Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 7, No. 4, December 2019, pp.1607-1617

An enhanced hybrid image encryption algorithm using Rubik's cube and dynamic DNA encoding techniques

Alaa A. Abdullatif[1], Firas A. Abdullatif[1], Sinan A. Naji[2]
[1] Department of Computer Science, College of Education for Pure Sciences, University of Baghdad, Iraq
[2] Department of Postgraduate Studies, University of Information Technology and Communications, Baghdad, Iraq

ABSTRACT

Image encryption is among the most active solutions to protect confidential pictorial information. However, to design a strong image encryption algorithm with no recognizable pattern, the researchers in this field have to enrich the confusion and diffusion properties. This study proposes an efficient hybrid system that combines two techniques. First, we propose a modified version of Rubik's Cube technique for scrambling colored image pixels to achieve fast confusion. This technique not only scrambles the position of image pixels but also scrambles the color channels. Then, dynamic DNA encoding algorithm is used to encrypt the pixel's values. DNA encoding rules are used in conjunction with a secret key. We propose to select the DNA rules dynamically to enhance the security level. Five fidelity metrics are employed to assess the capability of this system. These are PSNR, SSIM, NPCR, Entropy, and CCA. The results indicate that the proposed system enhances the general security requirements with enriched confusion and diffusion properties of the encrypted image.

Keywords: Image Encryption, Rubik's Cube technique, DNA encoding.

Corresponding Author:

Alaa A. Abdullatif,
Department of Computer Science, College of Education for Pure Sciences,
University of Baghdad, Iraq
E-mail: alaa.a.h@ihcoedu.uobaghdad.edu.iq

1. Introduction

Image encryption is a crucial issue in storing and exchanging different types of digital images. The main goal of any information security system is to protect confidential information against unauthorized access and attacks [1, 2]. Currently, we are generating a huge number of images. Governments and organizations have to deal with many sensitive and confidential images such as surveillance images, crime scene images, photos of suspects, military images, classified documents, medical images, etc. that should be stored, processed, and transmitted securely [3, 4].

Although many methods have been proposed in the literature to protect pictorial information, image encryption is among the most active solutions to protect confidential pictorial information [5, 6]. In recent years, image encryption has gained much interest and has been studied by mathematicians, information technology specialists, and engineers. However, encrypting data could attract the immediate attention of a third party.

The term *Image Encryption* can be defined as follows: "Given an arbitrary image, the goal of image encryption is to convert the pictorial information of the image into a certain encoded format, seemingly unreadable or a meaningless image, so that only authorized persons can access, process, and recognize it".

Although many existing studies have shown that the conventional textual encryption algorithms like RSA, IDEA, ElGamal, DES, etc. can be successfully used for image encryption applications [5, 7-13], numerous recent studies have shown that text-based encryption approaches do not efficiently encrypt images because of high computational cost and low level of security due to the following reasons [2, 14, 15]: (1) the huge amount of data in the ordinary images. With the current technologies, an image may contain millions of

pixels; (2) the high redundancy of information in images; (3) the high correlation between neighboring similar pixels that constitute perceptually meaningful entities [4, 9]. On the other hand, encrypting digital images is less sensitive than encrypting textual data due to the fact that any slight change in the pixel's intensity value will produce indistinguishable change in pixel appearance and it remains difficult for the human vision system to detect the slight change in pixel appearance due to the fact that the amount of the change is still so small that it does not alter the whole scene of the image. Numerous image encryption techniques are presented in the literature. These techniques can be grouped into three main categories [4, 5, 16, 17]:

1. **Textual-based Techniques:** These techniques are based on directly converting a 2D or 3D image into a 1D stream of data and this stream is encrypted using classical text encryption algorithms such as DES, RSA, Blowfish, etc. [5, 8-13].
2. **Visual-based Techniques:** These techniques have their basis in directly altering the image's visual contents. These techniques are grouped into these categories: confusion methods, diffusion methods, and their combination structure. The confusion methods only shuffle (i.e., permute) the locations of the image pixels [5, 18-20]. Although such methods are very fast, the main drawback is that the pixel's intensities remain the same. Thus, the histogram of the input image is identical to that of the corresponding encrypted image. This weakens such methods against statistical attacks.
   The diffusion methods are based on directly altering the pixel's values that cause a dramatic change in the pictorial information of the image. To achieve better performance, both methods (i.e., confusion and diffusion) are combined in one system. Thus, the pixels' positions and values are both altered.
3. **Hybrid Techniques:** Hybrid systems combine two or more different cryptographic techniques to enhance the security level. Generally, hybrid systems imply extra computational cost. For any proposed system, a trade-off is inevitable between the security requirements versus speed.

However, to design a strong image encryption algorithm with no recognizable pattern, the researchers in this field have to enrich the confusion and diffusion properties [21]. In recent years, image encryption using DNA principles has received increasing attention and constituted a new research direction [2, 14, 21]. DNA computing may comprise natural biological and algebraic operations to achieve a high level of diffusion [22, 23]. However, the principle of the Rubik's cube is employed in many studies to achieve fast confusion [24, 25].

This study proposes an efficient hybrid system for image encryption that combines two techniques: A modified Rubik's cube and dynamic DNA algorithms. Generally, combining different methodologies in one integrated system where one method can compensate for the weaknesses of the other to enhance the general security level.

The remaining part of this study is structured as follows: Section 2 presents the Rubik's cube technique. Section 3 introduces dynamic DNA encoding algorithms, while Section 4 discusses the proposed algorithm. Section 5 introduces fidelity measures and Section 6 provides the experimental results. Lastly, Section 7 presents the conclusion.

2. Rubik's Cube Algorithm

Rubik's Cube is a 3D structure toy that tests one's cleverness and skills. It was devised in 1975 by Erno Rubik [26]. Up to 2009, it was estimated that more than 350 million pieces were distributed around the world that makes it one of the best-selling games [27].

Inspired by the high similarity between the permutation of the Rubik's Cube and encryption, many of Rubik's Cube-based approaches have been presented in the literature for encrypting images [24, 25, 28, 29]. Although the Rubik's Cube is an order list with 54 fields (i.e., 6x9 values) that can be cracked within a limited time, applying the basic operations (such as face rotation, cube turns, and the combinations of these) makes it an interesting method for image pixels permutation due to the fact that colored images consist of millions of pixels and each one can take a random color in a set of more than 16 million colors.

Loukhaoukha et al. offered an early image encryption technique using Rubik's Cube technique [25]. The image pixels are shuffled repeatedly based on the basic operations of Rubik's cube. Using two predefined keys, XOR bitwise operator is fused with the odd rows and columns. Following this, these keys are flipped and XOR bitwise operator is fused with the even rows and columns. Diaconu et al. proposed a technique based on a modified Rubik's Cube together with a digital chaotic cipher [30]. The pixels are shuffled with Rubik's cube principle. Then, the chaos-based cipher is used for encrypting the image pixels. Helmy et al.

introduced a technique on the basis of the Rubik's cube in conjunction with RC6 algorithm for encrypting a group of images [24]. First, The RC6 is used to encrypt six images separately. These images are utilized to be the six faces on the cube. Then, Rubik's cube algorithm is applyied for additional permutation.
Practically, Rubik's cube algorithm is used as an essential step to add a high degree of permutation by scrambling the position of the image pixels. In general, digital images are arrays of numbers. The gray-scale images are represented as 2D matrix while colored images, such as RGB images, are represented as 3D matrix. Although most of the images that we want to deal with are color images, the classical Rubik's Cube algorithm is used with gray-scale images [25] [28].

3. Dynamic DNA Encoding

Deoxyribonucleic Acid (DNA) is defined as "a molecule that contains the genetic information of organisms" [23, 31]. Four biochemical molecules named: Adenine, Cytosine, Thymine, and Guanine (i.e., A, C, T, and G) comprises the code that represent the genetic information. Naturally, these molecules appear in pairs where A and T are complementary, and G and C are also complementary. The order that they appear is called the DNA sequence. Because biological operations act on all of them in parallel, many studies showed that DNA encoding provides a promising direction for developing fast encryption schemes using basic operations such as the ADD, SUB, and XOR [22, 23, 32, 33]. Therefore, we can define DNA cryptography as: "the field of studying how to apply DNA principles as an encoder and information carrier".
With digital data, the 0 and 1 are complements (i.e., inverse code), 10 and 01 are complements, and finally, 11 and 00 are also complements. If the encoding basics (i.e., A→00, C→01, G→10, T→11) are used and we consider and consider A↔T and C↔G are complements, then we get eight coding rules as shown in Table 1 [22, 23, 32, 33]. With DNA computing developments, the algebraic operations based on DNA sequence can be applied directly in binary. For example, Tables 2, 3, and 4 show the ADD, SUB, and XOR operations using rule No. 1. The foremost benefit of DNA encryption is the ability of hardware-based parallel implementation. Corresponding to the types of DNA rules shown in Table 1, there are eight kinds for each operation. For instant, there are eight types of DNA XOR. Thus, 24 types of encoding rules can be obtained; but the program must fulfil the complements A↔T and C↔G pairing rules. For example, suppose we have two DNA sequences [ATGC] and [CATG], by applying the XOR operation to these sequences using rule no. 1; the resultant sequence is [CTCT]. The XOR operation is reflexive and thus we can easily retrieve [ATGC] by fusing the resulted [CTCT] and [CATG] with XOR operation. Obviously, it is a fast cryptographic method in comparison with other cryptographic methods that imply complex mathematical operations.

Table 1. DNA encoding rules

Molecules	Rule No.							
	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01
T	11	11	10	10	01	01	00	00

Table 2. The ADD operation for DNA sequences based on Rule 1

ADD	A	C	G	T
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

Table 3. The SUB operation for DNA sequences based on Rule 1

SUB	A	C	G	T
A	A	T	G	C
C	C	A	T	G
G	G	C	A	T
T	T	G	C	A

Table 4. The XOR operation for DNA sequences based on Rule 1

XOR	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

Generally, the DNA-based image encryption methods can comprise three main steps as follows [14]: (1) convert the input image into DNA sequences array based on the DNA principles; (2) encrypt the image's DNA sequences using basic DNA operations in conjunction with a predefined key; (3) convert the resulting DNA sequences array into an encrypted image. Zhang et al. presented a DNA-based technique along with chaotic maps [34]. First, the pixels are shuffled using chaotic maps. Then, pixels values are encoded into DNA sequences array. Each sequence is converted into a random number of time(s) by a sequence of repeated calculations according to Chebyshev's chaotic map. Shehab et al. described an encryption method that combines DNA principles and round-reduced AES cryptographic algorithm [35]. Wu et al. suggested an encryption scheme based on combining DNA principles and multiple 1D chaotic systems [14]. First, three 1D chaotic systems are used to generate the key stream. Secondly, convert the key stream and then input image into the DNA arrays. Thirdly, XOR bitwise operations are applied to the DNA arrays. Then, the DNA arrays are fragmented into blocks which are randomly permuted. Finally, XOR and ADD operations are applied to these DNA arrays. Enayatifar et al. presented a hybrid encryption model on the bases of DNA masking, logistic maps, and genetic algorithms (GA) [36]. The DNA encoding and logistic maps are used to create a set of DNA masks while the GA is utilized to determine the best mask for encryption. More DNA-based image encryption schemes are presented in [21, 23, 37-39].

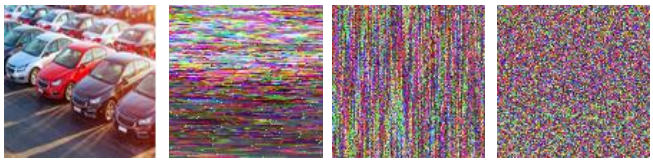
Up to date, although there has been much research devoted to image encryption techniques, there has seen limited research on how to evaluate these techniques. In most previous works, researchers performed tests and experiments using their own test images. The traditional method is done based on statistical metrics (see Section 5). Another frequently used approach is the subjective evaluation, in which a human visually makes a comparison of the encryption results for various techniques.

4. The Proposed Algorithm

The proposed hybrid image encryption algorithm comprises two main phases: First, a modified Rubik's cube encryption is employed to shuffle the pixels (i.e., confusion). Next, a dynamic DNA algorithm is applied to provide an enhanced level of encryption (i.e., diffusion).

4.1 The Modified Rubik's Cube Encryption

The Rubik's cube encryption in this work was originally inspired by the well-known pioneering algorithm developed by Loukhaoukha et al. [25], but has the following valuable improvements: (1) the classical Rubik's Cube algorithm was originally designed to encrypt gray-scale images. The approach developed in the current study is used for encrypting colored images. Hence, our approach not only shuffles the position of image pixels but also shuffles the color channels. This significantly improves the confusion against statistical and brute-force attacks; (2) the classical algorithm uses two keys for encrypting image pixels directly, while our approach employs two randomization keys, which are mined from the input image itself by collecting the most significant bit of image pixels using zigzag path. Based on these keys, the shuffling will be applied three rounds on face rotation, left turns, and right turns. Fig. 1 presents the shuffling outcomes of the proposed Rubik's Cube algorithm.



(a) (b) (c) (d)

Figure 1. Applying Rubik's Cube algorithm: (a) Input image, (b) Shuffling the rows, (c) Shuffling the columns, and (d) Shuffling the rows and columns.

Although the resulting image looks perfect, the confusion techniques only exchange the locations of the image pixels and channels while the intensities remain the same. Consequently, the dominant intensities remain dominant in the resulting encrypted image. For example, if the input image tends to dark, the corresponding encrypted image will also tend to be dark. Therefore, using confusion techniques alone is not enough even though they are simple and fast techniques. To enhance performance, the system should be augmented with other techniques. In this study, the Rubik's cube algorithm is augmented with dynamic DNA algorithm.

4.2 Dynamic DNA algorithm

Unfortunately, many previous works used DNA encoding rules in a systematic manner. The main drawback of such algorithms is that they can be effortlessly hacked by attackers as they work in a systematic way.
In this study, we propose using dynamic DNA rules which are dynamically selected according to a predefined key. This makes the system more secure against various attacks. For example, a pixel value can correspond to any of the four digital values. Every two binary bits of these values can then use a random encoding rule, which makes the key space larger, more difficult to decipher, and with a higher image encryption security. The general step-by-step algorithm at the sender's end (i.e., encryption part) is listed as follows:

The Proposed Algorithm (Encryption Part)

Input : A true color image I of size $(M \times N \times 3)$
Output: Encrypted image E

Begin

1. Construct randomization keys from most significant bit of I to get row_key[N] and column_key[M].
2. Apply Rubik's Cube algorithm to scramble image's pixels;
3. Hide the randomization keys in the resultant image to get (*I1).*
4. Generate 16 random numbers as a private Key called K.
5. Apply DNA coding for K called K_{DNA}.
6. For L=1 to 3 // the three components of RGB image (Red, Green, and Blue).
   For i=1 to N
   For j= 1 to M
   Select the DNA substitution rule (R)
   R= ((i * j * K [j]) modulo 8) + 1
   Convert the *I1*[i, j] into DNA code by
   rule (R).
   Apply dynamic DNA operations with K_{DNA} [j] based on (R).
   End //for j
   End //for i
   End // for L
7. Convert the DNA sequences into Encrypted Image E (Decoding).
8. Output Encrypted Image E.

End

At the receiver end, the receiver will use the encrypted image and the above-mentioned parameters to retrieve the original image. Therefore, the algorithm is its own inverse.

5. Fidelity measures

Fidelity measures are defined as "the type of metrics utilized to evaluate the performance of the proposed algorithm". Generally, these metrics calculate the difference level between two images. The most used fidelity measures are:

5.1 Peak Signal to Noise Ratio (PSNR)

The PSNR represents the peak error. It is calculated as follows [40-42]:

$$PSNR = 10\ log_{10}\frac{R^2}{MSE} \quad (1)$$

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j) - E(i,j)]^2 \quad (2)$$

where m and n are the image dimensions, R is the highest value of the pixels' intensities. The mean square error (MSE) represents the cumulative squared error (i.e., pixel differences) between the two images. The lower PSNR implies better encryption algorithm.

5.2 Number of Pixels' Change Rate Analysis (NPCR)

The NPCR represents the proportion of the number of pixels that are changed in comparison with the original input image. The NPCR is calculated as follows [14, 43, 44]:

$$D(i,j) = \begin{cases} 0, & if\ I(i,j) = E(i,j) \\ 1, & if\ I(i,j) \neq E(i,j) \end{cases} \quad (3)$$

$$NPCR = \left(\frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n} D(i,j) \right) \times 100 \quad (4)$$

where m and n are the image dimensions. The NPCR is in range [0,100]. The higher NPCR closer to 100 implies better encryption algorithm.

5.3 Entropy

Information entropy $E(m)$ represents the information randomness. It is calculated as follows [14]:

$$E(m) = \sum_{i=0}^{2^n-1} P(m) log_2 \frac{1}{P(m_i)} \quad (5)$$

where $P(m_i)$ is the probability of the m_i. Practically, $E(m)$ is in range [0,8]. The higher $E(m)$ closer to 8, implies better encryption algorithm.

5.4 Correlation Coefficient Analysis (CCA)

The CCA represents the amount of linear correlation between two pixels at the same indices in the two images. The CCA is calculated as follows [2, 3, 35]:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (6)$$

$$cov(x,y) = \frac{1}{n}\sum_{1}^{n}(x_i - E(x))(y_i - E(y)) \quad (7)$$

$$E(x) = \frac{1}{n}\sum_{1}^{n} x_i \quad (8)$$

$$D(x) = \frac{1}{n}\sum_{1}^{n}(x_i - E(x))^2 \quad (9)$$

The CCA is in range [-1,1]. The closer the value of r to zero implies better encryption algorithm.

5.5 Structural Similarity Index Measure (SSIM)

Inclusion of a recent measure such as SSIM can provide a fair comparison along with PSNR, NPCR, Entropy, and CCA. The SSIM is regarded as one of the most powerful methods of assessing the visual closeness of images, which can be calculated as follows [45]:

$$\text{SSIM(x,y)} = \frac{(2\,\mu_x\,\mu_y + C_1)\,(2\,\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (10)$$

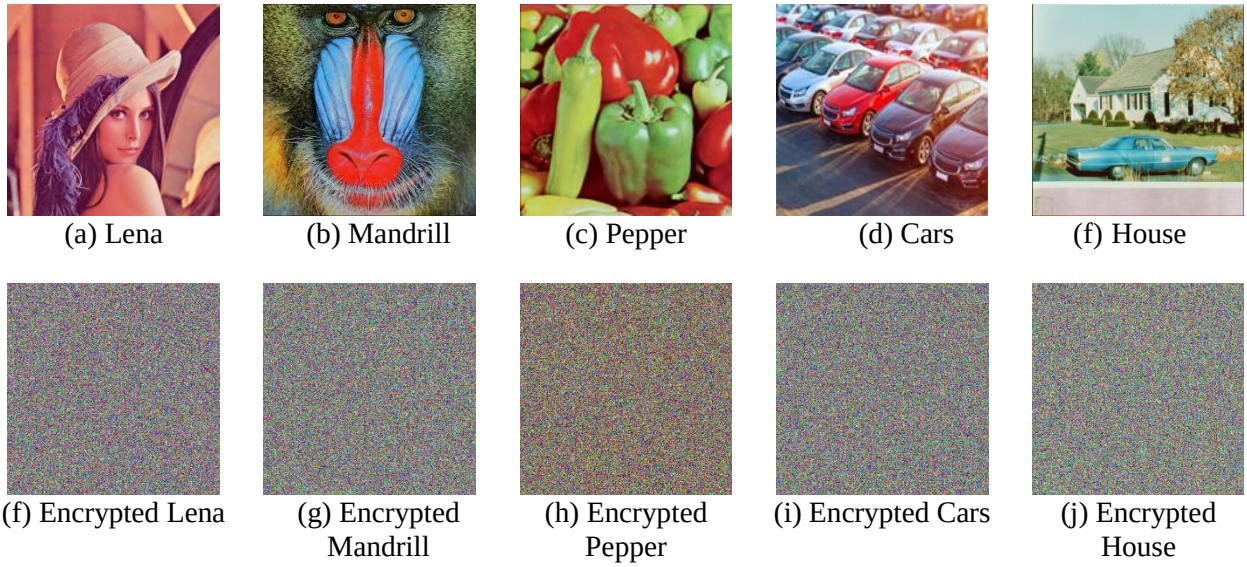
where μ is the mean intensity, σ is the standard deviation, C_1 and C_2 are constants > 0 that are included to avoid instability when $\mu_x, \mu_y, \sigma_{xy}, \mu_x^2, \mu_y^2, \sigma_x^2, \sigma_y^2$ are very close to zero. The SSIM is in range [-1,1]. The higher SSIM close to 1, implies high visual closeness between the two images. The lower SSIM implies better encryption algorithm.

6 Experimental Results

The experimental results provided in this section show the performance of the proposed technique. The experiments were conducted using images from two image datasets:

- **Set 1:** The "USC-SIPI image database" of the University of Southern California [46]. It is maintained primarily to support researchers in image processing and machine vision. The database is partitioned into different categories. The "Miscellaneous category" contains famous images such as Lena, Mandrill, Peppers, etc.
- **Set 2:** Our own image dataset comprises a collection from the Internet. This dataset consists of 260 images collected from different sources and includes various image types.

For the qualitative evaluation, Fig. 2 shows examples of applying the proposed technique. Fig. 2(a) presents the input image. Fig. 2(b) provides the resulting encrypted image. As shown in this figure, the encrypted images imply high confusion and randomization with no recognizable pattern.



(a) Lena (b) Mandrill (c) Pepper (d) Cars (f) House

(f) Encrypted Lena (g) Encrypted Mandrill (h) Encrypted Pepper (i) Encrypted Cars (j) Encrypted House

Figure 2. The results of the proposed technique (original test images and the encrypted images).

For quantitative evaluation of the system's output, five fidelity metrics are employed to assess the capability of this technique (see Section 5). The PSNR, SSIM, NPCR, Entropy, and CCA of the experimental results are listed in Table 5, which also exhibits excellent confusion and diffusion features.
For comparison with other works, demonstrates the comparison of NPCR, Entropy, and CCA for a well-known image "Lena" with other techniques presented in [22] [34] [47] [48]. It can be noticed that the results of the proposed system are equivalent or superior to these techniques.

Table 5. The PSNR, SSIM, NPCR, ENTROPY, and CCA of experimental results.

Images	PSNR	SSIM	NPCR	Entropy	CCA
Lena	8.1360	-0.0165	99.765	7.9983	0.0022
Mandrill	7.7846	-0.0344	99.938	7.9865	0.0027
Peppers	8.1245	0.0181	99.881	7.9851	-0.0063
Cars	9.9813	0.0024	99.743	7.9792	0.0034
House	9.2432	0.0012	99.752	7.9969	-0.0041

Table 6. The comparison with other works using a well-known image of "Lena"

Representative Work	NPCR	ENTROPY	CCA
Ref. [22]	99.600	7.9874	−0.0169
Ref. [34]	99.610	7.9980	0.0032
Ref. [47]	99.580	7.9967	0.0021
Ref. [48]	99.650	7.9970	-0.0038
Our System	99.765	7.9983	0.0022

Another measure that can be employed to demonstrate the quality of the encryption process is the image histogram that takes into consideration the statistical analysis of the two images. Fig. 3(a) and Fig. 3(b)

present the histograms of the input and encrypted images, respectively. As shown in these figures, the histograms of the two images differ considerably. Furthermore, the three histograms of the encrypted image imply high randomness. In other words, they do not offer any indication to be used by statistical attacks.

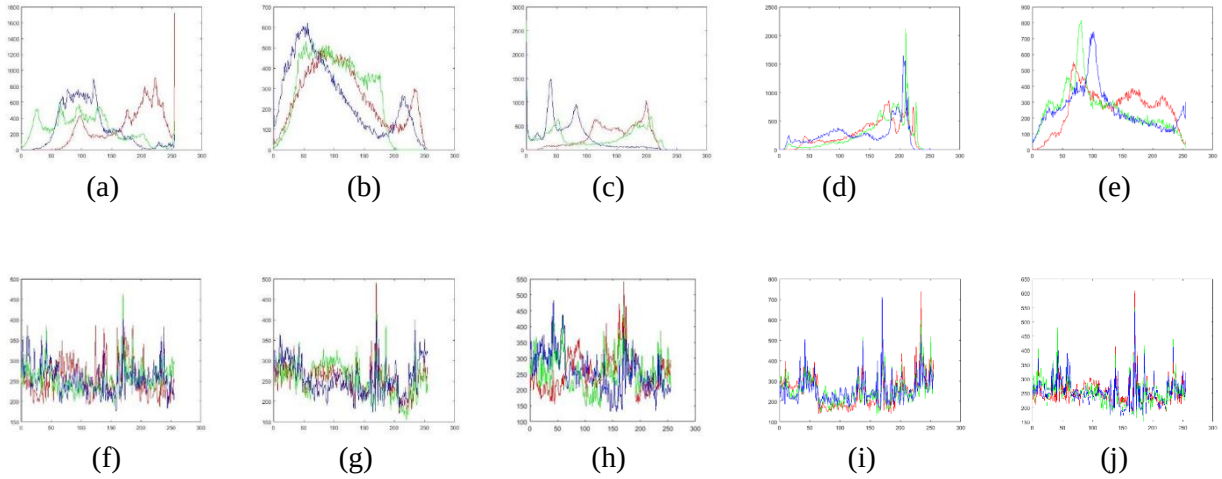


Figure 3. The histograms of images: (a) Histogram of Lena, (b) Histogram of Mandrill, (c) Histogram of Pepper, (e) Histogram of House, (f) Histogram of encrypted Lena, (g) Histogram of encrypted Mandrill, (h) Histogram of encrypted Pepper, (i) Histogram of House.

7. Conclusions

Information security (IS) is an essential issue in storing and exchanging of information between different parties. Nowadays, a huge number of digital images is generated every moment and the security of these images is becoming increasingly significant. In this study, we propose an efficient hybrid image encryption approach based on the basis of DNA sequence operations in conjunction with an adapted Rubik's cube algorithm. In general, the use of different approaches in one integrated system, where one approach can compensate for the weaknesses of another will improve the general performance of the system. The main contribution of this approach is its robustness because retrieving the original image without knowing the structure of the proposed system is really difficult.

The experimental results showed that the proposed system achieves a substantial security improvement with low computation cost. In general, bitwise processing enhances the performance in accordance to speed since the basic DNA encoding rules are based on the basic algebraic operations that offer high-speed encryption compared to the complex mathematical operations that other techniques use. Thus, the proposed system is appropriate for many practical applications.

For further development, future works may include hardware implementation for instant image encryption designed for mobile devices and digital cameras to keep one's private images more securely and free from risk of loss or attack.

References

[1] V. Pachghare, *Cryptography and information security*. PHI Learning Private Limited, Delhi, India, Second Edition, 2015.

[2] J. Zhang, D. Hou, and H. Ren, "Image encryption algorithm based on dynamic DNA coding and Chen's hyperchaotic system," *Mathematical Problems in Engineering*, vol. 2016, 2016.

[3] O. S. Faragallah *et al.*, *Image encryption: a communication perspective*. CRC Press, 2013.

[4] K. D. Patel and S. Belani, "Image encryption using different techniques: A review," *International Journal of Emerging Technology and Advanced Engineering*, vol. 1, no. 1, pp. 30-34, 2011.

[5] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Processing*, vol. 141, pp. 109-124, 2017.

[6] A. Uhl and A. Pommer, *Image and video encryption: from digital rights management to secured personal communication*. Springer Science & Business Media, 2004.
[7] A. A. Al-lehiebe, "Ciphered Text Hiding in an Image using RSA algorithm RSA," J . Coll. Educ. Women, vol. 26, no. 3, pp. 879–884, 2015.
[8] I. A. Taqi and S. M. Hameed, "A new Color image Encryption based on multi Chaotic Maps," Iraqi J. Sci., vol. 59, no. 4, pp. 2117–2127, 2018.
[9] Z. Yun-Peng, L. Wei, C. Shui-Ping, Z. Zheng-Jun, N. Xuan, and D. Wei-di, "Digital image encryption algorithm based on chaos and improved DES," presented at the 2009 IEEE International Conference on Systems, Man and Cybernetics, 2009.
[10] G. Zhao, X. Yang, B. Zhou, and W. Wei, "RSA-based digital image encryption algorithm in wireless sensor networks," presented at the 2010 2nd International Conference on Signal Processing Systems, 2010.
[11] Q. Gong-bin, J. Qing-feng, and Q. Shui-sheng, "A new image encryption scheme based on DES algorithm and Chua's circuit," presented at the 2009 IEEE International Workshop on Imaging Systems and Techniques, 2009.
[12] A. El-Deen, E. El-Badawy, and S. Gobran, "Digital image encryption based on RSA algorithm," *J. Electron. Commun. Eng*, vol. 9, no. 1, pp. 69-73, 2014.
[13] L. Li, A. A. A. El-Latif, and X. Niu, "Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images," *Signal Processing*, vol. 92, no. 4, pp. 1069-1078, 2012.
[14] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Applied Soft Computing*, vol. 37, pp. 24-39, 2015.
[15] L. Krikor, S. Baba, T. Arif, and Z. Shaaban, "Image encryption using DCT and stream cipher," *European Journal of Scientific Research*, vol. 32, no. 1, pp. 47-57, 2009.
[16] M. Hussain; and M. Hussain, "A Survey of Image Steganography Techniques," *International Journal of Advanced Science and Technology*, vol. 54, no. May, 2013.
[17] A. Baby and H. Krishnan, "Combined Strength of Steganography and Cryptography-A Literature Survey," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 3, 2017.
[18] T. Gao and Z. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, solitons & fractals*, vol. 38, no. 1, pp. 213-220, 2008.
[19] G. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme," *Optics Communications*, vol. 284, no. 12, pp. 2775-2780, 2011.
[20] Z. Tang, X. Zhang, and W. Lan, "Efficient image encryption with block shuffling and chaotic map," *Multimedia tools and applications*, vol. 74, no. 15, pp. 5429-5448, 2015.
[21] A. Akhavan, A. Samsudin, and A. Akhshani, "Cryptanalysis of an image encryption algorithm based on DNA encoding," *Optics & Laser Technology*, vol. 95, pp. 94-99, 2017.
[22] H. Liu and X. Wang, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457-1466, 2012.
[23] O. F. Rashid, Z. A. Othman, and S. Zainudin, "A novel DNA sequence approach for network intrusion detection system based on cryptography encoding method," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 7, no. 1, pp. 183-189, 2017.
[24] M. Helmy, E.-S. M. El-Rabaie, I. M. Eldokany, and F. E. A. El-Samie, "3-D Image Encryption Based on Rubik's Cube and RC6 Algorithm," *3D Research*, vol. 8, no. 4, p. 38, 2017.
[25] K. Loukhaoukha, J.-Y. Chouinard, and A. Berdai, "A secure image encryption algorithm based on Rubik's cube principle," *Journal of Electrical and Computer Engineering*, vol. 2012, p. 7, 2012.
[26] T. de Castella, "The people who are still addicted to the Rubik's Cube," *BBC News Magazine. bbc. com. Retrieved*, vol. 28, 2014.
[27] A. Jamieson, "Rubik's cube inventor is back with Rubik's 360," *The Daily Telegraph*, 2009.
[28] K. Abitha and P. K. Bharathan, "Secure Communication Based on Rubik's Cube Algorithm and Chaotic Baker Map," *Procedia Technology*, vol. 24, pp. 782-789, 2016.
[29] S. Kilaru, Y. Kanukuntla, A. Firdouse, and M. Bushra, "effective and key sensitive security algorithm for an image processing using robust Rubik encryption and decryption process," *University of Birmingham, ISSN (Print)*, vol. 2, pp. 2278-8948, 2013.
[30] A.-V. Diaconu and K. Loukhaoukha, "An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher," *Mathematical Problems in Engineering*, vol. 2013, 2013.

[31] A. K. Kaundal and A. Verma, "DNA based cryptography: a review," *International Journal of Information and Computation Technology*, vol. 4, no. 7, pp. 693-698, 2014.
[32] Y. Zhang and L. H. B. Fu, "Research on DNA cryptography," presented at the Applied cryptography and network security, 2012.
[33] X. Zhang, F. Han, and Y. Niu, "Chaotic image encryption algorithm based on bit permutation and dynamic DNA encoding," *Computational intelligence and neuroscience*, vol. 2017, Article ID 6919675, 2017.
[34] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical and Computer Modelling*, vol. 52, no. 11-12, pp. 2028-2035, 2010.
[35] E. Shehab, A. K. Farag, and A. Keshk, "An Image Encryption Technique based on DNA Encoding and Round-reduced AES Block Cipher," *International Journal of Computer Applications*, vol. 107, no. 20, 2014.
[36] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83-93, 2014.
[37] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Journal of Systems and Software*, vol. 85, no. 2, pp. 290-299, 2012.
[38] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 73, pp. 53-61, 2015.
[39] L. Liu, Q. Zhang, and X. Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map," *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1240-1248, 2012.
[40] G. N. Mohammed, A. A. H. Al-fatlawi, and A. T. Kamil, "Combined DWT-DISB based image watermarking optimized for decision making problems," Period. Eng. Nat. Sci., vol. 7, no. 3, pp. 1009–1020, 2019.
[41] S. I. M. Ali, M. G. Ali, L. Abd, Z. Qudr, and S. I. M. Ali, "PDA : A private domains approach for improved msb steganography image," Period. Eng. Nat. Sci., vol. 7, no. 3, pp. 1405–1411, 2019.
[42] M. J. Aqel, A. Umar, and M. Agoyi, "A performance Evaluation of Transform Domain Algorithm in Watermarking Based on Different Levels of Sub-Bands of Discrete Wavelet Transform," Periodicals of Engineering and Natural Sciences, vol. 7, No. 2, PP. 546–554, 2019.
[43] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31-38, 2011.
[44] G. Yang, H. Jin, and N. Bai, "Image encryption using the chaotic Josephus matrix," *Mathematical Problems in Engineering*, vol. 2014, 2014.
[45] K. Rao and H. Wu, "Structural similarity based image quality assessment," in *Digital Video image quality and perceptual coding*: CRC Press, 2005, pp. 261-278.
[46] The USC-SIPI image database [Online] Available: http://sipi.usc.edu/database/
[47] C. Song and Y. Qiao, "A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos," *Entropy*, vol. 17, no. 10, pp. 6954-6968, 2015.
[48] C.-Y. Song, Y.-L. Qiao, and X.-Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos," *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 18, pp. 3329-3334, 2013.