Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 34, Issue 4, 2023 DOI: https://doi.org/10.23851/mjs.v34i4.1411

Research Article Open Access

Enhancing Color Image Security: Encryption with Dynamic Chaotic Three-Dimensional System and Robust Security Analysis

Zainab Hasan Thabit[1], Sadiq A. Mehdi[2], Bashar M. Nema[1]*

[1]Department of Computer Science, College of Science, Mustansiriyah University, 10052 Baghdad, IRAQ.
[2]Department of Computer Science, College of Education, Mustansiriyah University, 10052 Baghdad, IRAQ,

*Correspondent contact: bmn774@uomustansiriyah.edu.iq

Article Info

Received
29/06/2023

Revised
19/07/2023

Accepted
23/07/2023

Published
30/12/2023

ABSTRACT

The rapid tech growth and widespread internet usage caused a surge in sharing multimedia (text, images, videos, audio) across public networks. Protecting this data is vital, demanding encryption to prevent unauthorized access. Image encryption distorts images for security. This paper highlights encryption's vital role in safeguarding multimedia, especially amid rising internet use and media exchange. It introduces a novel solution: a chaotic three-dimensional system for color image encryption. The study scrutinizes system traits using math software. It employs a new chaotic system to generate a crucial key sequence for pixel scrambling. Utilizing stream cipher encryption enhances security. Extensive security analysis tests its resilience against attacks like histogram and correlation techniques. Results are promising: a fairly uniform histogram, minimal correlation among pixels nearing zero, and entropy close to the ideal. Metrics like NPCR and UACI almost match ideal values, ensuring high security. Experiments confirm its effectiveness in encrypting diverse color images. The approach guarantees a uniform histogram, minimal pixel correlation nearing zero, entropy near the ideal value (8), and NPCR/UACI values close to ideals (99.61191% and 33.41068% respectively).

KEYWORDS: Chaotic system, Image Encryption, Performance Evaluation, Key generation, Differential and Statistical attack, UACI, NPCR.

الخلاصة

بسبب التقدم السريع في مجال الاتصالات والزيادة في استخدام الإنترنت لتبادل البيانات المتعددة الوسائط مثل النصوص والصور ومقاطع الفيديو والصوتيات عبر الشبكات العامة، أصبح من الضروري حماية هذه البيانات. تُعتبر طرق التشفير أساسية لحماية المعلومات من التسرُّب، حيث يقوم تشفير الصور بتحويلها إلى أشكال غير مقروءة لتأمينها من المستخدمين غير المرخص لهم. يركز هذا البحث على أهمية منهجيات التشفير في حماية البيانات المتعددة الوسائط، خصوصاً في ظل التزايد الملحوظ في استخدام الإنترنت وتبادل البيانات الوسائطية عبر الشبكات العامة. يقترح البحث حلاً جديدًا يعتمد على نظام فوضوي ثلاثي الأبعاد مصمم خصيصًا لتشفير وفك تشفير الصور الملونة. يستكشف البحث خصائص النظام وسلوكياته الديناميكية باستخدام برمجيات رياضية .تعتمد الخوارزمية المقترحة نظامًا فوضويًا جديدًا لتوليد سلسلة مفاتيح، تُستخدم لتشتيت بكسلات الصورة. يُطبَّق بعد ذلك تشفير سلسلة المفاتيح القائم على المفتاح، مما يعزز الأمان من خلال عملية توليد مفتاح صعبة التنبؤ. يخضع النظام المقترح لتحليل أمان شامل باستخدام تقنيات مثل تحليل الهيستوغرام والترابط لتقييم صموده ضد الهجمات الإحصائية والتفاضلية .تشير نتائج الدراسة إلى نتائج إيجابية: هيستوغرام موزع بشكلٍ متساوٍ نسبيًا، وقيم ترابط بين البكسلات المتجاورة دقيقة وتقترب من الصفر، والتشوش يقترب من القيمة المثالية. بالإضافة إلى ذلك، تقترب قيم NPCR (معدل تغيير عدد البكسلات) و UACI (متوسط تغيير الشدة الموحد) من القيمة المثالية، مما يدل على مستوى عالٍ من الأمان المقدم من النظام المقترح. تظهر النتائج التجريبية فعالية النظام المقترح في تشفير مختلف أنواع الصور الملونة، مؤكدة أن الهيستوغرام متساوٍ والترابط بين البكسلات المتجاورة صغير جدًا ويقترب من الصفر، والتشوش يقترب من القيمة المثالية (٨). كما تقترب قيم NPCR و UACI من القيمة المثالية والتي هي (٩٩,٦١١٩١٪) و (٣٣,٤١٠٦٨٪) على التوالي.

INTRODUCTION

Ensuring the safety of image data transmitted across networks has become a crucial aspect, and image encryption plays a vital role in achieving this goal. Over time, extensive research and development have been carried out in image encryption. As a result, numerous approaches and procedures have been created in an attempt to identify the fastest and most secure method for encrypting digital image content [1][2]. Image encryption presents a number of challenges, including encryption quality, processing time, and difficulties associated with the encryption key (such as key space and key exchange in the case of symmetric key) [3-5]. A more robust encryption technique is indicated by a higher level of noise and a more unintelligible encrypted image. Key space refers to the entire set of keys that the key generation algorithm can generate; a larger number of possibilities means greater security and resistance to attacks. It is essential to have a secure method for exchanging the encryption key because the same key is used for both encryption and decryption in symmetric key algorithms. Any exposure of the key could potentially jeopardize the entire system [6][7]. The aim of this research is to create, test, and assess a secure and dependable system for exchanging image data over networks. The proposed 3D chaotic system employs the characteristics of a chaotic system to generate long and pseudo-random keys, which are then used to encrypt image data.

Literature Survey of 3D Chaotic System Based Image Encryption

Numerous researchers have conducted studies in the field of image encryption to develop various techniques. Here is a concise summary highlighting various research and methodologies concentrated on chaotic image encryption. Zhang *et al.* [8] proposed a method that uses the magic square transformation. As a pretreatment, the magic square method is used. The second picture was then scrambled using an Arnold cat map, which is the most widely used map in chaos-based encryption. By utilizing the Henon method, an array will create the image's jumbled gray values image. Using chaotic maps, In the study by Kester [9], an enhanced cipher algorithm was introduced to facilitate the encryption of images with size (m×n). This was achieved through the shuffling of the RGB pixel values, allowing for the encryption and subsequent decryption of images based on these pixel values. During the decryption process, it is necessary to reconstruct the original RGB pixel values. For the initial picture preprocessing, Wang and Luan [10] devised a novel method consisting of two stages: confusion and diffusion. A series of reversible cell automata are then run on higher half-pixel bits in the diffusion step, and this produces the final cipher picture. The key plays a crucial role in every cryptographic algorithm, as it directly influences the level of security it can provide [11].

The New 3D Chaotic System

The primary objective is to develop a mathematical model that describes a novel three-dimensional chaotic system. This system is autonomous and can be obtained using the following procedure:

$$\frac{dx}{dt} = -a\,y + b\,x + y\,z - c\,y\,Cos(z) \quad (1)$$

$$\frac{dy}{dt} = -d\ Sin(z) - e\,y - f\,x^2 + g\,x\,z - h\,x\,Cos(z) \quad (2)$$

$$\frac{dz}{dt} = -i\,y\,x - j\,z - i\,Sin(y) - k\,x\,Cos(x) \quad (3)$$

where x, y, z and $t \in \Re$ called the states of system and a, b, c, d, e, f, g, h, i, j and k are positive parameters of the system.

A chaotic three-dimensional system is described by a mathematical model with positive parameters and state variables, denoted as and, respectively. The system exhibits a chaotic attractor when specific values of the parameters are chosen, leading to the following relationship: a chaotic attractor is seen in the new three-dimensional chaotic system (1):

a=15, b=6, c=0.5, d=12, e=13, f=7.4, g=21, h=11, i=5, j=20 and *k=3*. The initial conditions are *x(0)= -2, y(0)=2, z(0)=0.3*.

Numerical simulations of the nonlinear system were conducted using the MATHEMATICA program. The system displays rich and complex chaotic dynamics, as evidenced by the strange attractors observed in two-dimensional and three-dimensional space, as shown in Figure 2. The attractors are reminiscent of a butterfly flapping its wings, giving rise to the term "Butterfly Effect". Additional visualizations of the strange attractors are presented in Figure 1.

ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 34, Issue 4, 2023 DOI: https://doi.org/10.23851/mjs.v34i4.1411

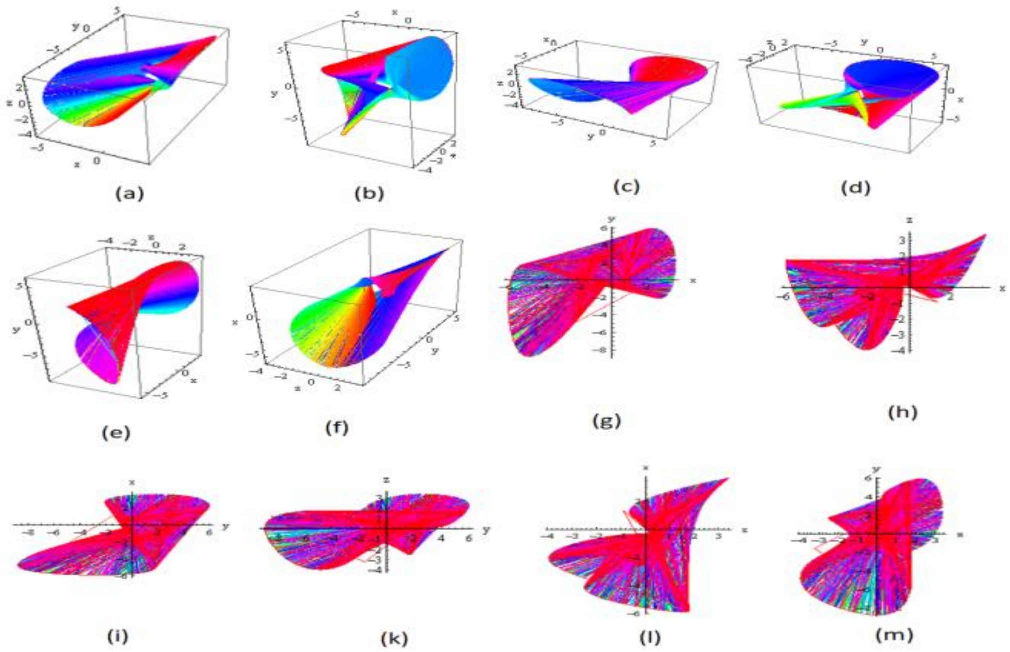

Figure 1. (a,b,c,d,e,f) : Phase portrait of system in 3D. (g,h,i,k,l,m) Phase portrait of system in 2D.

As is widely recognized, the waveform of a chaotic system should lack any periodicity. To verify that the newly proposed system exhibits chaotic behavior, we present time versus states plots obtained from numerical simulations using the MATHEMATICA software the waveforms of (x(t), y(t), z(t)) in the time domain are also displayed in Figure 2. These plots demonstrate that the waveforms are aperiodic, which is a hallmark of chaotic systems. also exhibit a Sensitivity test of the new chaotic system to initial conditions.

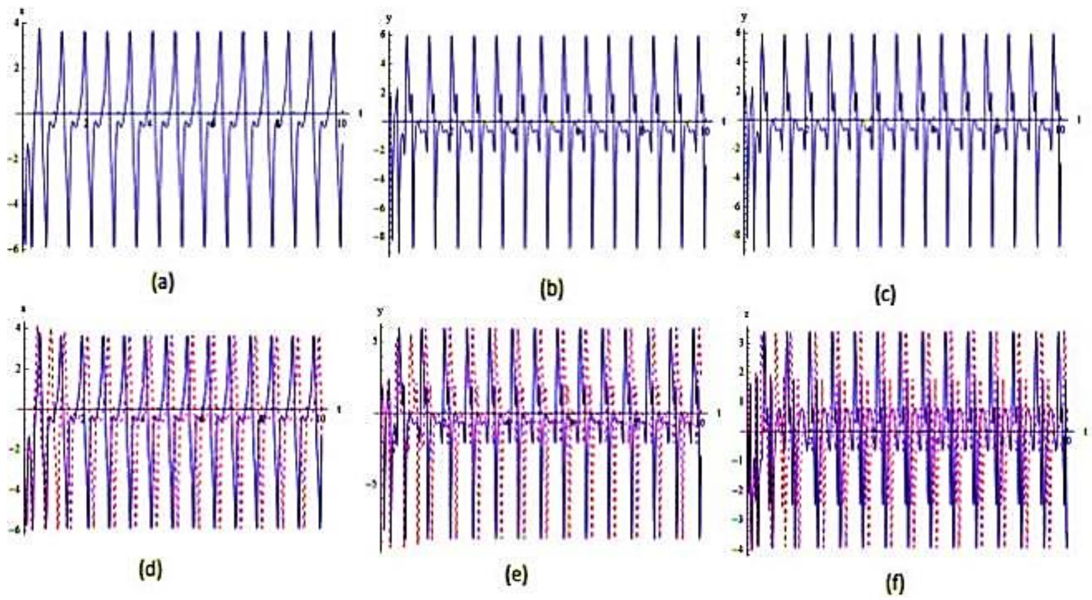

Figure 2. (a,b,c) Time versus *x*,*y*,*z* of the new chaotic system, (d,e,f)) Sensitivity test of the new chaotic system.

The defining characteristic of chaotic systems is their long-term unpredictability, which results from the sensitivity of the solutions to the initial conditions. Even for two initial conditions that are arbitrarily close, the resulting trajectories will diverge significantly over time. As a consequence, any finite number of digits in the initial condition will lead to a point in the future beyond which accurate predictions about the state of the system are impossible. Figure 3 illustrates this sensitivity of the chaotic

Proposed System

This paper presents the design of a proposed system for secure image interchange, encompassing encryption and transmission from sender to destination user. The two key stages of this system are the chaotic initial value distribution stage and the encryption/decryption stage, each consisting of multiple phases. The Novel Chaotic System, a high-dimensional chaotic system, is utilized as the key generator, with its differential equation mathematically

trajectories to initial conditions, as small variations in the initial conditions lead to significantly different outcomes over time.

described. Let the set of positive parameters of the Novel Chaotic System be denoted by The newly introduced three-dimensional chaotic system displays a chaotic attractor, which can be observed when the system parameters are assigned the following values: $a=15$, $b=6$, $c=0.5$, $d=12$, $e=13$, $f=7.4$, $g=21$, $h=11$, $i=5$, $j=20$, and $k=35M$. In addition, the system's initial conditions are set to x(0)=-2, y(0)=2, and z(0)=0.3, as illustrated in Figure 3, and the steps for the Novel Chaotic System key creation process are presented in Algorithm (1).

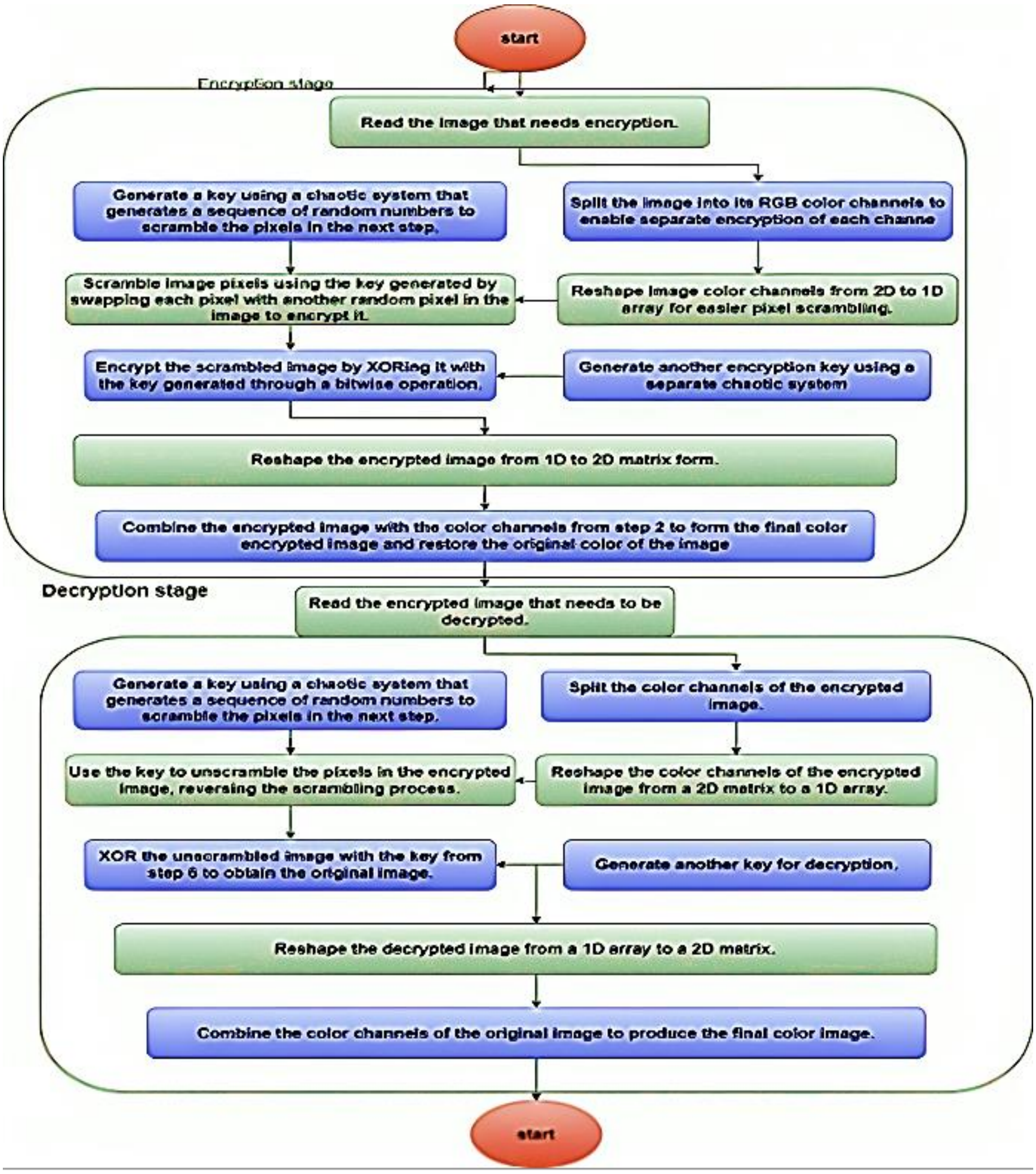

Figure 3. Block diagram of the proposed work.

ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 34, Issue 4, 2023 DOI: https://doi.org/10.23851/mjs.v34i4.1411

Algorithm (1): key Generation using Novel Chaotic System.

Input: Chaotic initial values (x_0,y_0,z_0)
Output: 3D Key sequence array

Begin
Apply the initial value (x_0,y_0,z_0)
For C=0 to length of dimensional image
  For i=0 to length of row image
    For j=0 to length of column image
      Utilize the proposed equations2 to compute (x_{n+1},y_{n+1},z_{n+1})
      X= input (x_{n+1})
      Y= input (y_{n+1})
      Z= input (z_{n+1})
      Utilize the new values (x_{n+1},y_{n+1},z_{n+1}) in equations(2,…,5)
    EndFor j
  EndFor i
EndFor C
X=reshape to two domination (X, Row, column)
Y=reshape to two domination (Y, Row, column)
Z=reshape to two domination (Z, Row, column)
Key 3D= X, Y, Z
End

In this work, the encryption process involves two stages. The first stage involves scrambling the image pixels by changing their locations using a random index distribution generated through the New Chaotic System. The second stage generates a sequential key that matches the size of the image and XORs the scrambled image with the key. This process is illustrated in Algorithm (2) and Figure 3.

Algorithm (2): Encryption Process

Input: original image, 3D Key sequence array
Output: Encrypted image

Begin
Step 1: Read the colored plain image (I) data.
Step 2: Let S = p × m.
Step 3: Divide the (I) image into three matrices (R, G, B), each matrix sized (p x m x 1).
Step 4: Repeat the first novel Chaotic System to generate three chaotic sequences {X1}, {Y1}, and {Z1}, where the size of the sequences is greater than or equal to S.
Step 5: Sort the generated chaotic sequences {X1}, {Y1}, and {Z1} in ascending order, resulting in sorted sequences {SX1}, {SY1}, and {SZ1} respectively.
Step 6: Generate index sequences (ISX1, ISY1, ISZ1)
  For each of the sorted sequences (SX1, SY1, SZ1) respectively.
  For each element in the original chaotic sequences (X1, Y1, Z1),
  find its position in the corresponding sorted sequence (SX1, SY1, SZ1),
  Store its position in the index sequence (ISX1, ISY1, ISZ1) respectively.
Step7: Repeat the Second novel Chaotic System to generate three chaotic sequences {X2}, {Y2},{Z2}
Step8: Sort sequences in ascending order manner ({SX2},{SY2},{SZ2})
Step9: Generate index For each sequences (IS) ;
  For each element in(X2, Y2, Z2)
  Find its position in sequences (SX2, SY2, SZ2)
  Store its position in index sequences (ISX2 ,ISY2 , ISZ2)
  End for
Step 10: Reshape the matrices (R, G, B) into vectors (VR, VG, VB) as follows:
  Step 10.1: Reshape the R matrix to a vector VR
  Step 10.2: Reshape the G matrix to a vector VG
  Step 10.3: Reshape the B matrix to a vector VB
Step11: Reorder the elements of (VR, VG, VB) vectors according to index sequences (ISX1, ISY1, ISZ1)
  For i from 1 to S do the following:
  Set CR(i) to the element of VR at the index ISX1(i)
  Set CG(i) to the element of VG at the index ISY1(i)
  Set CB(i) to the element of VB at the index ISZ1(i)
  End for
Step12: Apply XOR operation between vectors (CR,CG,CB) and sequences (ISX2,ISY2, ISZ2)
  Loop i from 1 to S:
  T1 ← mod(ISX2(i), 256)
  T2 ← mod(ISY2(i), 256)
  T3 ← mod(ISZ2(i), 256)
  DR(i) ← XOR(T1, CR(i))
  DG(i) ← XOR(T2, CG(i))
  DB(i) ← XOR(T3, CB(i))
  End loop
Step13: Apply XOR operation between vectors (DR, DG, DB) and sequences (ISX1, ISY1, ISZ1) // Encryption by first chaotic system
  Loop i ← 1 to S
  T1 ← mod(ISX1(i), 256)
  T2 ← mod(ISY1(i), 256)
  T3 ← mod(ISZ1(i), 256)
  ER(i) ← XOR(T1, DR(i))
  EG(i) ← XOR(T2, DG(i))
  EB(i) ← XOR(T3, DB(i))
  End loop
Step14: Reshape vectors (KR, KG, KB) to matrices (R`, G`, B`) each of size (p`×m`×1)
  Step14.1: R`← Reshape KR vector to matrix
  Step14.2: G`← Reshape KG vector to matrix
  Step14.3: B`← Reshape KB vector to matrix
Step15: Combine (R`,G`,B`) to create encrypted image (EI)
End.

RESULTS AND DISCUSSION

Proposed Results

Experimental results show that proposed is effective at encrypting various types of color images. Testing of the images revealed that they are completely random in shape, making it difficult for attackers to extract any useful information from them. Figure 4 shows how well suggested algorithm works at encrypting different kinds of color images while preserving security and confidentiality.

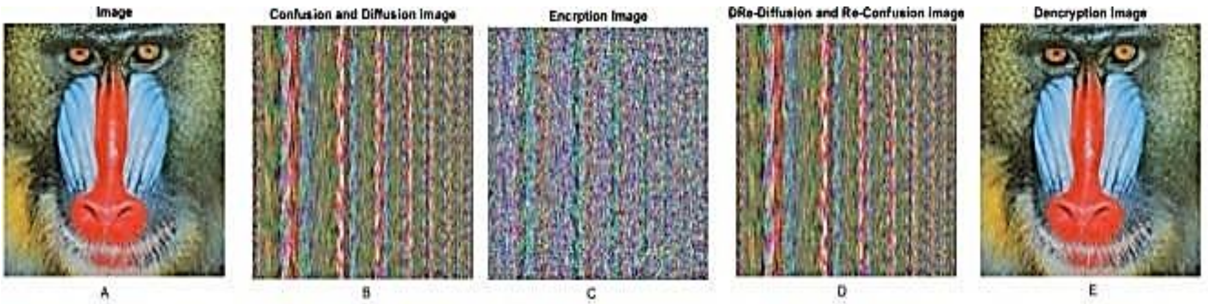

Figure 4. Experimental results: a) Original image, b) Confusion and Diffusion image, c) Encrypted image, d) Re-diffusion and re-confusion image, e) Decrypted image.

The test outcomes of an encryption technique using the Baboon image are shown in Figure 4. Panel (a) depicts the original image, while panel (b) depicts the Confusion and Diffusion image. A change in one bit or element of the plaintext must impact all of the bits or elements of the ciphertext, whereas confusion indicates that each bit or element known as plaintext affects several bits or elements of the ciphertext. Confusion and diffusion are two essential ideas in encryption. Section (c) depicts an image with encryption created by utilizing a secret key to the Confusion and Diffusion image. Panel (d) depicts the image of Re-Diffusion and Re-Confusion that is created by reversing the process of diffusion and confusion. This phase is crucial to improving the encoding method's security. The decrypted image was obtained by applying the reverse transformation with the identical secret key that was utilized for secrecy, as shown in panel (e). The efficiency of the technique of encryption is shown by the fact that the decrypted image is nearly identical to the genuine image. Overall, the results show that the technique of encryption presents an elevated degree of security while preserving image quality. Having the color histograms of the encrypted image equally spread across all components (RGB) is one way to ensure that encrypted images look random. Figure 5 depicts the RGB element histograms of original and encrypted images. The encrypted image's histograms seem to be evenly distributed across RGB, pointing to that the method of encryption reached randomness.

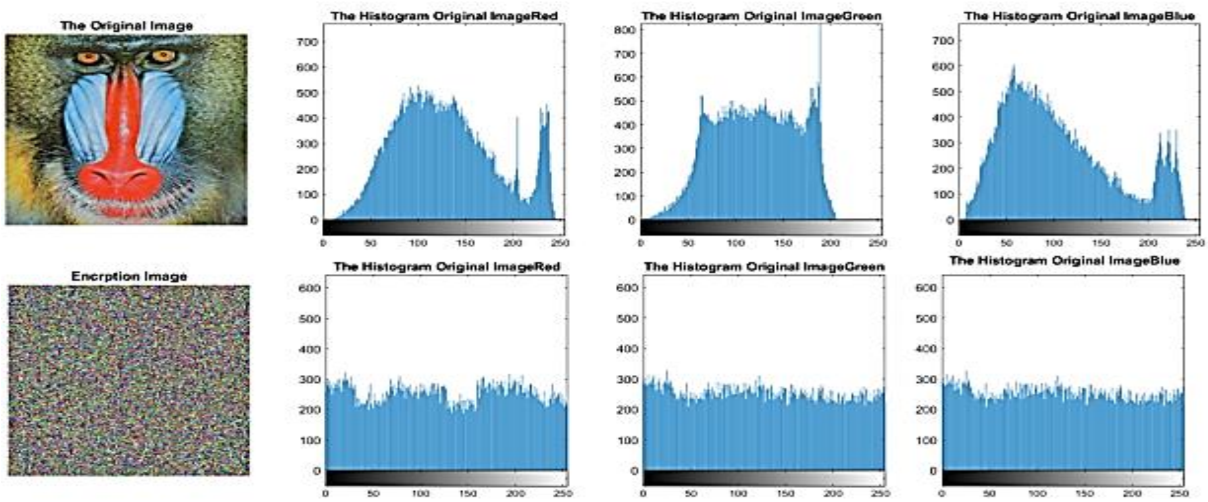

Figure 5. Histograms of original image and encrypted image.

ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 34, Issue 4, 2023 DOI: https://doi.org/10.23851/mjs.v34i4.1411

The histograms of the encrypted images show a uniform distribution of color values, indicating that the encryption algorithm is successfully generating random-like encrypted images. This makes it difficult for attackers to extract any useful information from the encrypted images

Correlation Coefficient Analysis

In order to thwart correlation analysis, it is crucial to minimize the correlation among adjacent pixels in an encrypted image. Figure 6 illustrates the correlation coefficients of the encrypted images produced by horizontally, vertically, and diagonally encrypting them using the proposed algorithm. Upon observing Figure 6, it is evident that the correlation coefficients of the encrypted images generated by the suggested algorithm approach zero, while the correlation coefficients of the original images tend to be closer to one. This observation indicates that the encrypted image pixels, when utilizing the proposed algorithm, exhibit a high level of independence and lack predictability. Consequently, the suggested algorithm demonstrates enhanced security characteristics.

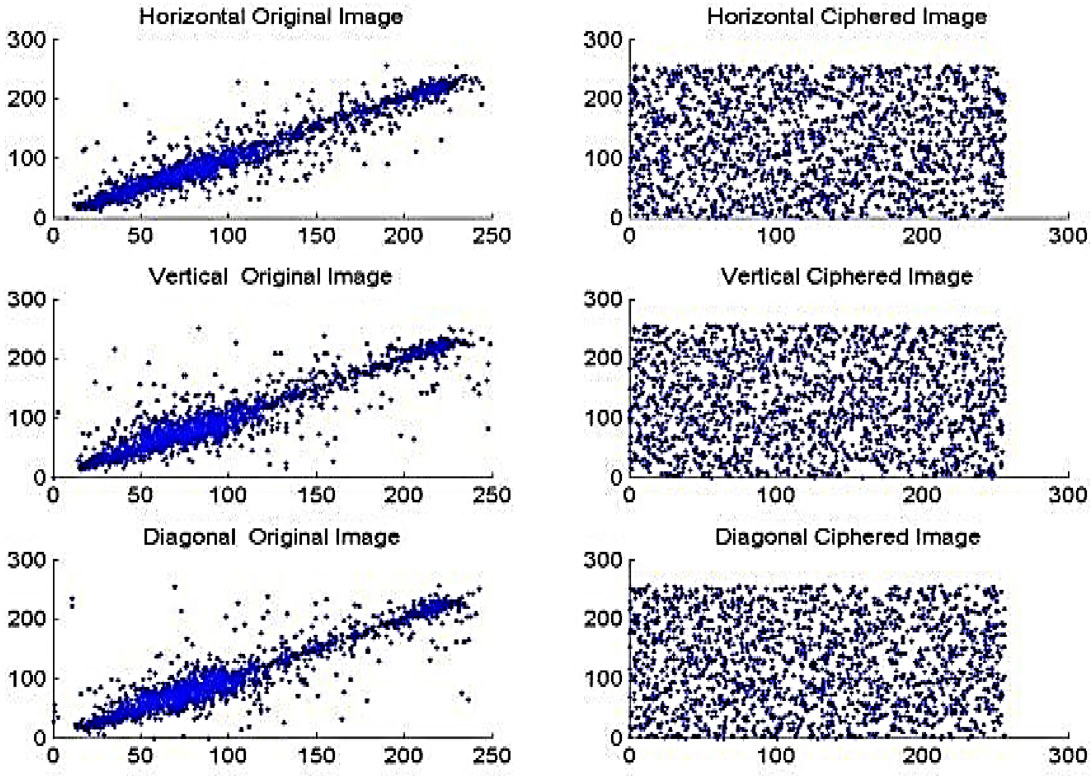

Figure 6. Correlation coefficients of the original and encrypted images.

Differential and statistical Attack Analysis

Overall, the results of chapter four indicate that the proposed chaotic encryption algorithm provides a high level of security and robustness against different attacks, making it suitable for applications in different fields, including image and video encryption, secure communication, and data protection, The original entropy measures the randomness in the pixel values of the original image, making it a good candidate for encryption. The encrypted entropy measures the randomness in the pixel values of the encrypted image, which indicates the quality of encryption. PSNR and MSE are measures of image quality and should ideally have high values for good encryption. NPCR and UACI are additional measures of encryption quality, which should be close to 100% for effective encryption. Encryption and decryption time measures how long it takes to perform these operations and are important considerations for real-time applications are presented in Table 1.

Table 1. Shows the results of performance tests for the suggested image encryption algorithm.

Image	Original Entropy	Encryption Entropy	PSNR	MSE	NPCR	UACI	Enc. Time	Dec. Time
LENA	7.4072	7.9976	∞	0	99.6987%	33.1019	5.1362707	5.31376110
BABOON	7.4086	7.9978	∞	0	99.7034%	33.0497	5.1096821	5.2717719

The original entropy measures the randomness in the pixel values of the original image, making it a good candidate for encryption. The encrypted entropy measures the randomness in the pixel values of the encrypted image, which indicates the quality of encryption. PSNR and MSE are measures of image quality and should ideally have high values for good encryption. NPCR and UACI are additional measures of encryption quality, which should be close to 100% for effective encryption. Encryption and decryption time measures how long it takes to perform these operations and are important considerations for real-time applications.

Proposed System and Lorenz System Comparison

The results show that the proposed chaotic systems outperform the compared Lorenz system in all the measures. Specifically, the correlation coefficients for the proposed systems are closer to 0, indicating a higher level of security against differential attacks. The entropy values for the proposed systems are closer to 8, indicating a more uniform distribution of the encrypted image. The NPCR and UACI values for the proposed systems are higher, indicating a better resistance against differential attacks. Finally, the execution time for the proposed systems is lower, indicating a faster encryption and decryption process. Overall, the results suggest that the proposed three-dimensional chaotic systems are more effective and efficient in encrypting color images compared to the Novel Chaotic System. Table 2 provides a comparison between the proposed three-dimensional chaotic systems and a three-dimensional chaotic Lorenz system in terms of different encryption performance measures for color image encryption. The measures include correlation coefficients, entropy, NPCR, UACI, and execution time.

Table 2. Comparison between our proposed systems and Lorenz system.

Image	Test name	Proposed System	Lorenz
	NPCR	99.9996	99.9994
	UACI	33.3333	33.3336
	Entropy	7.999	7.998
	PSNR	∞	∞
	MSE	0	0
	Correlation _H	-0.00012700	-0.0018037
	Correlation _V	0.00001287	0.00166835
	Correlation D	-0.00001323	-0.0011101
Lena. Size(512*512). PNG	Encryption time	5.1362707	6.125469
	Decryption time	5.21376110	5.824659
	NPCR	99.9999	99.9996
	UACI	33.3334	33.3335
	Entropy	7.99979	7.99978
	PSNR	∞	∞
	MSE	0	0
	Correlation _H	0.000833502	-0.00144434
	Correlation _V	-0.00189505	0.00146354
	Correlation D	0.00219941	0.005502857
Baboon. Size(512*768). PNG	Encryption time	8.5881602	8.98245
	Decryption time	6.8905297	7.7478567

CONCLUSIONS

The experimental findings pertaining to the quality of encrypted and decrypted image data showcase that the proposed encryption approach yields noisy encrypted data but delivers excellent quality in terms of reconstructed image data. The decrypting process achieves a MSE of zero due to the adoption of a lossless encryption technique based on bitwise XOR operation. It is worth noting that in stream cipher, there is no need for approximation or replacement procedures, ensuring a more precise encryption and decryption process. Results show that the suggested method has a sufficiently large key space to render brute force attacks impractical. To measure the security of the presented proposed system against statistical attack, differential attack, and brute-force attacks, detailed security analysis is done such as Histogram Analysis, Correlation, Noise Ratio and Speed Performance. From results of proposed work show the histogram is unify and correlation values for adjacent pixels very small and close to (0), while the entropy close to ideally value (8), also the values of NPCR and UACI are close to the ideal value which are (99.61191%) and (33.41068%) respectively. Because the Novel Chaotic System involves a differential equation, the process of creating keys for continuous chaotic maps is slower.

Disclosure and Conflict of Interest: The authors declare that they have no conflicts of interest.

REFERENCES

[1] H. Broer and F. Takens, Dynamical Systems and Chaos. Springer, New York, 2010. https://doi.org/10.1007/978-1-4419-6870-8

[2] Wang, X., LI, J., and Fang, J., Si'lnikov chaos of a 3-D quadratic autonomous system with a four-wing chaotic attractor. Proceedings of the 30th Chinese Control Conference, 2011, pp. 22-24.

[3] S. A. Mehdi and Z. L. Ali, A New Six-Dimensional Hyper-Chaotic System, 2019 International Engineering Conference (IEC), IEEE, pp. 211 - 215, 2019. https://doi.org/10.1109/IEC47844.2019.8950634

[4] M. Sueel, Cryptographic Pseudo-Random Sequences from the Chaotic Henon Map. Sadhana, 34(5), pp.689-701, 2009. https://doi.org/10.1007/s12046-009-0040-y

[5] S. A. Mehdi and A. A. Kadhim, Image Algorithm Based on a Novel Five-Dimensional Hyper Chaotic System and Sudoku Matrix, 2019 International Engineering Conference (IEC), IEEE, pp. 188-193, 2019. https://doi.org/10.1109/IEC47844.2019.8950560

[6] Z. H. Guan, F. Huang, and W. Guan, Chaos Based Image Encryption Algorithm. Physics Letters A,346, pp. 153- 157, 2005. https://doi.org/10.1016/j.physleta.2005.08.006

[7] S. A. Mehdi, Image encryption algorithm based on a novel 4D chaotic system, International Journal of Information Security and Privacy, Vol.15(4), pp. 118-131, 2021. https://doi.org/10.4018/IJISP.2021100107

[8] Y. Zhang, P. Xu and L. Xiang, Research of image encryption algorithm based on chaotic magic square, in: Advances in Electronic Commerce, Web Application and Communication, pp. 103-109, Springer, Berlin, Heidelberg, 2012. https://doi.org/10.1007/978-3-642-28658-2_16

[9] Q. A. Kester, Image encryption based on the RGB pixel transposition and shuffling, Int. J. Comput. Network Inform. Sec. 5 7, pp.43-50, 2013. https://doi.org/10.5815/ijcnis.2013.07.05

[10] X. Wang and D. Luan, A novel image encryption algorithm using chaos and reversible cellular automata, Commun.11. N onlinear Sci. Numer. Simul. V.18, pp. 3075-3085, 2013. https://doi.org/10.1016/j.cnsns.2013.04.008

[11] A. N. Abdulraheem and B. M. Nema, "Secure IoT Model Based on PRESENT Lightweight Modified and Chaotic Key Generator," 2020 1st. Information Technology to Enhance e-learning and Other Application (IT-ELA, Baghdad, Iraq, pp. 12-18, 2020. https://doi.org/10.1109/IT-ELA50150.2020.9253079

How to Cite

Z. H. Thabit, S. A. Mehdi, and B. M. Nema, "Enhancing Color Image Security: Encryption with Dynamic Chaotic Three-Dimensional System and Robust Security Analysis", *Al-Mustansiriyah Journal of Science*, vol. 34, no. 4, pp. 87–95, Dec. 2023.