Extremely-Large Key-Space Color Image Encryption Scheme using Combined Memristive Chaotic System

Saja Abdul Kadhim Abdul Hassan[1] and Raad Sami Fyath[2]

Authors affiliations:
1) Department of Computer Engineering, College of Engineering, Al-Nahrain University, Baghdad, Iraq
kadhimsaja@gmail.com

2) Department of Computer Engineering, College of Engineering, Al-Nahrain University, Baghdad, Iraq.
rsfyath@yahoo.com

Paper History:

Received: 6th Dec. 2024

Revised: 10th Mar. 2025

Accepted: 19th Apr. 2025

Abstract

The security level and robustness of memristive image encryption techniques depend on the order and dynamics complexity of the memristive system. The grid multi-double-scroll (GMDS) chaotic system (CS) offers extremely rich dynamics but the implementation of high-order chaos needs large computation time. To overcome this limitation, researchers have proposed the use of muti-lower-order CSs to assist the encryption process individually. This scenario may reduce the security level since the non-friendly user may attack each involved CS independently. This paper proposes an effective six-dimensional (6D) memristive chaotic system constructed by combining 5D, 5D, and 7D GMDS chaotic systems. Each of the six chaotic sequences is generated from three sequences corresponding to two or three of the basic CSs. The combined CS shares the same total key parameters (initial values and design parameters associated with the three basic CSs) and this leads to a key space of 2^{2392}, the highest among the reported image encryption techniques. The combined CS is used to assist the operation of a proposed color image encryption scheme consisting of four sequential stages that perform compressive sensing, scrambling, DNA encoding, and diffusion, respectively. Simulation results validate the feasibility and robust security of the proposed encryption scheme.

Keywords: Color Image Encryption; Memristive Chaotic Encryption; Combined Memristive Chaotic System

مخطط تشفير صور ملونة بمساحة مفتاحية كبيرة للغاية باستخدام نظام ميموريستر فوضوي مدمج

سجى عبد الكاظم عبد الحسن، رعد سامي فياض

الخلاصة:

يعتمد مستوى الأمان وقوة تقنيات تشفير الصور التي تستخدم نظام الميموريستر الفوضوي (Memristive Chaotic System) على تعقيد النظام المريستيفي وديناميكيته. يقدم نظام الفوضى المتعدد التمريرات المزدوجة الشبكي (Grid multi-double-scroll (GMDS)) ديناميكيه غنية جدًا، ولكن تنفيذ الفوضى عالية المرتبة يتطلب وقتاً طويلاً للحسابات. للتغلب على هذا القيد، اقترح الباحثون استخدام أنظمة فوضوية منخفضة المرتبة لدعم عملية التشفير بشكل فردي، مما قد يؤدي إلى انخفاض مستوى الأمان حيث يمكن للمهاجم استهداف كل نظام فوضوي على حدة. يقترح هذا البحث نظامًا فوضويًا مريستيفيًا فعالاً من المرتبة السادسة، يتم إنشاؤه من دمج ثلاثة أنظمة فوضوية ذات خمسة وستة وسبعة مراتب. يتم توليد كل سلسلة فوضوية من ثلاثة تسلسلات تعتمد على اثنين أو ثلاثة من الأنظمة الأساسية. يشترك النظام المدمج على نفس المعلمات المفتاحية (القيم الأولية ومعلمات تصميم الأنظمة الأساسية الثلاث)، مما يؤدي إلى مساحة مفاتيح بحجم ٢^٢٣٩٢، وهي الأكبر بين تقنيات تشفير الصور المبلغ عنها في الادبيات العلمية. تم استخدام هذا النظام الفوضوي لدعم خوارزمية مقترحة لتشفير الصور الملونة، والتي تتكون من أربع مراحل متتالية تشمل التحسس الانضغاطي (Compressive sensing)، التشويش

NJES is an **open access Journal** with **ISSN 2521-9154** and **eISSN 2521-9162**

(Scrambling)، الترميز باستخدام الحمض النووي (DNA encoding)، والانتشار(Diffusion) . أثبتت نتائج المحاكاة جدوى وقوة أمان الخوارزمية المقترحة.

1. Introduction

The security level and robustness of image encryption techniques can be enhanced strongly by adopting chaotic system (CS) rather than pseudo random number generator (PRNG) [1][2][3]. The CS has nonlinear dynamical behavior which is highly sensitive to initial conditions; tiny changes in initial conditions can lead to significant variations in long-term behavior [4][5]. Although, the CSs follow deterministic rules, where their state equations fully describe their dynamics without involving randomness, they have unpredictable behavior. Generally, the CS-assisted image encryption technique uses two identical CSs (same configuration and same initial conditions), one for the encryption process and the other for the decryption process as illustrated in Fig. 1 [6][7]. The efficiency of using CS in encryption techniques depends on the richness and strength of its nonlinear dynamics which are function of its dimension (order) [8][9] and its configuration (state space equations) [10][11].

Recently, there is increasing interest in using a memristive chaotic system (MCS) in image encryption techniques due to its highly-complex and extremely rich dynamical behavior [12][13][14][15]. The MCS combines the principles of chaos theory and the unique properties of memristors. In electrical circuits, the memristor is considered as the fourth basic passive element which acts as a nonlinear resistor that can remember the amount of charge that has previously flowed through it. This leads to nonlinear behavior and can give rise to chaotic dynamics [16][17]. A typical MCS can be described by a set of differential equations that incorporate the memristor's behavior and can be designed with high dimensions. For example, four-dimensional (4D) [18], 5D [19], 6D [20][21], and 7D [22] MCSs were designed by different research groups to realize highly secure image encryption systems. The design of these chaotic systems has been extended further to produce muti-scroll (MS) [23][24][25][26], multi-double-scroll (MDS) [27][28], grid MS (GMS) [29], and grid multi-double-scroll (GMDS) attractors [30]. The shapes of these attractors are illustrated in Fig. 2. The multi-scroll attractor is a complex chaos phenomenon having irregular scroll trajectories which offer higher tunability and complexity than single scroll attractors [23]. These features can be developed further by adopting GMS and GMDS chaotic systems. Lin et al. presented 5D, 6D, and 7D chaotic systems that are characterized by GMDS attractors extending in one, two, and three dimensions, respectively [30]. Their results showed that GMDS chaotic system offers extremely rich and very complex dynamics which makes it very efficient to realize high-secure and high-robust encryption techniques. These findings were deduced by applying the 6D GMDS chaotic system for the encryption of gray images.

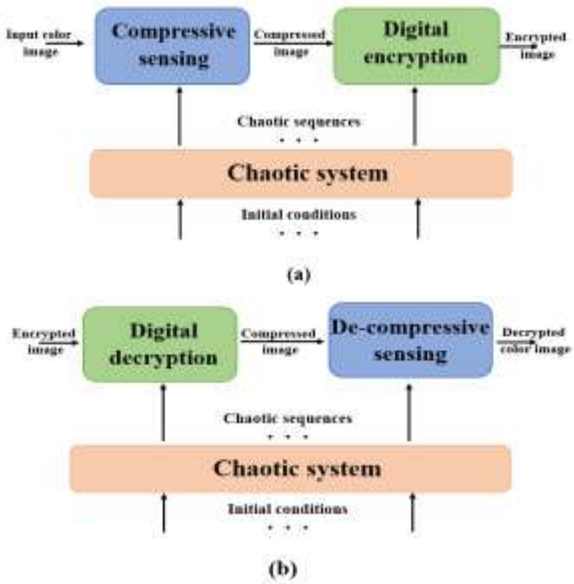


Figure (1): Basic block diagrams of chaotic image encryption (a) and decryption (b) techniques designed with compressive sensing

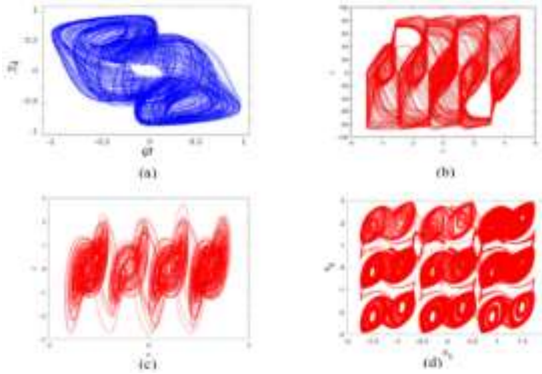


Figure (2): Examples of chaotic attractors (a) single scroll attractor [23], (b) multi-scroll attractor [26], (c) grid multi-scroll attractor [29], (d) grid multi-double-scroll attractor [30].

One approach to enhance further the security level and robustness of chaotic encryption techniques is to use a high-order CS [31]. This approach generally faces the challenge of increasing computation times required to generate the chaotic sequences used in the associated encryption and decryption processes. To solve this challenge, researchers proposed to use multi-lower-order CSs with each CS shares partially the encryption (decryption) process [3][32]. The main limitation of this approach is that the attacker may deal with individual lower-order CS rather than the main high-order one which may lead to reduce the security level. To overcome this limitation, researches proposed recently the design of effectively low-order CS with increasing number of chaotic parameters, and hence with enhanced nonlinear dynamical behavior, by combining multi-low-order CS [33][34].

This paper proposes a 6D combined memristive chaotic system for color image encryption/decryption scheme. The MCS is generated by combining 5D, 6D, and 7D GMDS chaotic systems which are characterized by extremely rich and complex dynamics. The proposed scheme is implemented digitally by cascading four chaotic assisted-sub-schemes (compressive sensing, scrambling, DNA encoding, and diffusion. The proposed CS has 45 key-shared parameters (18 initial values plus 27 basic chaotic systems parameters) leading to a key space $S = 2^{2392}$ which is highest value reported in the literature for digital image encryption.

The remainder of this paper is organized as follows. Section 2 introduces the proposed CS and gives some of it dynamical and randomness characteristics. The proposed image encryption/decryption scheme is described in Section 3 and its simulation results are presented in Section 4. Comparison with related work is given in Section5. A summary is given at the end of the paper in Section 6.

2. Proposed Combined Memristive Chaotic System

This section describes the construction of the proposed combined CS and examines its dynamical behavior. The proposed CS is constructed by linear combination of the three memristive grid multi-double-scroll chaotic systems described in [30] as illustrated in Fig. 3. Here, $\mathbf{x}(t)$, $\mathbf{y}(t)$, and $\mathbf{z}(t)$ present the state space vectors of the 5D, 6D, and 7D GMDS systems, respectively. The chaotic sequences of these three CSs are combined as described by Eq. 1 to yield the output 6D sequences qi-q6

$$q_i = p_x x_i + p_y y_i + p_z z_i \qquad i=1, 2, \ldots, 5 \quad \ldots\text{(1a)}$$

$$q_6 = p_x x_6 + p_y y_6 + p_z z_6 \qquad \text{(1b)}$$

where p_x, p_y, and p_z are the combining proportionality constants of the three systems, respectively. The dynamics of these systems are described by [30]

$$\begin{aligned}
\dot{x}_1 &= -x_1 + 0.5\,tanh(x_2) + 0.1\,tanh(x_4) + 0.2\,tanh(x_1)\\
\dot{x}_2 &= -x_2 + 10\,tanh(x_3) + W_1 tanh(x_1)\\
\dot{x}_3 &= -x_3 + tanh(x_4) - 4\,tanh(x_1)\\
\dot{x}_4 &= -x_4 + 18\,tanh(x_2) + d_1\,tanh(x_1) + tanh(x_4)\\
\dot{x}_5 &= b_1\,tanh(x_1) - c_1\,\mathbf{g}(x_5)
\end{aligned} \qquad (2)$$

$$\begin{aligned}
\dot{y}_1 &= -y_1 + 0.5\,tanh(y_2) + 0.1\,tanh(y_4) + 0.2\,tanh(y_1)\\
\dot{y}_2 &= -y_2 + 10\,tanh(y_3) + W_2\,tanh(y_1) + W_3\,tanh(y_2)\\
\dot{y}_3 &= -y_3 + tanh(y_4) - 4tanh(y_1)\\
\dot{y}_4 &= -y_4 + 18\,tanh(y_2) + d_2\,tanh(y_1) + tanh(y_4)\\
\dot{y}_5 &= b_2\,tanh(y_1) - c_2\,\mathbf{g}(y_5)\\
\dot{y}_6 &= b_3\,tanh(y_2) - c_3\,\mathbf{g}(y_6)
\end{aligned} \qquad \ldots \quad (3)$$

$$\begin{aligned}
\dot{z}_1 &= -z_1 + 0.5\,tanh(z_2) + 0.1\,tanh(z_4) + 0.2\,tanh(z_1)\\
\dot{z}_2 &= -z_2 + 10\,tanh(z_3) + W_4\,tanh(z_1) + W_5\,tanh(z_2) + W_6 tanh(z_3)\\
\dot{z}_3 &= -z + tanh(z_4) - 4tanh(z_1)\\
\dot{z}_4 &= -z_4 + 18\,tanh(z_2) + d_3\,tanh(z_1) + tanh(z_4)\\
\dot{z}_5 &= b_4 tanh(z_1) - c_4\,\mathbf{g}(z_5)\\
\dot{z}_6 &= b_5 tanh(z_2) - c_5\,\mathbf{g}(z_6)\\
\dot{z}_7 &= b_6 tanh(z_3) - c_6\,\mathbf{g}(z_7)
\end{aligned}$$

The control parameters of this chaotic system are $(a_1, \ldots, a_6)$, $(b_1, \ldots, b_6)$, $(k_1, \ldots, k_6)$, $(c_1, \ldots, c_6)$, and $(d_1,\ d_2,\ d_3)$. Further, $W_1 = a_1 + k_1 \sin(C_5)$, $W_2 = a_2 + k_2 \sin(C_{10})$, $W_3 = a_3 + k_3 \sin(C_{11})$, $W_4 = a_4 + k_4 \sin(C_{16})$, $W_5 = a_5 + k_5 \sin(C_{17})$, $W_6 = a_6 + k_6 \sin(C_{18})$. The function $\mathbf{g}$ is defined by $\mathbf{g}(\phi) = \phi - f(\phi)$. Note that $f(\phi)$ is the attractor function that is given by

$$f(\phi) = m[\sum_{i=0}^{M} \tanh(n(\phi + (1+2i)m)) + \sum_{i=0}^{M} \tanh(n(\phi - (1+2i)m))] \quad \ldots\text{(5)}$$

The dynamics of the q-chaotic system is governed by

$$\frac{dq_i}{dt} = p_x \frac{dx_i}{dt} + p_y \frac{dy_i}{dt} + p_z \frac{dz_i}{dt} \qquad i = 1, 2, \ldots, 5 \ldots\text{(6a)}$$

$$\frac{dq_6}{dt} = p_y \frac{dy_6}{dt} + p_z \frac{dz_6}{dt} + p_z \frac{dz_7}{dt} \qquad \ldots\text{(6b)}$$

Figures 4 a-c show examples of the phase portraits of the chaotic attractors of the 5D, 6D, and 7D memristive GMDS chaotic systems, respectively. The values of the initial conditions and chaotic system parameters used in the simulation are taken from [30]. Note that the double-scroll attractor extends in one, two, and three dimensions, respectively. All the three systems are characterized by very complex dynamical behavior which is an essential requirement to design high-secure encryption scheme. The phase trajectories of the attractors of the proposed chaotic system on the planes q_1-q_i (i=2, 3, .., and 6) are depicted in Figs. 5a-5e, respectively, which reflect enhanced dynamical complexity compared to the results of Fig. 4. The time response of the chaotic sequences q_1-q_6 are displayed in Fig. 6 which ensure chaotic behavior. In Fig.5, p_x, p_y, and p_z are set to 1 in the simulation.

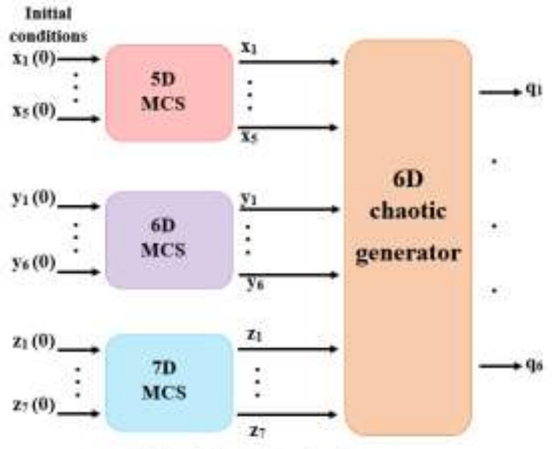


Figure (3): Block diagram of the proposed combined chaotic system.

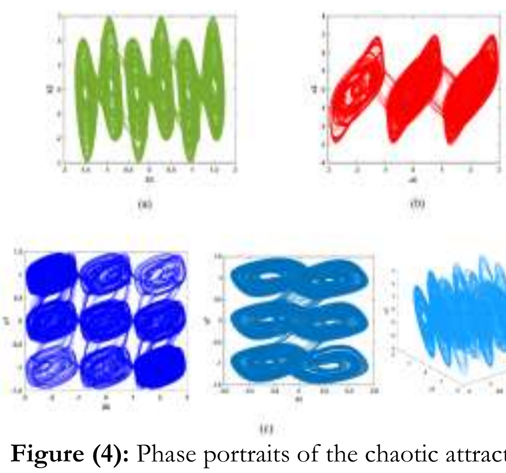


Figure (4): Phase portraits of the chaotic attractors of the 5D (a), 6D (b), and 7D (c) memristive GMDS chaotic systems.

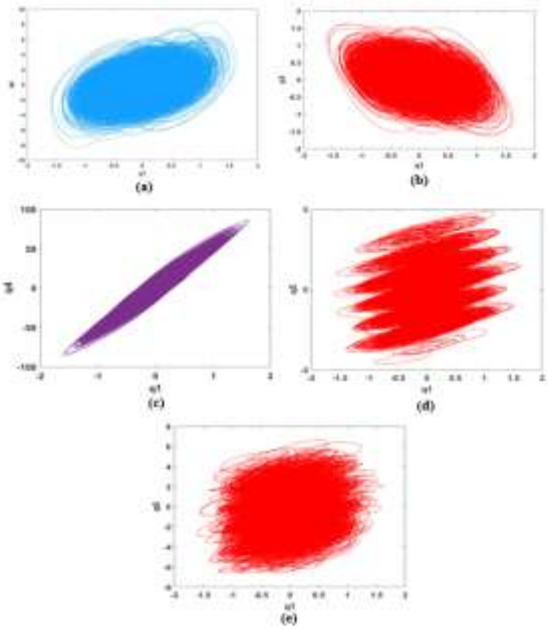


Figure (5): Phase trajectories of the attractors of the proposed chaotic system on the planes q_1-q_i. (i=2, 3, ...,6).

The autocorrelation is a measure for the similarity between a sequence and a shifted version of itself. If the chaotic sequences are used for generating encryption keys, then ideal sequences should have delta-autocorrelation functions. The plots of the autocorrelation functions of the six q-chaotic sequences are displayed in Fig. 7 which shows the delta-function behavior that indicates efficient results in terms of encryption security. This is because the plot shows very little correlation between each sequence and a shifted version of itself, even at very small lags, which is a desirable property for image encryption.

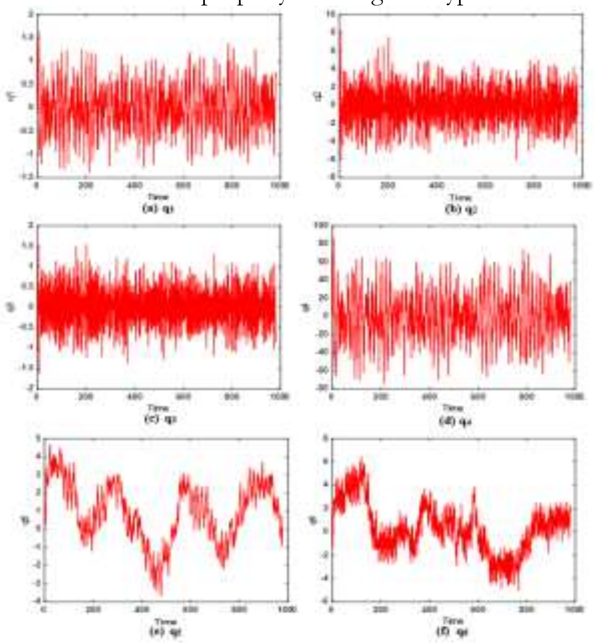


Figure (6): Time response of the chaotic sequences q_1-q_6.

The randomness of the q-chaotic sequences is evaluated using the National Institute of Standards and Technology (NIST) SP800-22 test suite. Data stream of bits is obtained from the proposed memristive CS which put into the NIST test set. The test results re displayed in Table 1 which show that all the p-values are greater than 0.01. This indicates that the system passes the NIST test and hence it can be well applied in the field of image encryption.

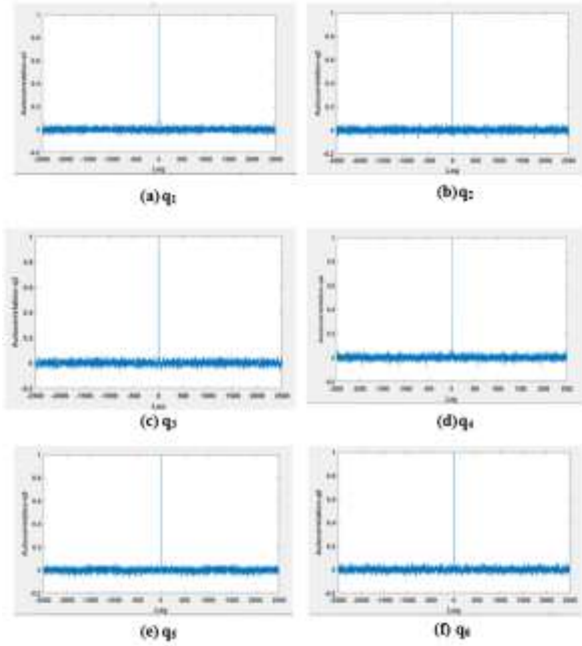


Figure (7): Plots of the autocorrelation functions of the six q-chaotic sequences.

It is worth to mention here that the combined 6D. CS is appeared as a virtual 18D CS but needs less and higher computation times compared with conventional 6D and 18D GMDS memristive systems, respectively. To discuss this point, let the symbol T_N denotes the computation time corresponding to Nth-order GMDS memristive CS. The simulation results reveal that $T_5/T_6 = 0.94$ and $T_7/T_6 = 1.028$. Assuming T_N/T_6 obeys the relation "a $\exp(_{bN})$", then a = 0.4344 and b = 0.15437. This leads to $T_{18}/T_6 = 6.99$ (assuming that the 18D GMDS memristive CS is designed using the same procedure adopted to design 5D, 6D, and 7D counterparts [30]). The simulation results also reveal that the relative computation time of the proposed CS $T_{proposed}/T_6 = 3.35$. Thus $T_{proposed} = 0.48\, T_{18}$. Note that $T_{proposed} = T_5 + T_6 + T_7 + T_{combining}$, where $T_{combined}$ is the computation time associated with the combing process. Hence $T_{combining}/T_6 = 0.124$.

3. Proposed Memristive Image Encryption and Decryption Schemes.

The proposed encryption scheme deals with a color image (RGB image) and its operation is assisted by the sequences generated by the proposed combined memristive chaotic system. The input color image is encrypted after passing it through four cascaded stages that perform compressive sensing, scrambling, DNA encoding, and diffusion (see Fig.8). The DNA encoding is implemented separately on the three color components [Red (R), Green (G), Blue (B)] and assisted by the chaotic sequences q_3, q_4, and q_5, respectively. The other encryption stages operate directly on the RGB domain and assisted by the chaotic sequences q_1, q_2, and q_6, respectively.

Table (1): NIST analysis of the proposed 6D chaotic sequences.

Test \ sequence	q_1	q_2	q_3	q_4	q_5	q_6	Result
Frequency	0.73991	0.16260	0.83430	0.53415	0.91141	0.90936	Pass
Block Frequency	0.06688	0.83430	0.16261	0.73991	0.53414	0.27570	Pass
Cumulative Sums forward	0.91141	0.73531	0.96429	0.63992	0.73991	0.90936	Pass
Cumulative Sums reverse	0.99146	0.96429	0.63711	0.91141	0.53414	0.63711	Pass
Runs	0.12232	0.87429	0.43726	0.53414	0.91141	0.43727	Pass
Longest Run	0.73991	0.27570	0.53726	0.27571	0.21330	0.83430	Pass
Rank	0.35048	0.02519	0.63771	0.31451	0.33414	0.83430	Pass
FFT	0.45044	0.63711	0.63711	0.73199	0.35048	0.02265	Pass
Non-Overlapping Template	0.21330	0.43712	0.27570	0.12232	0.21223	0.16260	Pass
Overlapping Template	0.73414	0.16260	0.43637	0.53414	0.91146	0.06196	Pass
Approximate Entropy	0.53414	0.02297	0.63718	0.35048	0.12232	0.43727	Pass
Serial1	0.12233	0.06196	0.43897	0.91141	0.73991	0.01263	Pass
Serial2	0.35048	0.43727	0.63712	0.06688	0.21330	0.27570	Pass
Linear Complexity	0.73992	0.83431	0.43771	0.73991	0.73991	0.96429	Pass

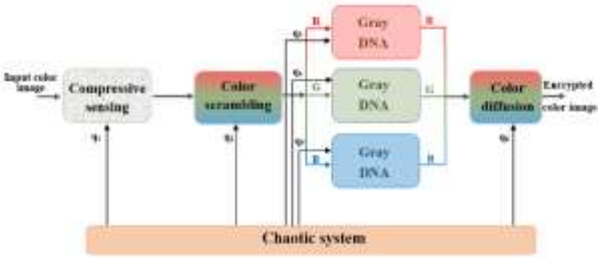


Figure (8): Proposed memristive color image encryption scheme.

The compressive sensing is achieved through four steps as illustrated in Fig. 9

i. Transfer the image to the discrete wavelet transform (DWT).
ii. Create the 2D measurement matrix using the chaotic sequence q_1.
iii. Compress the transferred image by using the measurement matrix.
iv. Quantize the result of step iii to produce the required compressed image.

The scrambling is based on 2D mapping of the compressed image with a chaotic image having the same size and created by using the chaotic sequence q_2. The process rearranges each pixel in the compressed image based on the index corresponding to it in the 2D memristive chaotic map generated by q_2. It sends each channel pixel value of the compressed image to a different pixel in scrambling image. The main advantage of the scrambling method is to make the encrypted image more resistant to various attacks such as brute-force attacks and statistical analysis. After the end of scrambling, the scrambled image passes to the DNA operation.

The DNA encoding stage splits the color scrambling image into three color channels (R, G, and B). The three channels are encrypted individually using the chaotic sequences q_3, q_4, and q_5, respectively. The DNA encryption of each channel is done in three steps. The first step is the DNA coding which encodes the image channel by using the principles of DNA (A, T, C, G) for each pixel value in the image. The second step is the rule operation which shuffles the DNA principles with complementary rule. The third step is encrypting the resulting image with XOR operation based on one of the chaotic sequences (q_3, q_4, and q_5). The final operation is merging the three channels into one color image and passing it to the diffusion operation.

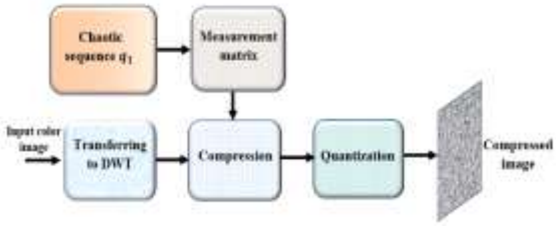


Figure (9): Compressive sensing algorithm.

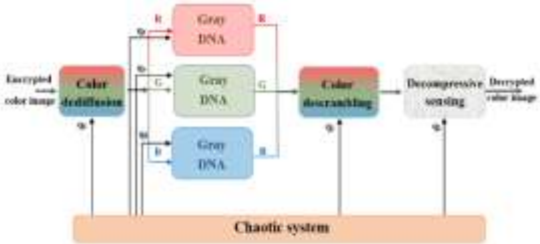


Figure (10): Proposed memristive color image decryption scheme.

The diffusion stage is the last part of the encryption scheme. After getting the DNA encrypted image, it creates 2D memristive chaotic image with same size of image using q_6 from the chaotic sequences. The operation defuses the entire image by taking each pixel with the index corresponding to it in the 2D memristive chaotic image generator in Bitwise XOR operation. This mechanism operates at the bit level, where each bit of the original data deals with a corresponding memristive chaotic bit generated in the 2D chaotic image. The main advantage of the diffusion method is enhancing the security by dispersing information widely and preventing the extraction of meaningful patterns from the encrypted data.

A block diagram of the proposed image decryption scheme is illustrated in Fig. 10 and uses four decryption stages corresponding to the four encryption stages used in the encryption scheme. The encryption image goes through dediffusion, DNA decoding, descrambling, and the decompressive sensing stages. The operation of these stages are assisted by the chaotic sequences q_6, (q_5, q_4, q_3), q_2, and q_1, respectively. Note that perfect decrypting process requires the use of q-chaotic sequence generation whose configuration and initial values match perfectly that used for the chaotic sequence generation adapted in the encryption scheme.

4. Results for the proposed Color Image Encryption/ Decryption Scheme

Simulation results corresponding to Pepper color image are presented in Figures 11and 12 to characterize the operations of the proposed digital encryption and digital decryption, respectively. Simulation results related to other 256×256 color images are given in Fig. 13. The encryption scheme contains four sequential stages; the corresponding images at the four outputs are shown in Fig. 11. The first stage is the compressive sensing assisted by the chaotic sequence q_1. The next three stages are scrambling, DNA encoding, and diffusion which are assisted by the chaotic sequences q_2, (q_3, q_4, q_5), and q_6, respectively.

The decryption algorithm is processed as done in the encryption algorithm but in reverse order and the results are shown in Fig. 12.

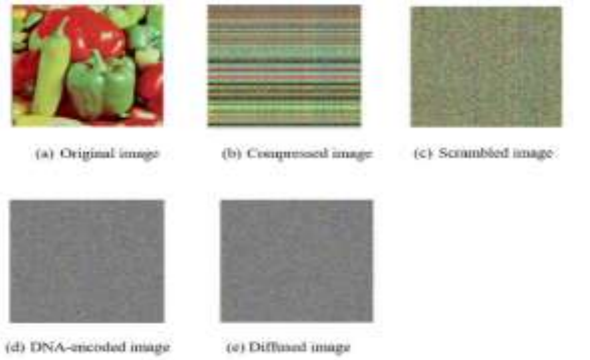


Figure (11): Simulation results of the encryption scheme corresponding to Pepper image.

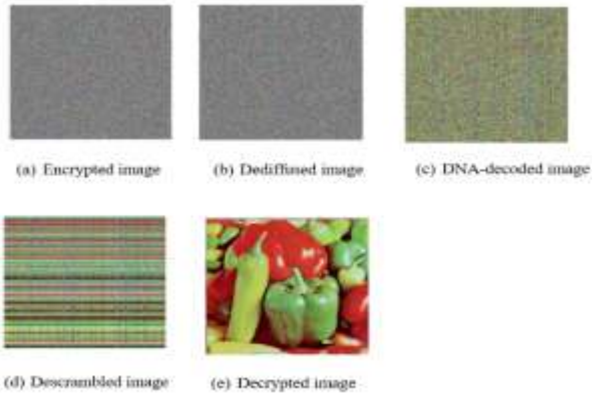


Figure (12): Simulation results of the encryption scheme corresponding to Pepper image.

Figure 13 shows the encryption/decryption simulation results for other color images (Lena, Baboon, Airplane, and Fruits).

4.2 Performance Evaluation Metrics

A security analysis is provided to evaluate the algorithm's performance. Unless otherwise stated, Pepper color image is used as the plain image to demonstrate the efficiency and security of the proposed scheme.

4.2.1 Histogram Analysis

The histogram analysis corresponding to the operation with Pepper input image is depicted in Fig. 14. It can be seen that the histogram of the encrypted image is quite uniform and significantly dissimilar to the histogram of the plaintext image. This prevents an attacker from learning anything about the plain image from its encrypted version. Note also that the histogram of the decrypted image almost matches that of the input image. This remark is also noticed for other input images as displayed in Fig. 15

4.2.2. Information Entropy

The performance of the proposed encryption scheme is tested through entropy measures. The entropy for the three-color channels of the final encrypted color images are presented in Table 2. These values in this table are very close to 8, which corresponds to the entropy of ideal encryption; $\log_2 256 = 8$, where 256 corresponding to the number of discrete intensity levels in each assuming color 8-bit system.

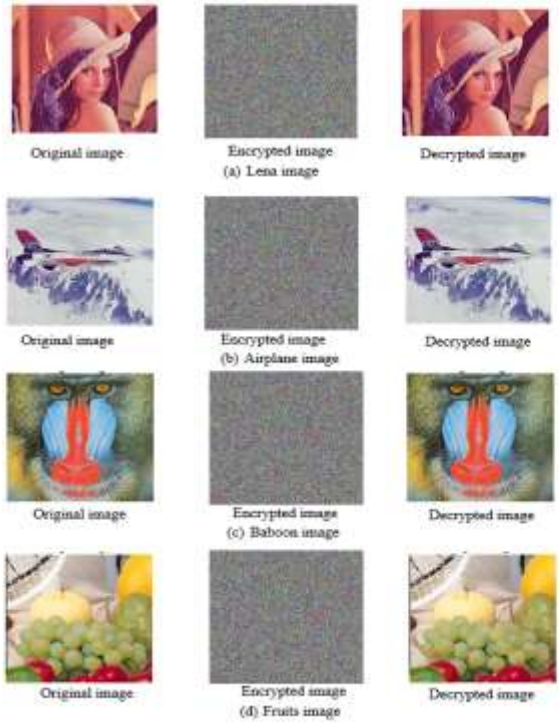


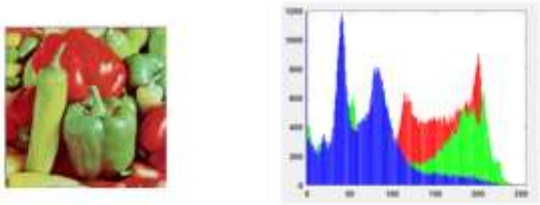
Figure (13): Simulation results when the proposed encryption/decryption scheme operates with a color input (plain) image of Lena, Baboon, Airplane, and Fruits images.

4.2.3 Correlation Coefficient Analysis

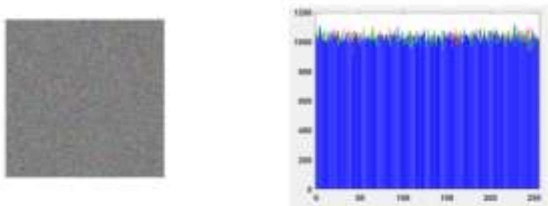
A correlation coefficient measures the similarity or difference between adjacent image pixels in the three directions: vertically (V), horizontally (H), and diagonally (D). In order to have an image encryption system which is cryptographically secure, a strong correlation between the adjacent pixels in all directions should be eliminated. The value of the correlation coefficient ranges from -1 to 1, such that -1 means that it has a negative correlation, $+1$ means that it has a positive correlation, whereas 0 corresponds to no correlation. Therefore, the encrypted image must have a correlation coefficient close to 0 between the adjacent pixels in all the directions so it would resist statistical attacks. Figures 16 and 17 display graphically the correlation analysis results of original and encrypted Pepper image in three directions and for the three-color channels, respectively. Table 3 lists the three-direction correlation coefficients for the RGB components of different original and encrypted images. The results in this table reveals that horizontal, vertical, diagonal correlation coefficients of the encrypted images are almost zero.

4.2.5 Key Space Analysis

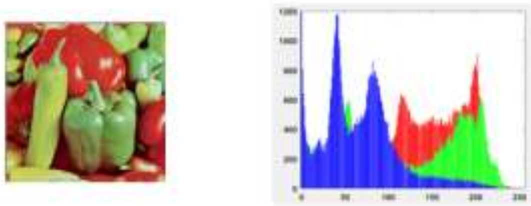
The key space of the proposed encryption algorithm can be estimated as follows. Let the algorithm uses double-precision numbers with 10^{-16} calculation precision. The key space S is estimated as $S = (10^{16})\ K$, where K is the total number of keys involved in the encryption operation [34]. The algorithm uses 45 keys coming from the 18 initial values of the sequences plus 27 chaotic system parameters $[(a_1, ..., a_6), (b_1,\ldots, b_6), (c_1,\ldots,c_6), (d_1, d_2,d_3)$, and $(k1,\ldots,k6)]$. Thus $S = (10^{16})^{45} = 10^{720} \approx 2^{2392}$ Encryption algorithm with key space $> 2^{100}$ is proved to be secure [27]. Thus, the proposed algorithm has sufficient large key space which ensures its high resistance to all types of brute-force attacks.



(a) Original image and its histogram



(b) Encrypted image and its histogram



(c) Decrypted image and its histogram

Figure (14): Simulation results of applying the histogram analysis to Pepper image.

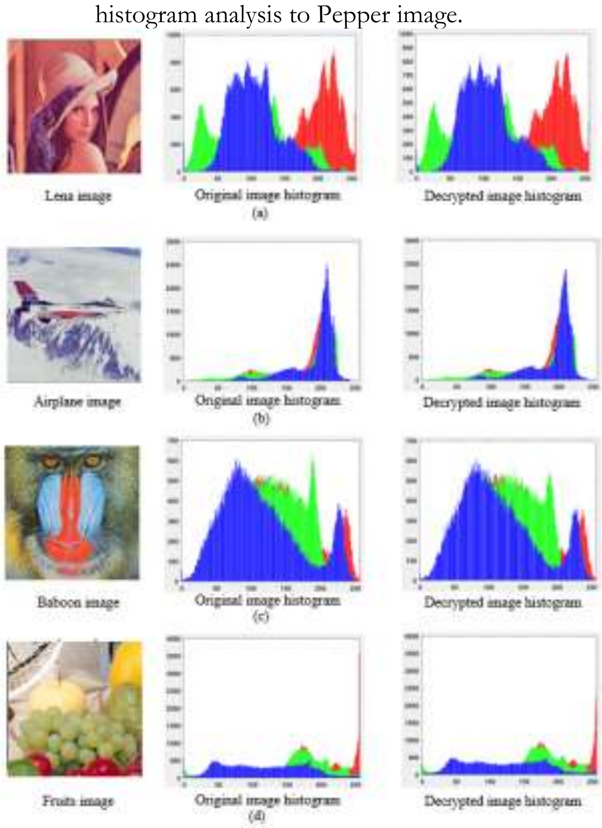
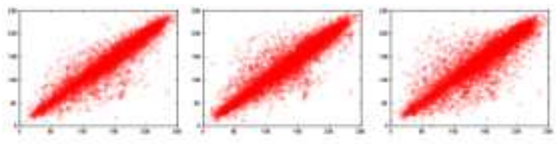


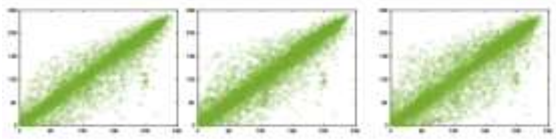
Figure (15): Simulation results of applying the histogram analysis to other images (Lena, Baboon, Airplane, and Fruits).

Table (2): Information entropy of different images.

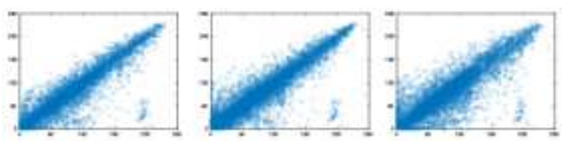
Image	RGB channels	Entropy values	
Pepper	Red	Original	7.3762
		Encrypted	7.9994
	Green	Original	7.6395
		Encrypted	7.9993
	Blue	Original	7.1346
		Encrypted	7.9993
Lena	Red	Original	7.3508
		Encrypted	7.9993
	Green	Original	7.6217
		Encrypted	7.9994
	Blue	Original	7.1294
		Encrypted	7.9993
Airplane	Red	Original	6.8271
		Encrypted	7.9992
	Green	Original	6.8696
		Encrypted	7.9993
	Blue	Original	6.4582
		Encrypted	7.9993
Baboon	Red	Original	7.6295
		Encrypted	7.9994
	Green	Original	7.3200
		Encrypted	7.9993
	Blue	Original	7.6276
		Encrypted	7.9993
Fruits	Red	Original	7.1835
		Encrypted	7.9992
	Green	Original	7.4587
		Encrypted	7.9993
	Blue	Original	7.7574
		Encrypted	7.9992



(a) Red channel



(b) Green channel



(c) Blue channel

Figure (16): Correlation distribution test results for the original Pepper image.

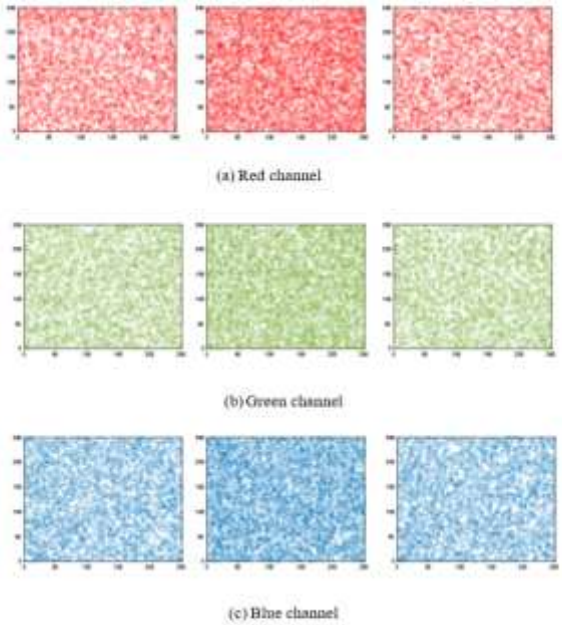


Figure (17): Correlation distribution test results for the encrypted Pepper image.

Table (3): Three-direction correlation coefficients of RBG color components of the original and encrypted images.

Image	Image Type	Channel	Horizontal	Vertical	Diagonal
Lena	Original	Red	0.93504	0.94772	0.88727
		Green	0.92763	0.96216	0.89509
		Blue	0.87152	0.92669	0.81233
	Encrypted	Red	-0.00047	0.00309	-0.00118
		Green	0.00101	-0.00465	-0.00559
		Blue	-0.00428	0.00501	0.00141
Baboon	Original	Red	0.94384	0.91705	0.89278
		Green	0.91335	0.87271	0.83453
		Blue	0.94571	0.92795	0.90049
	Encrypted	Red	-0.00172	0.00147	-0.00114
		Green	0.00503	-0.00605	-0.00687
		Blue	-0.00707	0.00488	0.00727
Pepper	Original	Red	0.95992	0.96766	0.92911
		Green	0.97651	0.98344	0.95930
		Blue	0.95019	0.96594	0.917256
	Encrypted	Red	-0.00056	0.00314	0.00016
		Green	0.00256	-0.00085	-0.00993
		Blue	-0.00349	0.005126	0.00636
Airplane	Original	Red	0.94105	0.92919	0.88115
		Green	0.95182	0.94040	0.90156
		Blue	0.91577	0.88973	0.82729
	Encrypted	Red	0.00036	0.00448	-0.00319
		Green	0.00302	-0.00331	-0.00691
		Blue	-0.00149	0.00910	0.00442
Fruits	Original	Red	0.94552	0.96090	0.91343
		Green	0.96108	0.971467	0.93871
		Blue	0.96574	0.97395	0.94515
	Encrypted	Red	-0.00115	0.00409	0.00019
		Green	0.00424	-0.00197	-0.00729
		Blue	-0.00304	0.00399	0.00378

4.2.4 Peak Signal-to-Noise Ratio

Table 4 lists the peak signal-to-noise ratio (PSNR) of the decrypted images. Note that the PSNR is almost image dependent. Among the five images considered in this work, the Baboon image has the lowest PSNR (=32.3dB). The other four images have PSNR values between 39.2 and 41.7 dB.

Table (4): Peak signal-to-noise ratio results for five different images.

Image	Lena	Baboon	Pepper	Airplane	Fruits
PSNR (dB)	**41.7**	**32.3**	**40.3**	**39.6**	**39.2**

4.2.6 Key Sensitivity Analysis

Many simulation tests are performed to address the sensitivity of the encryption process to initial conditions of the chaotic sequences. The results indicate that the decryption process completely fails when the initial value of any sequence is subjected to a very small variation in the decryption system from its value in the encryption system. Table 5 shows examples of the simulation results where the decrypted image corresponding to Pepper input image is recorded when the decryption system initial condition of one of the sequences q_1-q_6 deviates by a tiny value of 10^{-15}, 10^{-20} or 10^{-25}, from its encryption system value.

4.2.7 Differential Attack Analysis

For efficient encryption process the number of pixels change rate (NPCR) should be greater than 99% and the unified average change intensity (UACI) should also be greater than 33.35%. It is close to it. As a result, any slight difference in the plain image would result in a significant difference in the encrypted image. The NPCR and UACI of the proposed encryption scheme are calculated for different input images and the results are listed in Table 6. Note that the NPCR value is > 99% and the UACI value > 33.35%, which means that the system is efficient in terms of the differential attacks.

Table (5): Decrypted images corresponding to Pepper input image in the presence of tinny mismatch between the encryption/decryption initial values of one of the chaotic sequences q1-q6.

Correct Key		$+10^{-15}$ / $+10^{-20}$ / $+10^{-25}$
	q_1	
	q_2	
	q_3	
	q_4	
	q_5	
	q_6	

Table (6): NPCR and UACI of different color image channels.

Image	Channel	NPCR	UACI
Pepper	Red	99.7013	33.5564
	Green	99.7053	33.5694
	Blue	99.6991	33.5489
Lena	Red	99.6685	33.5094
	Green	99.7373	33.5087
	Blue	99.6868	33.5902
Baboon	Red	99.7222	33.5453
	Green	99.6542	33.5035
	Blue	99.7342	33.5029
Airplane	Red	99.6543	33.5515

	Green	99.6700	33.5858
	Blue	99.7078	33.5084
Fruits	Red	99.6708	33.5041
	Green	99.6844	33.5964
	Blue	99.6651	33.5066

5. Performance Comparison with Related Work

This section presents performance comparison between the proposed encryption system and some recently published chaos-based encryption systems. All the systems are assumed to deal with a single input image. Table 7 reflects performance comparison related to correlation coefficient of adjacent pixels, key space, information entropy, and PSNR of the decrypted image. Gray input images are considered in this table with Pepper gray image is adopted for our work. Investigating the results in this table highlights the following finding

i. The vertical correlation coefficient of the proposed work is closer to zero. The horizontal and diagonal correlation coefficients are almost negligible and lie within the limits offered by other encryption systems. These results indicate that the proposed system is effective in disrupting strong correlations in images.
ii. The proposed system has the largest key space, indicating its ability to withstand exhaustive attacks.
iii. The proposed system offers the higher ciphertext entropy and closer to 8. Thus, the information in the ciphertext is more chaotic, better concealed, and more disorganized.
iv. The highest PSNR is achieved with the proposed system which is higher than 40.35 dB. This indicates that this system achieves excellent reconstruction and visualization results.

The next step is to compare the resistance of the encryption systems to differential attacks. The results are presented in Table 8 where number of pixels change rate (NPCR) and unified average change intensity (UACI) are used as measures. Note that the proposed system has NPCR and UACI values closer to the ideal values than other encryption systems, which indicates the effective resistance to differential attacks.

Table (7): Comparison with other related work corresponding to a single-image encryption.

Ref.	Encryption Techniques	Correlation Coefficient of Adjacent Pixels			Key Space	Entropy	PSNR (dB)	Chaos Type and Degree
		Horizontal	Vertical	Diagonal				
[35]	Digital/Optical (CS, DRPE with FrFT, Confusion/Diffusion)	- 0.0019	0.0051	- 0.0078	2^{400}	7.9984	34.1	4D Memristive
[36]	Digital Scrambling and Diffusion	0.0039	0.0049	- 0.0027	2^{456}	7.9990	-	4D Memristive
[37]	Digital/Optical (Convolutional Neural Network (CNN) with Dynamic Adaptive Diffusion and Dual-Channel Bit-Level Fusion)	0.0086	0.0042	0.0216	2^{624}	7.9986	9.6	5D Hamiltonian Conservative
[38]	Digital (Bidirectional Bit-Level Cyclic Shift and Dynamic DNA-Level Diffusion)	- 0.0036	- 0.0012	0.0024	2^{128}	7.9994	-	3D Memristive
[39]	Digital (Compressive Sensing, Premutation, and Bidirectional Z-Shaped Diffusion)	- 0.0015	-0.0072	0.0007	2^{399}	7.9987	33.6	4D Based on The Continuous Hopfield Neural Network Model
[40]	Digital (CBC Mode and Reversible Steganography with Premutation and Diffusion)	- 0.0105	0.0137	0.0152	2^{199}	7.9992	-	3D (Logistic Map, Chen)
[41]	Digital (Premutation and Diffusion)	- 0.0014	0.0038	- 0.0083	2^{144}	7.9973	10.1	4D Grid-scroll Memristive
[42]	Digital (Confusion and Diffusion)	0.0023	- 0.0024	- 0.0008	2^{512}	7.9973	27.7	5D (Aizawa, Ricker, Sine-Circle, Chirikov)
This Work	Digital	0.0009	- 0.0027	0.0026	2^{2392}	7.9998	40.3	6D GMDS Memristive

Table (8): NPCR and UACI Comparison with other related work.

Ref.	NPCR %	UACI %
[35]	99.6300	33.5700
[37]	99.6033	33.4519
[38]	99.6173	33.4528
[39]	99.6101	33.8414
[40]	99.6000	33.4400
[41]	99.6063	33.4607
[42]	99.6100	33.4000
This work	99.7019	33.5582

6. Conclusions

A 6D memristive chaotic system has been proposed by combining three grid multi-double-scroll memristive CSs of dimensions 5, 6, and 7 and used to assist the operation of a proposed color image encryption/decryption scheme. The combined CS passes successfully the NIST randomness test and offers an encryption key space of 2^{2392} which is the highest compared with that reported in the literature. The encryption scheme adopts chaos-assisted four sequential digital stages which improves the security level of image data significantly. This is done by exploiting the unique characteristics of the proposed CS to produce encryption patterns that are difficult to predict and, therefore, more resistant to various types of attacks.

7. References:

[1] B. Xu, X. Luo, Y. Wang, L. Bai, K. Chen, and J. Zhao, "A 4D trigonometric-based memristor hyperchaotic map to ultra-fast PRNG," *IEEE Trans. Ind. Informatics*, vol. 20, no. 6, pp. 8673–8683, June 2024, doi: 10.1109/TII.2024.3372017.

[2] W. Alexan *et al.*, "Triple layer RGB image encryption algorithm utilizing three hyperchaotic systems and its FPGA implementation," *IEEE Access*, vol. 12, art. no. 3446733, pp. 118339–118361, August 2024, doi: 10.1109/ACCESS.2024.3446733.

[3] M. N. E. Farandi, A. Marjuni, N. Rijati, and D. R. I. M. Setiadi, "Enhancing image encryption security through integration multi-chaotic systems and mixed pixel-bit level," *Imaging Sci. J.*, art. no. 2398954, pp. 1–18, August 2024, doi: 10.1080/13682199.2024.

[4] V. Dhakshinamoorthy, G. C. Wu, and S. Banerjee, "Chaotic dynamics of fractional discrete time systems," *CRC Press*, 2024. doi: 10.1201/9781003425113.

[5] C. C. Ilie, Z. S. Schrecengost, and E. M. van Kempen, " Nonlinear dynamics and chaos", *CRC Press*, 2022. doi: 10.1201/9781003365709-9.

[6] W. Yun, C. Qian, L. Bo, and H. Chen-yang, "A tri-valued memristive chaotic system with hidden attractors and its image encryption application," *Eur. Phys. J. B*, vol. 97, no. 3, February 2024, doi: 10.1140/epjb/s10051-024-00662-y.

[7] Z. Fan, X. Sun, J. Zhao, C. Zhang, and B. Du, "Dynamics analysis and feasibility verification of a 3D discrete memristive chaotic map with multi-vortex-like volume behavior," *Chaos, Solitons and Fractals*, vol. 185, art. no. 115070, p. 115070, May 2024, doi: 10.1016/j.chaos.2024.115070.

[8] C. Wang, D. Tang, H. Lin, F. Yu, and Y. Sun, "High-dimensional memristive neural network and its application in commercial data encryption communication," *Expert Syst. Appl.*, vol. 242, art. no. 122513, pp. 1-12, November 2023, doi: 10.1016/j.eswa.2023.122513.

[9] R.Ding *et al.*, "Parametric controllable planar multi-scroll chaotic attractors in a 3-D memristive tabu learning single neuron model," *Biochem. J.*, vol. 1, art. no. 131150, pp. 1–21, May 2024.

[10] L. Xiong, X. Wang, X. Zhang, and T. He, "Dynamic behavior analysis, color image encryption and circuit implementation of a novel complex memristive system," *Optoelectron. Lett.*, vol. 20, no. 3, pp. 183–192, March 2024, doi: 10.1007/s11801-024-3096-3.

[11] D. Ding *et al.*, "Extreme multi-stability and microchaos of fractional-order memristive Rulkov neuron model considering magnetic induction and its digital watermarking application," *Nonlinear Dyn.*, vol. 112, no. 17, pp. 15523–15545, April 2024, doi: 10.1007/s11071-024-09610-y.

[12] J. Venkatesh *et al.*, "A fractional-order memristive two-neuron-based Hopfield neuron network: dynamical analysis and application for image encryption," *Mathematics*, vol. 11, no. 21, October 2023, doi: 10.3390/math11214470.

[13] Y. Cao, Z. Li, and S. He, "Complex hidden dynamics in a memristive map with delta connection and its application in image encryption," *Nonlinear Dyn.*, vol. 112, no. 9, pp. 7597–7613, January 2024, doi: 10.1007/s11071-024-09344-x.

[14] X. Leng, X. Wang, and Z. Zeng, "Memristive Hopfield neural network with multiple controllable nonlinear offset behaviors and its medical encryption application," *Chaos, Solitons and Fractals*, vol. 183, art. no. 114944, , pp.1-11, May 2024, doi: 10.1016/j.chaos.2024.114944.

[15] Q. Lai, L. Yang, G. Hu, Z. H. Guan, and H. H. C. Iu, "Constructing multiscroll memristive neural network with local activity memristor and application in image encryption," *IEEE Trans. Cybern.*, vol. 54, no. 7, pp. 4039–4048, January 2024, doi: 10.1109/TCYB.2024.3377011.

[16] M. Hu, X. Huang, Q. Shi, F. Yuan, and Z. Wang, "Design and analysis of a memristive Hopfield switching neural network and application to privacy protection," *Nonlinear Dyn.*, vol. 112, no. 14, pp. 12485–12505, April 2024, doi: 10.1007/s11071-024-09696-4.

[17] Q. Deng, C. Wang, and H. Lin, "Memristive Hopfield neural network dynamics with heterogeneous activation functions and its application," *Chaos, Solitons and Fractals*, vol. 178, art. no. 114387, January 2024, doi: 10.1016/j.chaos.2023.114387.

[18] Z. Liu, C. Wu, J. Wang, and Y. Hu, "A color image encryption using dynamic DNA and 4-D memristive hyper-chaos," *IEEE Access*, vol. 7, art. no. 2922376, pp. 78367–78378, June 2019, doi: 10.1109/ACCESS.2019.2922376.

[19] F. Yu *et al.*, "Chaos-based application of a novel multistable 5D memristive hyperchaotic system with coexisting multiple attractors," *Complexity*, vol. 2020, art. no. 8034196 ,pp. 1-19, March 2020, doi: 10.1155/2020/8034196.

[20] F. Yu *et al.*, "A 6D fractional-order memristive Hopfield neural network and its application in image encryption," *Front. Phys.*, vol. 10, art. no. 847385, pp. 1–14, March 2022, doi: 10.3389/fphy.2022.847385.

[21] N. A. Khan, M. A. Qureshi, and N. A. Khan, "Evolving Tangent Hyperbolic memristor based 6D chaotic model with fractional order derivative:

Analysis and applications," *Partial Differ. Equations Appl. Math.*, vol. 7, art. no. 100505, pp. 1-15, March 2023, doi: 10.1016/j.padiff.2023.100505.

[22] L. Kou *et al.*, "Data encryption based on 7D complex chaotic system with cubic memristor for smart grid," *Front. Energy Res.*, vol. 10, art. no. 980863, pp. 1–13, September 2022, doi: 10.3389/fenrg.2022.980863.

[23] S. Fu, Z. Yao, C. Qian, and X. Wang, "Star memristive neural network: dynamics analysis, circuit implementation, and application in a color cryptosystem," *Entropy*, vol. 25, no. 9, August 2023, doi: 10.3390/e25091261.

[24] Q. Lai, Z. Wan, H. Zhang, and G. Chen, "Design and analysis of multiscroll memristive Hopfield neural network with adjustable memductance and application to image encryption," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 34, no. 10, pp. 7824–7837, October 2023, doi: 10.1109/TNNLS.2022.3146570.

[25] F. Li, L. Bai, Z. Chen, and B. Bao, "Scroll-growth and scroll-control attractors in memristive bi-neuron Hopfield neural network," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 71, no. 4, pp. 2354–2358, April 2024, doi: 10.1109/TCSII.2023.3331058.

[26] Q. Lai and Y. Chen, "Multi-scroll attractor and its broken coexisting attractors in cyclic memristive neural network," *Chaos*, vol. 33, no. 8, August 2023, doi: 10.1063/5.0159391.

[27] H. Lin, C. Wang, C. Xu, X. Zhang, and H. H. C. Iu, "A memristive synapse control method to generate diversified multistructure chaotic attractors," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 42, no. 3, pp. 942–955, March 2023, doi: 10.1109/TCAD.2022.3186516.

[28] Q. Lai, Y. Liu, and Z. Chen, "Multiscroll chaos and extreme multistability of memristive chaotic system with application to image encryption," *J. Vib. Eng. Technol.*, vol. 12, no. 3, pp. 3487–3505, June 2024, doi: 10.1007/s42417-023-01060-x.

[29] Q. Lai and Z. Chen, "Grid-scroll memristive chaotic system with application to image encryption," *Chaos, Solitons and Fractals*, vol. 170, art. no. 113341, pp. 1-19, December 2023, doi: 10.1016/j.chaos.2023.113341.

[30] Q. Lai, Z. Wan, and P. D. K. Kuate, "Generating grid multi-scroll attractors in memristive neural networks," *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 70, no. 3, pp. 1324–1336, March 2023, doi: 10.1109/TCSI.2022.3228566.

[31] M. Es-Sabry *et al.*, "Securing images using high dimensional chaotic maps and dna encoding techniques," *IEEE Access*, vol. 11, art. no. 3315658, pp. 100856–100878, September 2023, doi: 10.1109/ACCESS.2023.3315658.

[32] F. Yu *et al.*, "Chaos-based engineering applications with a 6D memristive multistable hyperchaotic system and a 2D SF-SIMM hyperchaotic map," *Complexity*, vol. 2021, art.no. 6683284, March 2021, doi: 10.1155/2021/6683284.

[33] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Opt. Laser Technol.*, vol. 101, pp. 30–41, January 2018, doi: 10.1016/j.optlastec.2017.10.024.

[34] M. S. Hasan, A. Dhungel, P. S. Paul, M. Sadia, and M. R. Hossain, "Normalized linearly-combined chaotic system: design, analysis, implementation, and application," *IEEE Open J. Ind. Electron. Soc.*, vol. 4, art. no. 3328497, pp. 486–505, November 2023, doi: 10.1109/OJIES.2023.3328497.

[35] Y. Du et al., "Optical image encryption algorithm based on a new four-dimensional memristive hyperchaotic system and compressed sensing," Chinese Phys. B, vol. 32, no. 11, pp. 1–20, May 2023, doi: 10.1088/1674-1056/acef08.

[36] L. Xiong, X. Wang, X. Zhang, and T. He, "Dynamic behavior analysis, color image encryption and circuit implementation of a novel complex memristive system," Optoelectron. Lett., vol. 20, no. 3, pp. 183–192, March 2024, doi: 10.1007/s11801-024-3096-3.

[37] Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, "Double image encryption algorithm based on neural network and chaos," Chaos, Solitons and Fractals, vol. 152, art. no. 111318, pp. 1-16, August 2021, doi: 10.1016/j.chaos.2021.111318.

[38] K. Qian et al., "A novel image encryption scheme based on memristive chaotic system and combining bidirectional bit-level cyclic shift and dynamic DNA-level diffusion," Front. Phys., vol. 1, art. no. 963795, pp. 1–19, August 2022, doi: 10.3389/fphy.2022.963795.

[39] M. Gong, X. Chai, Y. Lu, and Y. Zhang, "Exploiting four-dimensional chaotic systems with dissipation and optimized logical operations for secure image compression and encryption," IEEE Trans. Circuits Syst. Video Technol., vol. 43, art. no. 3375868, pp. 1-14, March 2024, doi: 10.1109/TCSVT.2024.3375868.

[40] W. Song et al. , "A fast parallel batch image encryption algorithm using intrinsic properties of chaos," Signal Process. Image Commun., vol. 102, art. no. 116628, pp. 1-10 , January 2022, doi: 10.1016/j.image.2021.116628.

[41] Q. Lai and Z. Chen, "Grid-scroll memristive chaotic system with application to image encryption," Chaos, Solitons and Fractals, vol. 170, art. no. 113341, pp. 1-17, March 2023.

[42] E. Güvenoğlu, "An image encryption algorithm based on multi-layered chaotic maps and its security analysis," Conn. Sci., vol. 36, no. 1, pp. 1-32, February 2024, doi: 10.1080/09540091.2024.2312108.