Basrah Journal for Engineering Sciences, Vol. 23, No. 1, (2023), 56-63

Review Article

Journal homepage: www.bjes.edu.iq
ISSN (Online): 23118385, ISSN (Print): 18146120

OPEN ACCESS

A Comprehensive Review of Color Image Encryption Technology

Alyaa I. Dawood [1,*], Qabeela Q. Thabit [2], Taqwa O. Fahad [3]

[1] *Engineering Technical College-Basrah, Southern Technical University, Basrah, Iraq*
[2] *Basrah Education Directorate, Ministry of Education, Basrah, Iraq*
[3] *Biomedical Engineering Department, University of Technology-Iraq, Bagdad, Iraq*
E-mail addresses: alyaa.dawood@stu.edu.iq , qabelh2010@gmail.com , taqwa.o.fahad@uotechnology.edu.iq
Received: 15 November 2022; Accepted: 1 January 2023; Published: 2 July 2023

Abstract

Today, with the continuous increase in the use of computer networks and the rapid evolution of information technologies. The secure transmission of data over the Internet has become an urgent necessity to preserve the privacy of users and protect sensitive information from theft and distortion. images are most of this transferred data, so it was necessary to protect it by encrypting them using algorithms that ensure the protection of information access to the receiver. Color images contain sensitive information and details that must be secured and protected. This paper produces a comprehensive review of image encryption methods and classifies them based on various concepts such as chaotic maps, DNA, etc. with comparisons between existing approaches to accessing different security parameters. Additionally, the types of encryption keys were reviewed along with some common types of attacks and the most important methods for measuring encryption efficiency.

Keywords: Security, Encryption, Decryption, Cipher, Encryption key, Attacks.

https://doi.org/10.33971/bjes.23.1.8

1. Introduction

Image cryptography plays a critical role in ensuring image transmission security and storage through internet networks. However, image encryption faces significant challenges due to the large amount of data involved. Cyber security protection plays an essential role and is one of the crucial issues in medical, air, military and private meetings that may contain classified information [1]. Digital color images are an important issue in modern communications, as the information contained in the images has increased at this stage, and they are used as the main vector file for transmitting information [2].

Most of the present encryption algorithms for text data are used to encrypt images directly. These algorithms are often not suitable as the decrypted text is required to be equal to the original text. This condition is unnecessary for image encryption, whereas the image size is often larger than the text size [3]. Encryption is defined as converting an ordinary message by a lock called a key into a cipher text that unreadable by anyone without decrypting it, while decryption is the process of transforming a cipher text into the original text, so that it can be read again [4]. Secret keys play a critical part in the encryption process. Due to the fact that security encryption relies mostly on secret keys, there are two types, private and public keys [5]. Several studies have sought to develop theories for encrypting images and making them more complex [1-5], while others tend to complicate the key that decrypts images [6].

In this research, the basic concepts of the image encryption process will be presented, the types of attack to which images are exposed, and the most important research conducted in this field.

2. Basic terms and encryption, decryption block diagram

The block diagram in Fig. 1 illustrates the basic terms of the image encryption process and described as follows [7]:

1. Input image: It is the original image that contains information that needs to be secured during its transmission thru the public network, also known as a normal image.
2. Cipher image: It is the original image itself changed into an unreadable form by encryption, also called an encrypted image.
3. Encryption: The transformation process of the plain image into a cipher image by a method of encryption and secret key.
4. Decryption: On the receiving side, the normal image is retrieved from the encrypted image using a decryption approach and a secret key.
5. Key: The cryptographic security approach mainly depends on the secret key, there are two types: a private and a public key. The key is required for both encryption and decryption to work. The security of information always requires strong keys.

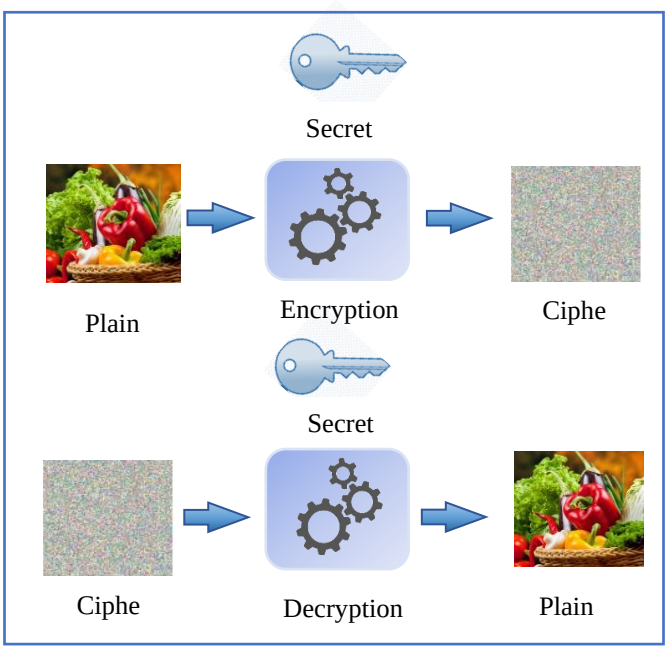

Fig. 1 Block diagram of encryption (sender side)/ decryption (receiver side) process.

3. Image encryption

Image data has special characteristic such as visualization, a large amount of data, high level redundancy, and high pixels' correlation. Encryption techniques are very useful tools for protecting confidential information. Therefore, several methods have been proposed to securely encrypt and decrypt image data. There are several operations available for image encryption, based on how pixels are dealt with such as scrambling, diffusion, shuffling, rotation, substitution, confusion, and transposition [8]. Diffusion and permutation are quite popular due to their effectiveness and ease of implementation. Scrambling is accomplished by relocating the position of the pixel [9] while diffusion involves changing their values or blending them together for more robustness [10]. An image encryption algorithm can be categorized into two broad types: a full encryption algorithm and a partial encryption algorithm (selective encryption) which are classified according to the domain orientation. The domains are either spatial, frequency or mixed of them (hybrid domain) [11].

3.1. Full encryption vs partial encryption

Full encryption algorithms deal with the whole image and encrypt the entire image. Image encryption relies on information secrecy, therefore the balance between encrypted data confidentiality is critical, encryption efficiency, time, and cost are the challenges still faced in image encryption [11]. A full encryption algorithm is more computationally complex than a partial encryption algorithm, since encryption-decryption will take longer, and therefore, it is suitable in military and law enforcement applications [12].

Partial encryption techniques encrypt a portion of an image rather than the entire image using a region of interest (ROI). Partial encryption algorithm can be used to encrypt the desired portions of an image such as the least or most significant bits of the bitplanes. Visual Cryptographic Algorithms (VC) also fall into this category Partial Cryptographic Algorithms: Partial image encryption techniques separating information by perception into sensitive and insensitive data [11]. Due to the fact that only the lowest part of the data is encrypted, the partial encryption algorithms have greatly reduced the computational requirements, which makes it very suitable for applications that do not require large data [13]. Both a full encryption algorithm and a partial encryption algorithm are categorized according to the domain orientation which are either spatial, frequency or mixed of them (hybrid domain).

3.1.1. Spatial domain

In the spatial domain method, the pixels that are the details of the image are taken into account and various actions are applied directly to these pixels [14]. An image's spatial domain corresponds to its position in the scene. The position changing in the image corresponds to a changing in the scene that is mean the distances in pixels in the image agree with the actual distances in the scenes (for example, in meters).

3.1.2. Frequency domain

The frequency encryption schemes, every change in the coefficients in the transformation domain results in changing all the pixel values in the spatial domain of the image [6], therefor many researches have turned to the frequency domain, which is considered the most efficient domain [15].

3.1.3. Hybrid domain

Hybrid domain encryption, it is a mix of spatial and frequency domains [16]. It achieves higher security by combining the precision of spatial domain algorithms and the effectiveness of frequency domain algorithms [17].

4. Encryption key

In the field of cryptography, in order for the encryption process to be more robust, a strong encryption key must be present. The encryption is divided according to the type of the key into two main types:

1. Secret key (symmetric) cryptography.
2. Public key (asymmetric) cryptography.

In a secret cryptography, both parties (the sender and receiver) know the same private key. Messages are decrypted by the receiver with the same key as they are encrypted by the sender [17]. A pair of keys are used when using public key encryption, anyone can encrypt messages but only those who know the private key can decrypt and retrieve the original message. [18]. The following section outlines the most common theories

5. Encryption algorithms

A color image encryption system based on compressed sensing and a multi-image cross-pixel scrambling approach was proposed in [19]. The color image is decomposed firstly into three sub-images (R, B, and G), then they are processed sparsely by the discrete wavelet transform, and the different Gaussian random matrices are used to observe them. The multi-image cross-pixel scrambling approach is used in the final encryption process.

Li et al. [20] use a hyperchaotic system and apply a transforming- scrambling-diffusion model to encrypt the color images. The chaotic sequence is constructed from the 4D hyperchaotic system by successively converting each pixel of the simple image into gray code, then scrambling it. A one-dimensional matrix is created from the pixel matrix using the gray code transformation. To finish the entire domain of

scrambling, the chaotic sequence was moved around and arranged in a one-dimensional matrix in the appropriate way. Later, an image diffusion bit operation was performed. By using matrix transformation, the cipher picture can be recreated.

Choi et al. [21] design an algorithm to encrypt medical images. The proposed algorithm consists of two phases. A Combined Cellular Automata algorithm (CoCA) was used to change the pixel values of a plane image in the first phase. The second step entails moving every pixel in the 3D generalized chaotic cat map used to encrypt the image. Three colored channels can be altered in a color space, and they can also simultaneously impact how pixels are positioned in two dimensions-vertically and horizontally. To raise the security level of the encryption system, the pixel shuffling step is repeated n times. When the plane image is combined with the key image created by two CoCAs, the pixel values are modified at random, producing a far better outcome. If a damaged portion of an encrypted image was broadcast on purpose, it won't be recoverable after decryption if it was destroyed by unexpected noise or accidentally transmitted a 3D chaotic cat map that is generally.

DNA algorithm with the spatiotemporal chaotic system is used in [22] to encrypt color images. The distribution information of the plain image was hidden, by using three levels of DNA matrices based on the random DNA encoding principles to transform the basic image. A scrambling matrix created by a mixed linear-nonlinear linked map lattice system is used to combine and permute these matrices. DNA deletion-insertion operations are used to decompose the scrambled matrix into three matrices. The three contents of matrices are encrypted using DNA randomly decoding rules and then recombine into three cipher image channels. Additionally, other studies looked at how DNA can be used for variety of purposes, including but not limited to text and digital data encoding and not just images [23].

A Chaos-based color image encryption technique in [24] presented utilizing a 3D histogram equalization method that equalizes chaotic sequences histograms of Lorenz systems. A histogram-equalization by Lorenz and Rossler-systems is used in order to achieve the confusion and diffusion of image data. A confusion stage involves scrambling the colored pixels of the input image, whereas a diffusion stage involves replacing those pixels with scrambled images and sequences of the Rossler-system. Overall security analysis of the scheme indicated that the scheme is more confidential and resistant to classical attacks.

As it is introduced in [25], hybrid parallel chaotic maps for image encryption have a common security issue, which is their small key space. Moreover, they use hybrid technique of Discrete Wavelet Transform in addition to permutation and diffusion chaotic function to combine these maps in order to improve the execution and quality of the encryption. While [26] use three-dimension chaotic mapping to overcome chaotic complexity and security vulnerabilities shortcoming in low dimension based chaotic maps.

In [27] proposed an encryption scheme by using DNA sequence and DCT transform. The scheme applied complex biological operation and improved the diffusion ability of image encryption. The encryption scheme consists of three phases-setup of secret- key, DCT, and encryption process. In first phase a key image generation based on a random image generated using a random generator and then using the random function to generate an integer matrix. The secret image key obtained based on DNA sequence. The plane image was divided it into (R, G, B) layers and applied DCT to gain coefficient matrices on each layer, these coefficients should be quantized based on JPEG compression standard matrix. The DCT coefficients are encoded into DNA sequences matrices and scrambled using XOR operation, finally all layers of image were accumulated to create the encrypted image

Noura et al. [28], propose an algorithm uses a hybrid 2D chaotic map combined with a sine - cosine cross-chaotic map. The algorithm depends on the confusion and diffusion phases. Pixel shuffling is implemented by 2D sin-cosine crosschaotic map generation in the confusion phase. The final encrypted image for the diffusion phase was generated by bitwise XORing the scrambled image with a chaotic self-diffusion matrix generated by a 1D Logistic Tent map. A cipher image and key are supposed to have as complex a relationship as possible under confusion. A cipher image is created by making each bit depend on multiple parts of the key, which conceals the relationship between the two. The cipher image can therefore be difficult to retrieve the key from.

The SinePiecewise is a linear chaotic map proposed in [29] to make improvements in the characteristics of the original chaotic map which uses a method of 10-bit representation and varied DNA coding, providing better dynamic performance and larger parameter space. Basically, the encryption algorithm has four parts. The key streams are generated in the first part, followed by shuffling step, where each pixel in the image has two processes by DNA algorithm (encryption and decryption), whereas two of five DNA nucleotides will undergo a third encryption and decryption, the last part is the XOR operation.

Deep learning-based color image encryption is one of the methods Liu et al. [30] offer for block-based key embedding. To guarantee the complexity of the generated key, a deep learning model is paired with a chaotic system. A neural network model is used to forecast the initial chaotic sequence, and the key information produced by the prediction is then encrypted into the color image in blocks and layers. The color image encryption scheme splits the color image into three color matrices (R, G, and B). Three new chaotic key sequences are predicted and generated by a neural network, embedded in blocks of three-color matrices, and then scrambled and diffused to create the final encrypted image.

Cheng et al. [31] proposed a color image encryption algorithm using a two-dimensional chaotic system (2D Sin-Cos-Henon (2D-SCH)). It is a hyperchaotic system that uses random scrambling and localization diffusion for color image encryption. SHA512 (Secure Hash Algorithm) was used at first for generating the secret key. The secret key generates chaotic sequences, which are used later to design the random scrambling. As a result, the image diffuses around two initial points generated by the secret key. The system has a short implementation time where the three channels of the color image are encrypted simultaneously.

In [32], a novel Twin Attractor Chaotic (TAC) system was proposed analyzed using the Lyapunov stability and Power spectrum analysis, which yields two attractors possessing complex dynamics while revising parameters. Color images are encrypted using pixel-level confusion and diffusion schemes. The original image matrix separated in to three channels (R, G, B). The TAC system used for two different chaotic attractors, called TAC-Nak and TACNas attractors,

both of which have the same three-dimensional equations but different parameter values. The encryption phase produces a complex state of encryption model with different parameters. Encryption phase was divided into three states, in first state the key was generated, and then both the row and column are ordered to create pixel-level confusion. The third state diffusion row and column were performed the final encrypted image.

The final encrypted image, Xu et al. [33] proposed an algorithm in combination with Rabinovich hyper-chaos to be applied to compressive sensing purpose. A DWT transform will be applied to the plaintext image to transform it into a sparse form. A circular diffusion operation is performed by double reset of the bit plane and the function of encryption engine with an improved hyperchaotic sequence. As a final step, the compressed sensing sampling of the encrypted image will be performed by the combined random Gaussian measurement matrix. Double reset chaotic operations are performed to change the position of each pixel of and a function of encryption engine is introduced to obfuscate the pixel values fully. The algorithm was found to be well resistant to differential attacks, statistical attacks, and brute force attacks.

In [34], Wang et al. proposed an image encryption scheme uses a complex network to generate the pixel values of the encryption sequences in order to shuffled the bit-level, while scrambling the pixel positions by the chaotic sequences that generated by a neural network with time-delayed. The key space is greatly expanded by using a time-delayed network and a multistable hyper-chaotic network as a nodal model. Decryption and encryption sequences are generated by selecting different nodes within the complex network. Twenty nodes are used to achieve the synchronization accuracy necessary for correct decryption.

A Hopfield neural network with a bidirectional flipping algorithm was proposed in [35] for image encryption. The plaintext image was segmented into blocks, then a block scrambling was applied to the resulting image. The scrambling process was provided by flipped block bidirectionally. A hash algorithm was applied to determine the initial values chaotic system. Through diffusion transformation, Hopfield neural network optimized a diffusion matrix to derive a ciphertext image.

6. Performance analysis

An encryption system must be secure against all types of file attacks currently known. The next section outlines the most common types of tests used for testing cryptosystems.

6.1. Key space

The key space analysis depicts the possibility of acquiring an encryption key by applying all the possible keys [36] Security image encryption systems require a large key space. A high level of security is achieved by using a key space larger than 2100, which is composed of the initial conditions of the chaotic system and seed keys. The key space is 252 bytes for the most popular double-precision floating-point format known as binary64 (according to the IEEE 754 standard) [37]. A simple comparison of key space shown in Table 1.

Table 1. Key space comparison for the works discussed in [21-32].

Ref.	Algorithm	Key space
21	3D Generalized Chaotic Cat Map and Combined Cellular Automata	2^{416}
22	DNA encoding and spatiotemporal chaotic system	2^{213}
24	3D Lorenz-3D Roessler chaotic system	2^{548}
26	3D Piecewise-Henon Map	2^{216}
27	SPWLCM and DNA coding	2^{279}
28	Hybrid chaotic map	2^{262}
29	fractional order discrete improved Henon map and Rubik's cube transform	2^{448}
30	Deep Learning and Block Embedding	2^{70}
31	2D Sin-Cos-Henon Map	2^{512}
32	Twin Attractor Chaotic	2^{531}
33	4D Rabinovich hyperchaotic system	2^{1010}

6.2. Key sensitivity analysis

It is a measure of how much variance is present between the encryption and decryption processes. A good encryption algorithm must be enough sensitively to the secret key [38] i.e., changing one bit should yield a completely different encrypted result [39] it is clear shown in Fig. 2. In general, a chaotic cipher's key sensitivity refers to the initial state sensitivity as well as the control parameter sensitivity [40].

6.3. Histogram analysis

An image histogram shows the weight of pixels in an image, which is an important feature of image analysis [38]. Histograms provide information about the tone of an image [24]. Using the histogram, it is possible to intuitively determine how effective the image is at preventing attacks. It is easy to attack the original image which has uneven pixel values distribution [33]. If the distribution values in the histogram are equal or at least close, it indicates that the cipher image has a good frequency distribution as explained in Fig 3.

6.4. Information entropy analysis

Information entropy analysis is used to determine how much the encrypted data is complex [24], in other words, it is used to measure if it is possible to predict or certain the source of information or not. The encoded data is considered too complex to provide information about the original data [37]. A greater entropy of information indicates stronger randomness and a more uniform distribution of gray values, and vice versa. The ideal value must be near to 8, a comparison of information entropy for the algorithms in section 5 shown in Table 2.

6.5. Correlation analysis

Plaintext images are strongly correlated in horizontal, vertical, and diagonal directions. A key requirement of encryption algorithms is to destroy correlations between adjacent pixels [37]. Through the correlation coefficient analysis, two images can be determined to be independent based on the correlation between their pixels. Correlation values that are linear indicate poor independence. The two images are more independent when the correlation values are more nonlinear, thus, a greater correlation between the two images results in a weight that is closer to one; conversely, a greater degree of independence results in a weight that is closer to zero [13].

Table 2. A comparison entropy analysis for the works discussed in [20-34].

Ref.	Algorithm	Entropy
20	Hyperchaotic	7.9991
21	3D Generalized Chaotic Cat Map and Combined Cellular Automata	7.99837
22	DNA encoding and spatiotemporal chaotic system	7.9979
24	3D Lorenz-3D Roessler chaotic system	7.99935
26	3D Piecewise-Henon Map	7.9983
27	SPWLCM and DNA coding	7.9911
28	Hybrid chaotic map	7.9973
29	fractional order discrete improved Henon map and Rubik's cube transform	7.9974
30	Deep Learning and Block Embedding	7.9916
31	2D Sin-Cos-Henon Map	7.9993
33	4D Rabinovich hyperchaotic system	7.9987
34	chaotic neural network	7.9919
35	Hopfield Neural Network and Bidirectional Flipping	7.9988

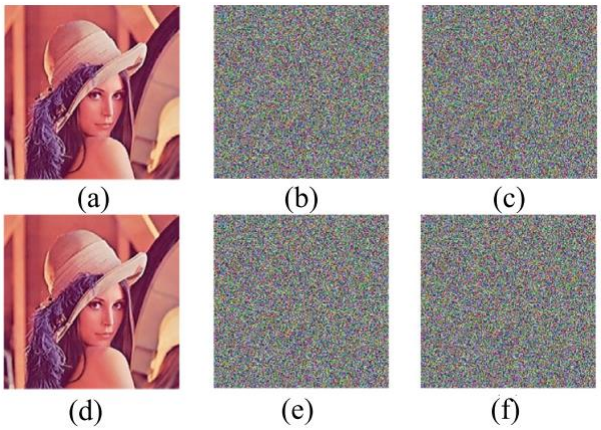

Fig. 2 Effect of key sensitivity: **(a)** Plane image, **(b)** Encrypted image (a) with key k1, **(c)** Encrypted image (a) with key k2, **(d)** Decrypted image (a) with correct key, **(e)** Decrypted image (a) with wrong key k2, **(f)** Decrypted image (a) with wrong key k1 [23].

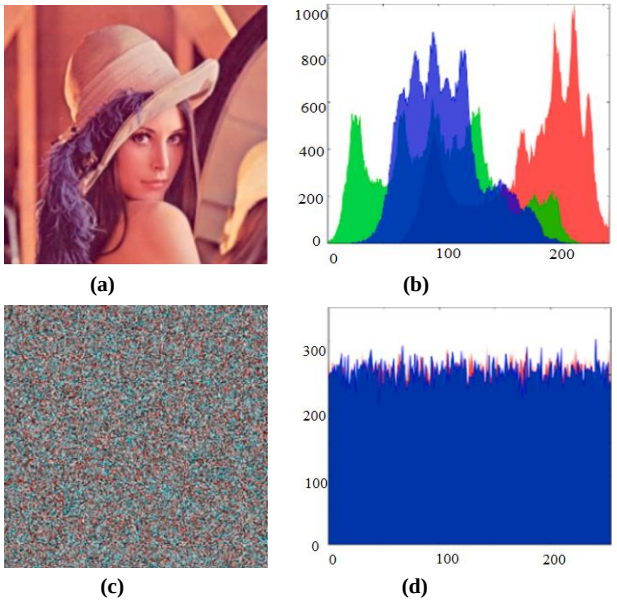

Fig. 3 (a) Plane image, **(b)** Histogram of plane image, **(c)** Encrypted image, **(d)** Histogram of encrypted image [31].

6.6. NPCR and UACI

The number of pixels change rate (NPCR) and unified average changing intensity (UACI) are two performance indices are usually adopted to investigate the impact of a change in 1-bit in the plain image to the corresponding encrypted image [20]. They are calculated as in function (1) and (2):

$$NPCR = \sum_{i,j} \frac{d(i,j)}{m \times n} \times 100\ \% \tag{1}$$

Where,

$$d(i,j) = \begin{cases} 1, & c1(i,j) \neq c2(i,j) \\ 0, & otherwise \end{cases}$$

$$UACI = \frac{1}{m \times n} \sum_{i,j} \frac{|c1(i,j) - c2(i,j)|}{255} \times 100\ \% \tag{2}$$

Where m, n is the height and width of encrypted image ($c2$) while ($c1$) is the plane image. The value of NPCR must be approximately to 99 % while UACI must be near to 33 %. A brief comparison of the above-mentioned algorithms in terms of the common measures used by the researchers was presented in Table 1 showing the strengths and weaknesses of each. Table 2 summarizes the comparison of the algorithms discussed in section 5 for the parameters presents in this section.

7. Resistance to different types of attacks

7.1. Differential attack analysis

Secure image encryption algorithms should be able to withstand differential attacks very well. Attackers may try to change small details in the original image that is used for encryption and compare the difference in results [41] (that is, the original cipher image and the original cipher image with very small changes) thus, the attacker tracks the relationship between the two ciphered images and the original image [42].

7.2. Cropping attack analysis

Cropping attacks are the most common type of attacks. During the transmission of digital images over multimedia, some data may be lost due to congestion in the network or a malicious attack, in which case the pixel value of the missing part will be set to zero [9]. An image encrypted with a non-robust algorithm can lose its original information when decrypted [43].

7.3. Noise attack

Images are mainly polluted by noise during transmission via a public channel, such as Gaussian noise (GN), speckle noise (SN), pepper and salt noise (SPN) [44], which makes image recovery more difficult. In a perfect encryption scheme, noise caused by pixels differing in a decoded image should be minimized. The most common methods for testing cryptographic algorithms are differential attacks and noise attacks.

In some cases, it may be necessary to visually check the robustness of the encryption algorithm and to observe how clear the encrypted images are through the cover.

8. Conclusions

Images are used in a wide variety of fields, such as online learning, engineering, military, research experiments, medical imaging fields, art exhibitions, and marketing. Images are increasingly transmitted and stored digitally, which raises the fundamental issues of confidentiality, integrity, authentication, and non-repudiation of images. In this paper, image encryption techniques in various domains are extensively discussed. In the last years, a detailed survey has been conducted on the most common papers. Some common types of attacks and the types of encryption keys were also briefly discussed. In spite of the fact that many multimedia security algorithms have been developed, they still can't resist all possible attacks within the limits of their capabilities. The methods for picture encryption demanded great levels of confusion, almost no association with the input images, low levels of computing cost, and high levels of resilience to various attacks.

Table 3. A summery comparison for the algorithms discussed in section 5.

Ref.	Algorithm	Parameters					NPCR	UACI
		Correlation			Histogram	Key-sensitivity		
		Horizontally	Vertically	Diagonal				
20	Hyperchaotic	0.0013	0.0015	-0.0024	Uniform	High	99.63	33.52
21	3D Generalized chaotic cat map and combined cellular automata	0.0019	0.0048	-0.0048	Good	-	99.62	33.608
22	DNA Encoding and spatiotemporal chaotic system	R:0.0092 G:0.0002 B:0.0076	R:0.0203 G: -0.0025 B:0.0006	R: -0.0073 G: -0.0131 B:0.0111	Uniform	Very high	99.65	33.457
24	3D Lorenz-3D Roessler chaotic system	R: -0.000006 G: 0.005602 B: 0.000011	R: 0.00010 G: -0.00002 B: 0.00081	R:0.000006 G:-0.000055 B:0.000980	Uniform	Very high	99.67	33.53
25	Coupled chaotic system of piecewise and Henon mapping	-0.0027	-0.0012	-0.0033	Uniform	Very high	99.62	33.41
26	3D Piecewise-Henon map	-0.0012	-0.0027	-0.0033	Uniform	High	99.609	33.463
28	Hybrid chaotic map	R: - 0.0007 G: 0.0003 B: 0.0025	R: - 0.00134 G: 0.0046 B: - 0.0005	R: 0.00231 G: - 0.0056 B: 0.0018	Highly uniform	High	99.61	33.51
30	Deep learning and block embedding	R: - 0.0046 G: - 0.0015 B: - 0.0091	R: 0.0072 G: 0.0056 B: - 0.0076	R: 0.0009 G: - 0.0125 B: - 0.0145	Uniform	-	-	-
31	2D Sin-Cos-Henon map	R:0.0005 G: -0.0009 B: -0.0009	R:0.0002 G:0.0003 B:0.0014	R:0.0001 G: -0.0003 B: - 0.0007	Uniform	-	99.60	33.46
32	Twin attractor chaotic	R:0.0031 G: -0.0046 B: -0.0022	R:0.0076 G: -0.0010 B:0.0038	-	-	-	99.607	33.455
33	4D Rabinovich hyperchaotic system	-0.0021	-0.0787	0.0059	Good	High	99.78	33.37
35	Hopfield neural network and bidirectional flipping	-0.0016	0.0043	-0.0026	-	-	99.609	33.463

References

[1] Y. Xie, J. Yu, S. Guo, Q. Ding, and E. Wang, "Image encryption scheme with compressed sensing based on new three-dimensional chaotic system", Entropy, Vol. 21, No. 9, 2019. https://doi.org/10.3390/e21090819

[2] X. Zhang, L. Wang, Y. Niu, G. Cui, and S. Geng, "Image encryption algorithm based on the H-fractal and dynamic self-invertible matrix", Computational Intelligence and Neuroscience, Vol. 2019, ID 9524080, 2019. https://doi.org/10.1155/2019/9524080

[3] I. S. Rupa, K. Manideep, N. M. Kamale and S. Suhasini, "Information Security using Chaotic Encryption and Decryption of Digital Images", International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), pp. 1-7, 2022. https://doi.org/10.1109/ICSES55317.2022.9914081

[4] M. Karolin, and T. Meyyappan, "Image encryption and decryption using RSA algorithm with share creation techniques", International Journal of Recent Technology and Engineering, Vol. 9, Issue 2, pp. 2797-2800, 2019. https://doi.org/10.35940/ijeat.B4021.129219

[5] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map", Future Generation Computer Systems, Vol. 107, pp. 333-350, 2020. https://doi.org/10.1016/j.future.2020.02.029

[6] G. Ye, K. Jiao, X. Huang, M. Goi, and S. Yap, "An image encryption scheme based on public key cryptosystem and quantum logistic map", Scientific Reports, Vol. 10, 2020. https://doi.org/10.1038/s41598-020-78127-2

[7] M. Kaur, S. Singh, and M. Kaur, "Computational image encryption techniques: a comprehensive review", Mathematical Problems in Engineering, 2021. https://doi.org/10.1155/2021/5012496

[8] T. Li, J. Shi, X. Li, J. Wu, and F. Pan, "Image encryption based on pixel-level diffusion with dynamic filtering and DNA-level permutation with 3D Latin cubes", Entropy, Vol. 21, No. 3, 2019. https://doi.org/10.3390/e21030319

[9] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, "Image encryption and hiding algorithm based on compressive sensing and random numbers insertion", Signal processing, Vol. 172, 2020. https://doi.org/10.1016/j.sigpro.2020.107563

[10] M. Demirtas, "An Image Encryption Method by Sub-image Shuffling, Bit-level Permutation and Diffusion using Chaotic Maps", El-Cezeri, Vol. 9, No. 2, pp. 708-720, 2021. https://doi.org/10.31202/ecjse.995766

[11] U. Zia, M. Mc Cartney, B. Scotney, J. Martinez, M. Abu Tair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains", International Journal of Information Security, Vol. 21, pp. 917-935 2022. https://doi.org/10.1007/s10207-022-00588-5

[12] W. Jang, and S. Y. Lee, "Partial image encryption using format-preserving encryption in image processing systems for Internet of things environment", International Journal of Distributed Sensor Networks, Vol. 16, No. 3, 2022. https://doi.org/10.1177/1550147720914779

[13] S. K. Patel and S. Chandran, "Analysis of Spatial Domain Image Steganography Technique for high-capacity", International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), pp. 1-7, 2022. https://doi.org/10.1109/ACCAI53970.2022.9752614

[14] M. Saikia, B. and Baruah, "Chaotic map-based image encryption in Spatial domain: a brief survey", Proceedings of the First International Conference on Intelligent Computing and Communication, pp. 569-579, 2017. https://doi.org/10.1007/978-981-10-2035-3_58

[15] A. Belazi, A. A. El-Latif, A. V. Diaconu, R. Rhouma, and S. Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms", Optics and Lasers in Engineering, Vol. 88, pp. 37-50. 2017. https://doi.org/10.1016/j.optlaseng.2016.07.010

[16] B. S. Aashiq, and R. A. Amirtharajan, "Robust medical image encryption in dual domain: Chaos-DNA-IWT combined approach", Medical and Biological Engineering and Computing, Vol. 58, pp. 1445-1458, 2020. https://doi.org/10.1007/s11517-020-02178-w

[17] Y. Chen, S. Xie, and J. Zhang, "A hybrid domain image encryption algorithm based on improved henon map", Entropy, Vol. 24, No. 2, 2022. https://doi.org/10.3390/e24020287

[18] S. Kumar, B. K. Singh, S. Pundir, S. Batra, and R. Joshi, "A Survey on Symmetric and Asymmetric Key Based Image Encryption", 2nd International Conference on Data, Engineering and Applications, IEEE, pp. 1-5, 2020. https://doi.org/10.1109/IDEA49133.2020.9170703

[19] S. Yao, L. Chen, and Y. Zhong, "An encryption system for color image based on compressive sensing", Optics and Laser Technology, Vol. 120, 2019. https://doi.org/10.1016/j.optlastec.2019.105703

[20] C. Li, F. Zhao, C. Liu, L. Lei, and I. Zhang, "A hyperchaotic color image encryption algorithm and security analysis", Security and Communication Networks, Vol. 2019, 2019. https://doi.org/10.1155/2019/8132547

[21] U. S. Choi, S. J. Cho, and S. W. Kang, "New Color Image Encryption for Medical Images Based on Three Dimensional Generalized Chaotic Cat Map and Combined Cellular Automata", Advances in Science, Technology and Engineering Systems Journal, Vol. 5, Issue 2, pp. 104-110, 2020. https://doi.org/10.25046/aj050213

[22] K. Xuejing, and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system", Signal Processing: Image Communication, Vol. 80, 2020. https://doi.org/10.1016/j.image.2019.115670

[23] Q. Q. Thabit, A. A. Al-Saffar and I. A. Abed, "A new DNA strand-based encryption algorithm using symmetric key generation table", Al-Qadisiyah Journal for Engineering Sciences, Vol. 15, Issue 1, pp. 32-37, 2022. https://doi.org/10.30772/qjes.v14i4.803

[24] D. S. Malik, and T. Shah, "Color multiple image encryption scheme based on 3D-chaotic maps", Mathematics and Computers in Simulation, Vol. 178, pp. 646-666, 2020. https://doi.org/10.1016/j.matcom.2020.07.007

[25] I. Yasser, F. Khalifa, M. Mohamed, and A. Samrah, "A new image encryption scheme based on hybrid chaotic maps", Complexity, Vol. 2020, Article ID 9597619, Hindawi Publisher, 2020. https://doi.org/10.1155/2020/9597619

[26] C. Liu and Q. Ding, "A Color Image Encryption Scheme Based on a Novel 3D Chaotic Mapping", Complexity, Vol. 2020, Article ID 3837209, 2020. https://doi.org/10.1155/2020/3837209

[27] A. A. Yassin, A. M. Rashid, A. J. Yassin, and H. Alasadi, "A novel image encryption scheme based on DCT transform and DNA sequence", Indonesian Journal of Electrical Engineering and Computer Science, Vol. 21, No. 3, pp. 1455-1464, 2021. https://doi.org/10.11591/ijeecs.v21.i3.pp1455-1464

[28] N. Khalil, A. Sarhan, and M. A. Alshewimy, "An efficient color/grayscale image encryption scheme based on hybrid chaotic maps", Optics and Laser Technology, Vol. 143, 2021. https://doi.org/10.1016/j.optlastec.2021.107326

[29] S. Zhang, and L. Liu "A novel image encryption algorithm based on SPWLCM and DNA coding", Mathematics and Computers in Simulation, Vol. 190, pp. 723-744, 2021. https://doi.org/10.1016/j.matcom.2021.06.012

[30] Y. Liu, G. Cen, B. Xu, and X. Wang, "Color Image Encryption Based on Deep Learning and Block Embedding", Security and Communication Networks, Vol. 2022, Article ID 6047349, 2022. https://doi.org/10.1155/2022/6047349

[31] Z. Cheng, W. Wang, Y. Dai, L. and Li, "2D Sin-Cos-Henon Map for Color Image Encryption with High Security", Journal of Applied Mathematics, Vol. 2022, Article ID 9508749, 2022. https://doi.org/10.1155/2022/9508749

[32] V. Sangavi, and P. Thangavel, "An Exalted Three Dimensional Image Encryption Model Availing a Novel Twin Attractor Chaotic System" Procedia Computer Science, Vol. 204, pp. 728-735, 2022. https://doi.org/10.1016/j.procs.2022.08.088

[33] D. Xu, L. Guodong, X. Wenxia, and W. Chengjing, "Design of artificial intelligence image encryption algorithm based on hyperchaos", Ain Shams Engineering Journal, Vol. 14, Issue 3, 2023. https://doi.org/10.1016/j.asej.2022.101891
[34] S. Wang, H. Ling, and J. Jun, "An image encryption scheme using a chaotic neural network and a network with multistable hyperchaos", Optik, Vol. 268, 2022. https://doi.org/10.1016/j.ijleo.2022.169758
[35] H. Zhang, and S. Yang, "Image Encryption Based on Hopfield Neural Network and Bidirectional Flipping", Computational Intelligence and Neuroscience, Vol. 2022, Article ID 7941448, 2022. https://doi.org/10.1155/2022/7941448
[36] A. Bisht, M. Dua, S. Dua, and P. Jaroli, "A color image encryption technique based on bit-level permutation and alternate logistic maps", Journal of Intelligent Systems Vol. 29, Issue 1, pp. 1246-1260, 2020. https://doi.org/10.1515/jisys-2018-0365
[37] G. Cheng, C. Wang, and H. Chen, "A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture", International Journal of Bifurcation and Chaos, Vol. 29, No. 9, 2019. https://doi.org/10.1142/S0218127419501153
[38] G. Ye, K. Jiao, X. Huang, B. Goi, and W. Yap, "An image encryption scheme based on public key cryptosystem and quantum logistic map", Scientific Reports, Vol. 10, No. 1, pp.1-19, 2020. https://doi.org/10.1038/s41598-020-78127-2
[39] G. K. Shraida,and H. A. Younis, "An Efficient Diffusion Approach for Chaos-Based Image Encryption and DNA Sequences", Iraqi Journal for Electrical and Electronic Engineering, Vol. 18, Issue 2, pp. 69-74, 2022. https://doi.org/10.37917/ijeee.18.2.9
[40] M. Alawida, J. S. Teh, A. Mehmood, and A. Shoufan, "A chaos-based block cipher based on an enhanced logistic map and simultaneous confusion-diffusion operations", Journal of King Saud University-Computer and Information Sciences, Vol. 34, Issue 10, pp. 8136-8151, 2022. https://doi.org/10.1016/j.jksuci.2022.07.025
[41] K. C. Jithin, and S. Sankar, "Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set", Journal of Information Security and Applications, Vol. 50, 2020. https://doi.org/10.1016/j.jisa.2019.102428
[42] M. H. Annaby, M. A. Rushdi, and E. A. Nehary, "Color image encryption using random transforms, phase retrieval, chaotic maps, and diffusion", Optics and Lasers in Engineering, Vol. 103, pp. 9-23. 2018. https://doi.org/10.1016/j.optlaseng.2017.11.005
[43] Z. Chen, Y. Yang, and X. Jiang, "An Image-Encryption Algorithm Based on Stage-Merging Bit Scrambling", Applied Sciences, Vol. 12, No. 14, 2022. https://doi.org/10.3390/app12146972
[44] Y. Zhou, L. Bao, and C. L. Philip Chen, "A new 1D chaotic system for image encryption", Signal Processing Vol. 97, pp. 172-182, 2014. https://doi.org/10.1016/j.sigpro.2013.10.034