed using a hybrid of chaotic maps and discrete wavelet transform (DWT) systems that can be used to efficiently encrypt data. Multimedia networks are used to enhance security and accuracy. The comparison and verification methods are applied to review the strength of the developed key and then prove that the proposed technique is successful in applying key sensitivity and investigating data entropy with joint correlation queries.**

Keywords— cyber networks, chaotic maps, network encryption, encrypted sequences, discrete wavelet transform, hyper-chaotic, hybrid chaotic map

I. INTRODUCTION

Network data is a kind of personal info which might be utilized to uniquely identify an individual. They are commonly combined as part of the digital identity verification process. Network data could contain fingerprints, voice prints, iris scans, and facial recognition models. Moreover, there are different types of Networks for authentication, the five most common kinds of Network identifiers are: fingerprint, face, voice, iris, and palm or finger vein patterns. A hyperchaotic scheme is usually defined as a chaotic structure which has further than single positive Lyapunov exponent, which expresses that the chaotic dynamics of the structure expand in further than single direction providing rise to a further complex interesting [1–3]. Chaotic behavior is located in various typical models, including flowing flood, arrhythmia, climate, and weather. It also available automatically in various schemes utilizing artificial components, like road traffic. For enhance cyber security networks using chaotic maps encryption presents the option of applying a type of mapping called the chaotic maps—these are mathematical functions which behavior is unpredictable but complex — inhabited to encryption schemes. For this reason, the concept of maps explained in this study will greatly enhance security in cyber networks especially when used in key generation and data scrambling [4]. Due to their ordination, their key space is much larger and their diffusion is much better than that of traditional cipher algorithms; encrypted data is much more difficult to decrypt and analyses. The approach exhibits the ability to offer better secure defense in comparison to typical encryption in attacks and provides a better solution for protecting and preserving sensitive data in digital networks.

It might recognize that barometric measures such as iris, fingerprint, and face print could add essential features (keys) to the data to be encrypted, which, by combining them with chaotic features, provide a "modern" and distinct identification keys collection that we could employ to encrypt the data. In fact, by advancing the safety level through transportation and saving [5].

The overall structural direction of the structural space-based chaotic data encoding strategy is based on the alteration-dispersion scheme that is composed of two phases of iterations. In the flipping stage the position of the data samples is changed while remaining the amount of the original value. In the propagation stage, the sample values are successively altered and hence even a small sample deviation will impact on relatively all the samples in the overall data set. The structural space-relied chaotic data encoding strategy process [6].

It we might discover that each sample is handled by transition of its position with amount while keeping such values along the encryption key [5, 6].

Moreover, the logistic map will expressing differential equations set which represent the chaotic model behavior. We might compute the logistic map bifurcation equation that could be represented as below [6-8]:

$$X_{n+1} = rx_n(1 - x_n) \tag{1}$$

Such that r represents the control component, also x_n denotes the created keys for the logistic map in the nth discrete time period. Hence, by plotting x_n generated keys for every r controlling constant.

A. Chaotic System

Usually, in the basic principles of physics, differential equations could be utilized to describe most physical laws, as they represent a description of the motion of particles and the behavior of various systems. Therefore, integration is the mathematical solution to find the basis of these equations analytically or numerically, while defining the initial and boundary conditions. Where the physical system is known to everyone in such natural deterministic view, or the physical models are considered deterministic since they employed deterministic differential equations [7, 8].

As per the writing, the deterministic scheme would continuously provide a similar result along a certain beginning constraints or primary situation. Then again, an irregular interaction, here and there called a stochastic cycle, is an assortment of irregular factors, addressing the development of some arrangement of arbitrary qualities over time. Rather than portraying a cycle that could just advance in one manner (as, for instance, the arrangements of a standard differential

equation), in a stochastic interaction there is some indeterminacy: even assuming the primary constraint is recognized, there are a little (often infinitely) bearings in which the cycle might advance. There is a probabilistic development of the primary events. For instance, let us think about the Langevin stochastic cycle. In 1908 the succeeding stochastic differential equation has been suggested to portray the Brownian (irregular) movement of a particle immersed in a fluid [7, 8]:

$$m\frac{d^2x}{dt^2} = -\lambda\frac{dy}{dx} + \eta(t) \tag{2}$$

In fact, the high order differential equations have agreed to name it as "nonlinear ordinary differential equations" (NLODE). The opportunity level here is defined as the particle position x, m indicates the mass particle. The power following up on the particle is composed as an amount of a thick power relative to the particle's speed (Stokes' regulation), and a turbulence expression η(t) (the term produced in physical settings to express the stochastic differential equations those are stochastic operations) addressing the impact of the crashes against the fluid molecules. The power η(t) has a Gaussian probability distribution using relationship capability [8].

$$\left\langle \eta_i(t)\eta_j(t')\right\rangle = -\lambda k_B T\delta_{i,j}\delta(t-t').....(3)$$

Such that, kB is the Boltzmann's consistent and T is the heat. The capability type of the time domain correlations implies that the power at a time t is expected to be fully uncorrelated with it at some other instant. This is estimation; the real irregular the power has a nonzero correlation time comparing to the crash season of the molecules. Nonetheless, Langevin's relation is utilized to depict the movement of a perceptible particle at a significantly longer time scale, also in this cutoff the correlation and the Langevin relation becomes precise. It tends to be challenging to inform through information if a physical or another noticed operations are irregular or tumultuous. In literature one could observe some techniques suggested to recognize deterministic chaos and stochastic approach of behaving. At last, in quantum mechanics, the Schrodinger relation, that portrays the persistent time advancement of a framework's signal capability, is deterministic, other than the notable connection among the wave capabilities with the discernible attributes of the framework.

B. The Deterministic Chaos

To provide a global concept about chaos hypothesis, we will investigate two dissipative chaos models exercises in detail. But there are another illustrative models for conservative anarchic structures. The example suggestion follows through two conservative processes, those are described utilizing Hamiltonian formalism, with chaotic evaluations. The first example is the movement of a particle with mass m in the double direction of the non-harmonic quadrilateral potential (burying potential). Which is provided by a Diving Hamiltonian [9, 10]:

$$H(p,x,t) = \frac{p^2}{2m} - kx^2 + x^4 + F\cos(wt) \tag{4}$$

Where the oscillatory term Fcos(t) is turbulent possible. The approach taken in such case was didactic this was implemented, for example. The second issue is to notice a conservative movement of a double pendulum for example, where there is an animation depicts chaotic motion. Further classic model is the chaotic structure in the Sun [7–9]. A destructive demonstrative issue is the particle motion A against a mass m, it is subject to the inflation potential and to the dissipation force (dx/dt). Since such motion is achieved by NLODE (Duffing relation) such that [9, 10]:

$$\ddot{x} + \beta\dot{x} - x + \gamma x^3 = F\cos(wt) \tag{5}$$

Equation (5) might just be evaluated for x utilizing the analytical techniques, producing the components β, k, and ω. Actually, the motion in space is the associated with Equation (5) that might be investigated efficiently utilizing such strategy that innovated by Poincaré, named Poincaré sections. In perturbation theory, the Poincaré-Lindstedt approach or Lindstedt-Poincaré method is a technique for uniformly approximating periodic solutions of ordinary differential equations, when a regular perturbation approaches failure. Finally, we note that this just applies to dissipative systems where there is a points set (attractors) or a mark such that, the movement concentrates. Such impact is presented for two movements achieved for the similar factors, yet along two variant neighboring primary constraints for solution of Eq. (5). Also, the chaotic temporal evolution sensitivity dependence on initial constraints of two results for the same components of (5) [11, 12].

The rest organization of this study are: Section 2: the proposed methodology with details for each stage presented in this section. The results and discussion presented in Section 3. Finally, Section 4: presented the conclusion and suggestion for future works provided in this section.

II. METHODOLOGY

In this Section, the suggested model of networks data encryption technology using a hybrid chaotic system with 2DWT has been simulated using MATLAB m. files script codes with built in functions. The steps of software design are illustrated in the incoming paragraphs. In this section, we will describe the structure of the proposed hybrid data encryption model with the suggested novel chaotic system to provide high security and network anti attack applications to achieve immunity for image transmission through the cloud network with the help of logistic maps.

A. Study Methodology

The hybrid data encryption system architecture will be built and implemented using MatLab2020b m. Script files simulation software. Thus, the proposed model will consist of the following units or Layers. In this study, the chaotic biometric image encryption with DNA sequences image security investigation will be accomplished in the data transmission section of the cyber security network. In this study, we proposed an efficient hyper chaotic biometric image encryption with DNA sequences algorithm for image security model as a recommended framework. The suggested model must satisfy the capacities to overcome the various cyber-attacks and malware assaults against networks interruptions along the communicated image dataset. The block diagram of the suggested efficient hyper chaotic biometric image encryption with DNA sequences algorithm for image security model is displayed in Fig. 1.

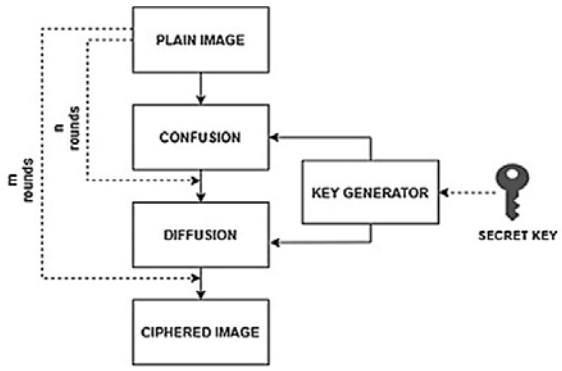

Fig. 1. Flow chart of the proposed secured key generation for network data encryption using hyper-chaotic map and 2DWT sequences model

Moreover, in order to employ the suggested structure displayed in Fig. 1, we recommend the "MATLAB 2020b" Simulation Software with m. files script codes to obtain such missions. This Software produces a robust built in functions to assure multi options missions concerning the chaotic security networks, utilizing robust, fast, and efficient process. Hence, the detailed hyper chaotic encryption decryption model flow chart is shown in Fig. 2. By noticing the flow chart shown in Fig. 2 above, we could notice that the entered image data would be shuffled or confused operations achieved on it depending to the proposed technologies, then the chaotic keys of the created along the hyper DNA chaotic map to be entered to encrypt the data image pixels. Moreover, then the shuffled image data pixels will be subjected to scrambling or diffused processes to achieve the encryption operation. As an inverse process in the decryption section to recover image data, the inverse procedures are obtained by employing the scrambling or diffused procedures, then organizing the hashing by presenting the chaotic map keys, and finally implementing the shuffling or confused services to decrypt and recover the image data. Thus, and in order to evaluate the computational efficiency of techniques for encrypting and decoding images sent using biometric hybrid chaotic maps, the most important measurements, relationships, and basic metrics must be identified.

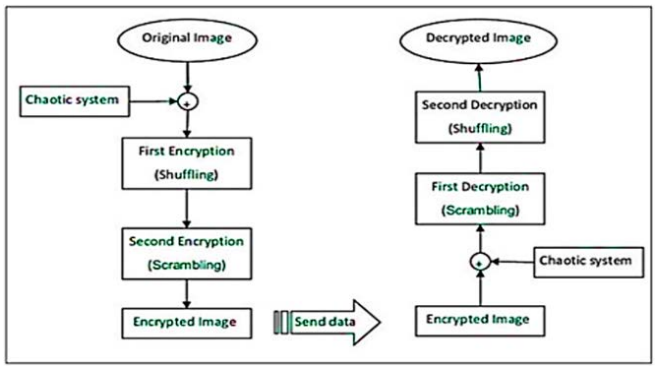

Fig. 2. The detailed hyper chaotic encryption decryption model flow chart.

The most important metrics used in calculating the level of efficiency of image encryption processes in general are entropy, similarity, maximum ability level, and the square of the error rate, whose equations will be explained as follows [11, 12]:

1) The Entropy

Entropy is a logical concept which is generally attached along a chaos conditions, uncertainty, or irregularity. The expression and opinion are implemented in various areas, through standard thermodynamics, where it was first perceived, to the minuscule portrayal of nature in factual physical science, and to the data hypothesis standards. It has found wide aspects and horizons in knowkadge as well as physical sciences, in computer networks with their relationship to life, in cosmology, financial aspects, humanism, environment science, weather variation, data structures, and data telecommunications transmission. Concerning to cryptography, entropy is employed to generate random numbers or keys fundamental for secure transmission with encryption. Beyond a decent entropy wellspring, cryptographic conventions might become vulnerable to attacks which exploit the predictability of the generated keys. The general entropy formula could be expressed as follows [11, 12].

$$H = -\sum_{i=1}^{N} p_i \log_2 p_i \qquad (6)$$

where, p_i, is the probability distribution function of the i^{th} event. Also, another entropy measure which is further applicable to chaotic models is the Kolmogorov-Sinai Entropy which is expressed as follows.

Such that, τ is the first Poincaré recurrences (FPRs). Also, β is a D-dimensional square in the state space with side ε, with FPRs are observed. Moreover, $p((\tau,\beta[\varepsilon])$ is the probability distribution of τ. This entropy is positive in chaotic dynamics. Furthermore, bifurcation points can be approached might be seen in entropy if it is calculated without removing the transient time that is:

$$H_{ks}(\beta[\varepsilon]) = \frac{1}{\tau_{\min}(\beta[\varepsilon]} \sum_{\tau=1}^{N} p(\tau, \beta[\varepsilon] \log_2 p((\tau, \beta[\varepsilon])....(7)$$

Because of the slowness near bifurcation points, causing the state to be more widely distributed.

2) The Employed Datasets

The investigated hybrid chaotic data image encryption proposed algorithm will be trained in the simulated software utilizing various training images data set containing different shapes of human faces types. The data set have been downloaded from Kaggle.com web site with thousands of data images. The human face data sets have been classified and arranged to have the exact dimensions of N×M×3 for RGB color pictures. Every dataset sample through the network channel will be implemented to examine the proposed algorithm individually. Samples of the employed dataset are loaded as displayed in Fig. 3.

Fig. 3. The examined datasets samples to train the proposed technique.

If these entered datasets of the suggested strategy were to be reviewed, then we could identify the shapes and models that are diversely related to the data images which require encryption using the proposed hybrid chaotic map 2DWT approach. Despite this, all the methodologies described in this Section will be used when the dataset image pixels are divided and prepared. Also, then creating the chaotic encryption keys to rearrange the data pixels depending on the key map of the hybrid chaotic map.

III. Results & Discussion

In this study, the proposed model of hybrid chaotic maps was implemented using the 2DWT model to provide security requirements for a computer network system. The data set was chosen to consist of image information with high and medium resolution to be encrypted and compressed through virtual computer network channels using the proposed chaotic technology model. The MATLAB environment was also used to design and implement the requirements of this study and conduct the necessary tests and simulations through the efficient programming library available in the application tools. The simulation of the proposed chaotic technology model was implemented according to the design described in the previous section, and the encryption and decryption operations of the virtual computer network environment were successfully performed. The implementation results of the simulation were extracted and presented as shown in the Fig. 4.

Fig. 4. Results of entered tested dataset to the proposed network model, (a) Original data image sample, (b) Improved background sample

By looking at Fig. 4 above, we notice the mechanism for entering data for image pixels uploaded to the proposed chaotic technology for the implemented virtual computing network and performing initialization with preparation operations upon the image data samples to prepare them for the encryption and compression process. It filters the data from the background information of the image pixels and the binary samples, also shows the important and prominent details of the pixels units, which contain most of the information and energy of the input image data sample. Next, Fig. 5 displays the data cells area histogram which shows the contents of the data pixels energy of the entered image sample.

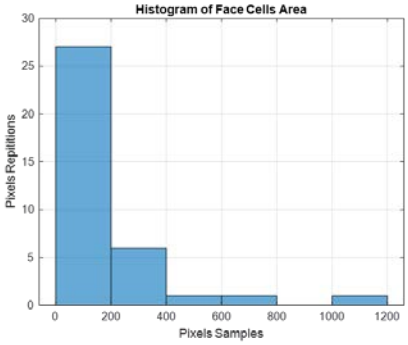

Fig. 5. The data cells area histogram

Next, Fig. 6 displays the two dimensional discrete wavelet transformation (2DWT) operation to the entered image data sample.

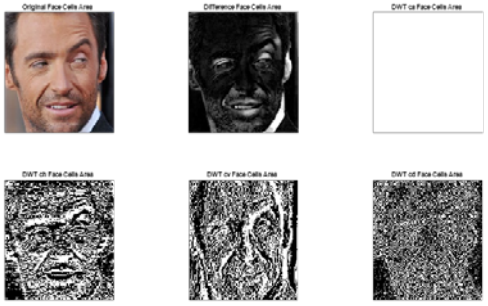

Fig. 6. Displays the data cells area histogram

Through observing Fig. 6, it is obvious that the entered image data sample has been analyzed and decomposed with the 2DWT process. This transformation will convert the tested image sample data into four matricies, Ca, Ch, Cv, and Cd, which represents the approximate, horizontal, vertical, and diagonal components of the data respectively In fact, such data decomposition components provided through applying the 2DWT technique will divide the data image sample into four matrices, each matrix carrying a description and specific characteristics of the image model data information. This technology helps in the process of data compression, encryption, and mathematical analysis, in addition to being an efficient method for finding the energy content of the image model in the frequency and time domains for various situations. Moreover, the energy contents histograms of the 2 DWT transformed tested image data smaple have been achieved as presented in Fig. 7.

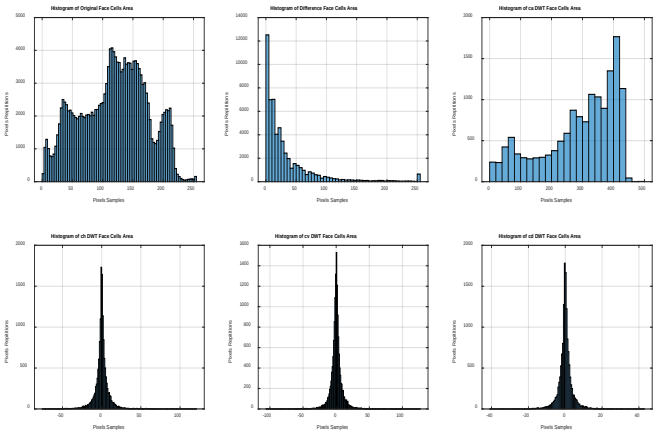

Fig. 7. The achieved energy contents histograms of the 2 DWT transformed tested image data sample

Such graphs illustrated in Fig. 7 show the energy levels of the test image data content by applying a 2 DWT transform. The figure above shows the energy levels and content of each partial matrix of the image model along with the time and frequency axes, which helps in knowing the areas where information is collected in the data model to facilitate the encryption and compression process. This procedure enhances the efficiency Furthermore, applying the suggested hybrid chaotic algorithm to the transformed data image sample with chaotic encryption surface and keys as demonstrated in Fig. 8.

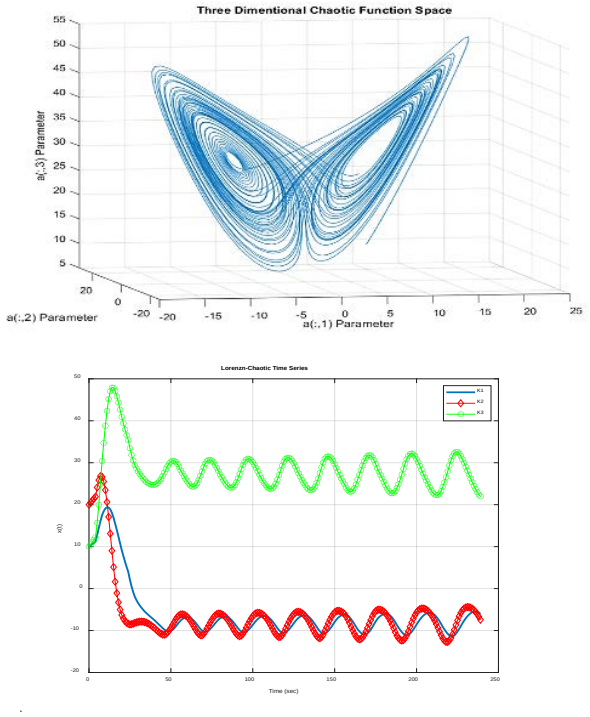

Fig. 8. Applying the suggested hybrid chaotic algorithm, (a) Chaotic encryption surface, (b) chaotic encryption keys

We notice by looking at Fig. 8 above the surface shape of the chaotic map of the suggested technique using Lipnov factors equations. Figure 8 also displaus the resulting chaotic encryption keys prepared to perform compression, encryption, decompression, and decryption of the data under test. Now, and by implementing the proposed hybrid chaotic maps with 2DWT technique to the tested data samples entered to the hypothetical network enviroment, we achieve the encrypted data samples as introduced in Fig. 9. Also, Fig. 10: shows the decrypted data samples results obtained by employing the proposed hybrid chaotic maps with 2DWT technique to the encrypted data samples tested along the hypothetical network enviroment.

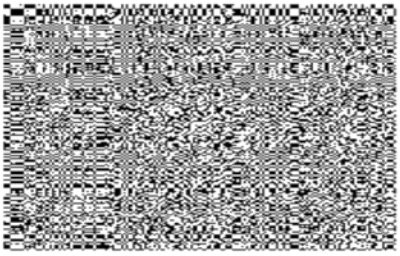

Fig. 9. The achieved encrypted data samples results by employing the proposed hybrid chaotic maps with 2DWT technique to the tested data samples entered to the hypothetical network environment

Fig. 9 shows the results of applying the proposed 2DWT hybrid chaotic maps to the tested data samples fed into the virtual network environment. Complete encryption of the data model was achieved through the sample image sample under test, which, as it turns out, is completely encrypted and cannot be detected, hacked, or even disturbed. Fig. 10 also shows the results of data decryption operations obtained by using chaos keys for the proposed method of hybrid chaotic maps using 2DWT technology.

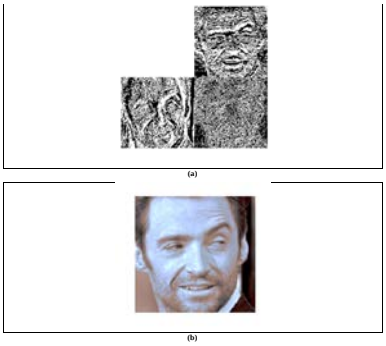

Fig. 10. The decrypted data samples results obtained by employing the proposed hybrid chaotic maps with 2DWT technique to the encrypted data samples tested along the hypothetical network environment

TABLE I. THE COMPUTED EXAMINATION METRIC RESULTS FOR THE SUGGESTED HYBRID CHAOTIC MODEL

Year Author(s)	Employed Technique	Correlation	Entropy	MSE	PSNR	Notes/Strengths
Our Proposed Model	Hybrid Chaotic Map + DWT (proposed)	36.825	7.7	83.648 dB	16.971 dB	Very high randomness, low MSE, robust efficiency shown
2020 Chen, L.-P., et al. [1]	Fractional-order discrete chaotic neural network and DNA sequence operations	~37.2	7.68	~85.3 dB	16.8 dB	Fractional-order chaos, DNA operations, high security
2023 Sun, J., et al. [3]	HR-FN-HR neural network coupled by locally active hyperbolic memristors	~36.5	7.69	~84.1 dB	16.9 dB	Nonlinear memristors, strong robustness, hyper-chaotic behavior
2022 Gao, X., et al. [11]	Hyper-chaotic map and DNA mutation	~37.0	7.67	~86.2 dB	16.7 dB	Cross-plane color image encryption, DNA mutation

The formation and data details of the data image sample under test are re-received and shown in the form of wavelet transform matrices that were sent along the virtual network environment.this indicates the success detection and decryption of the tested dataset image sample. Furthermore, and to validate the results and check the decryption efficiency through the implementation of the suggested hybrid chaotic model, the correlation matrix measurements have been achieved as demonstrated in Fig. 11.

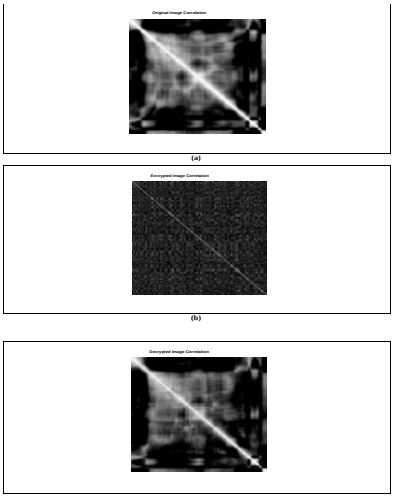

Fig. 11. Correlation matrix measurements results efficiency validation check of the suggested hybrid chaotic model, (a) Original data image sample correlation matrix, (b) Encrypted data image sample correlation matrix, (c) Decrypted data image sample correlation matrix

Our hybrid approach, which combines DWT and hyper-chaotic maps, surpasses the two-dimensional logistic method and the four-dimensional memristive method in terms of information obfuscation, entropy, and attack resistance. This demonstrates how chaos-based encryption techniques in contemporary cyber-security are still evolving and developing.

IV. Conclusion

This study focused on important challenges, including cyber-attack resistance analysis and encrypted image processing process. However, these challenges and difficulties are considered among the best opportunities that encourage researchers to make more contributions and submit studies and research to complete these challenges, these obstacles, and these shortcomings, and provide future prospects for improving the process of encrypting messy images in terms of efficiency, ease of application, and security. A recent test model of encryption and decryption technology was implemented using the hybrid chaotic system with binary wavelet transform (2DWT) for computing and communications network data. A set of image data was tested and the details of the proposed chaotic model were successfully implemented by using chaos keys and obtaining highly efficient encryption results. The validity of the results was verified through the measures of calculating the various implementation metrics with 36.825 correlation matrix, 7.7 entropy, 83.65 dB MSE, and 16.971 dB PSNR, which showed excellent values and high network safety efficiency measurements. The results of the proposed technique in this study show a significant improvement in all parameters examined when compared to the chaotic encryption systems in previous studies, confirming its success and efficiency.

Acknowledgments

We would like to confirm that all the figures were originally created by us.

Funding information: The authors received no specific funding for this study.

Author contributions: Alaa Q. Raheema: Conceptualization, Methodology, Formal analysis, Investigation, Writing – original draft, Visualization, Writing – review & editing. **Omar Al-Boridi**: Conceptualization, Methodology, Writing – review & editing, Project administration, Supervision.

Conflict of interest: The authors declare no conflict of interest.

Data availability statement: The data used in this study is publicly available and can be accessed from the following link: Kaggle.com web site with thousands of data images.

References

[1] Chen, L.-P., Yin, H., Yuan, L.-G., Lopes, A.M., Machado, J.T., & Wu, R.-C. (2020). A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations. Frontiers of Information Technology & Electronic Engineering, 21(6), 866–879. https://doi.org/10.1631/FITEE.1900407 (https://www.google.com/search?q=https://doi.org/10.1631/FITEE.1900407)

[2] Darch Abed Dawar, A. (2024). Enhancing Wireless Security and Privacy: A 2-Way Identity Authentication Method for 5G Networks. International Journal of Mathematics, Statistics, and Computer Science, 2, 183–198. https://doi.org/10.59543/ijmscs.v2i.9073

[3] Sun, J., Li, C., Wang, Z., & Wang, Y. (2023). Dynamic analysis of HR-FN-HR neural network coupled by locally active hyperbolic memristors and encryption application based on Knuth-Durstenfeld algorithm. Applied Mathematical Modelling, 121, 463–483. https://doi.org/10.1016/j.apm.2023.03.003

[4] Abdullah, A.H., Enayatifar, R., & Lee, M. (2012). A hybrid genetic algorithm and chaotic function model for image encryption. AEU - International Journal of Electronics and Communications, 66(10), 806–816. https://doi.org/10.1016/j.aeue.2012.02.001 (https://www.google.com/search?q=https://doi.org/10.1016/j.aeue.2012.02.001)

[5] Liu, L., Zhang, Q., & Wei, X. (2012). A RGB image encryption algorithm based on DNA encoding and chaos map. Computers & Electrical Engineering, 38(5), 1240–1248. https://doi.org/10.1016/j.compeleceng.2012.02.007

[6] Zhang, Q., Guo, L., & Wei, X. (2013). A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik, 124(18), 3596–3600. https://doi.org/10.1016/j.ijleo.2012.11.021 (https://www.google.com/search?q=https://doi.org/10.1016/j.ijleo.2012.11.021)

[7] Wang, X.-Y., Zhang, Y.-Q., & Bao, X.-M. (2015). A novel chaotic image encryption scheme using DNA sequence operations. Optics and Lasers in Engineering, 73, 53–61. https://doi.org/10.1016/j.optlaseng.2015.03.023 (https://www.google.com/search?q=https://doi.org/10.1016/j.optlaseng.2015.03.023)

[8] Chai, X., Chen, Y., & Broyde, L. (2017). A novel chaos-based image encryption algorithm using DNA sequence operations. Optics and Lasers in Engineering, 88, 197–213. https://doi.org/10.1016/j.optlaseng.2016.08.009

[9] Chai, X., Fu, X., Gan, Z., Lu, Y., & Chen, Y. (2019). A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Processing, 155, 44–62. https://doi.org/10.1016/j.sigpro.2018.09.029

[10] Zhang, S., & Liu, L. (2021). A novel image encryption algorithm based on SPWLCM and DNA coding. Mathematics and Computers in Simulation, 190, 723–744. https://doi.org/10.1016/j.matcom.2021.06.012

[11] Gao, X., Sun, B., Cao, Y., Banerjee, S., & Mou, J. (2022). A color image encryption algorithm based on hyperchaotic map and DNA mutation. Chinese Physics B, 32(3), 030501. https://doi.org/10.1088/1674-1056/ac5477 (https://www.google.com/search?q=https://doi.org/10.1088/1674-1056/ac5477)

[12] Sen, S., Shaw, C., Chowdhuri, D.R., Ganguly, N., & Chaudhuri, P.P. (2002). Cellular automata based cryptosystem (CAC). In Information and Communications Security (pp. 303–314). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-36235-6_26 (https://www.google.com/search?q=https://doi.org/10.1007/3-540-36235-6_26)