Signal Processing 164 (2019) 163–185

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Review

An overview of encryption algorithms in color images

Hossein Movafegh Ghadirli [a], Ali Nodehi [a,*], Rasul Enayatifar [b]

[a] Department of Computer Engineering, Gorgan Branch, Islamic Azad University, Gorgan, Iran
[b] Department of Computer Engineering, Firoozkooh Branch, Islamic Azad University, Firoozkooh, Iran

ARTICLE INFO

Article history:
Received 29 December 2018
Revised 4 June 2019
Accepted 7 June 2019
Available online 8 June 2019

Keywords:
Color image encryption
Image encryption

ABSTRACT

Nowadays, security in data transfer is of special importance. Images are of the most attractive kinds of data in the encryption domain. Color images are more attractive than the gray-level images due to provision of more information. In the present study, various existing color (RGB mode) image encryption schemes have been examined comprehensively based on the application domains in addition to summarizing over 50 studies in this field, most of which being published in the last year. In addition, in this study, color image encryption has been categorized into ten schemes, then the proposed schemes have been compared and their advantages and limitations have been highlighted. Moreover, a complete list of common security analysis techniques for (gray or color) image encryption has been discussed which are capable of evaluating the method potential resistance to different possible attacks. The present study has been carried out to provide detailed knowledge regarding the existing image encryption schemes in the area of the RGB images. Finally, in the current study, various open issues and research directions have been considered in order to explore the promising areas for future developments.

1. Introduction

Data transmission on various communication networks has led to the sensitivity of the security of multimedia data. Previously, text encryption was conducted through methods such as RSA (developed by Rivest, Shamir and Adleman), Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA), however image encryption differs from text encryption as some intrinsic characteristics including high redundancy or bulky data capacity are merely present in images [1]. In addition, text encryption methods lacked sufficient speed and power in diffusing and shuffling the image data [2]. Digital images carrying a huge volume of information account for large proportion [3]. Overall, there are two main approaches exploited to protect digital images: information hiding including watermarking, anonymity, steganography, and cover channel, and encryption including conventional encryption and other methods such as chaotic encryption [4].

Mehra et al. [5–7] presented a modified fusion technique in wavelet transform domain. In their proposed method, low and high frequency components are merged together to improve the image content. Also unlike optical asymmetric encryption technique based on phase- and amplitude-truncation approach, it generated four asymmetric keys corresponding to each image.

One of the chaotic encryption techniques is presented in [8] in which Rehman et al. provided a new approach based on the Logistic Chaotic Map, Burger Map and dynamic substitution boxes. Their proposed method ensures a high security for gray images to be used in insecure communication channels. In [9] a light-weight encryption method for digital images is presented in which TD-ERCS chaos map and XOR operation are used. Also Khan et al. [10] proposed a new method for encryption of the images whose pixels are intrinsically correlated. In fact, the difference between their algorithm and existing methods was the use of chaotic confusion and diffusion to eliminate all dependencies between pixels. In similar attempts, other methods [11] and [12] were presented to improve the security of the encryption algorithm by enhancing the confusion step using Lorenz, Gingerbreadman, Skew Tent map and Hénon Map algorithms. Another chaos-based encryption method is proposed in [13]; it is based on three main components: chaotic maps (nonlinear chaotic algorithm and logistic map), discrete cosine transform (DCT) and orthogonal matrix (via Gram-Schmidt process). The experiments results have shown that this algorithm is capable of coping with various types of attacks. Adding DNA encoding to the PWLCM chaos Liu et al. [14] tried to improve the confusion and diffusion phases of their presented algorithm. In their technique, the number of iterations is not constant and is determined by Chebyshev maps.

In September 2018, a search was carried out by the researchers on the important keywords associated with image encryption in databases such as ACM Digital Library, Elsevier, Google Scholar, IEEE Xplore, Scopus, Springer link, and Wiley online. The search

* Corresponding author.
E-mail addresses: hossein.movafegh@gmail.com (H.M. Ghadirli), alinodehi@hotmail.com (A. Nodehi).

https://doi.org/10.1016/j.sigpro.2019.06.010
0165-1684/

Table 1
Results of search based on various keywords related to image encryption (2005–2018).

Keywords	ACM DL	Elsevier	Google Scholar	IEEE Xplore	Scopus	Springer Link	Wiley Online
Audio Encryption	3518	27	83	22	39	5	0
Image Encryption	8367	1058	5540	1007	2633	409	18
Text Encryption	6108	137	128	1094	159	1	1
Video Encryption	8463	95	586	928	163	24	3

results in Table 1 indicated the fact that the number of studies related to image encryption was much higher than those on the text, audio, and video encryption. In this study, some image encryption methods have been reviewed on the basis of the popularity, specific usages, citations, novelty, etc.

Different classifications have been proposed for image encryption techniques; however they have been classified into 10 main techniques in the current study. In Section 4, these techniques will be described as color image encryption based on chaos, permutation, optical, deoxyribonucleic acid (DNA) based, frequency, hash based, evolutionary, bit plane, double (multiple)-image, scrambling.

Color images are more attractive than the gray-level images due to provision of more information; so far, a lot of studies have been accomplished in the field of color image encryption [1,15–17]. Algorithms of the color image encryption can be classified into two main categories based on different spatial and transformed domains. Three color channels including red, green, and blue channels are considered in encrypting the color images which are calculated independently in the majority of the color image encryption algorithms.

The color plain image P has a size of $H \times W$, with W and H being respectively the width and height of the image. The value of each pixel consists of R, G, and B (red, green, and blue, respectively) color components. Thus, the color image can be transformed into three gray images depending on its color planes, with the size of matrix of each color (R, G, or B) as $H \times W$.

As it is illustrated in Fig. 1, the color Lena image (Fig. 1(a)) with size of 512 × 512 is the color original image with red, green, and blue components shown in Fig. 1(b)–(d), respectively. The value of each gray pixel ranges from 0 to 255; in addition, each pixel can be converted to a 8-bit binary value, obtained by Eq. (1) [18].

$$f(x,y) = p_{(8)}p_{(7)}p_{(6)}p_{(5)}p_{(4)}p_{(3)}p_{(2)}p_{(1)} \quad (1)$$

In which, f(x,y) is the value of the pixel at coordinates of (x, y). Therefore, a color image P with a size of $H \times W$ can be expanded to three binary images of R_b, G_b, and B_b with a size of $H \times 8W$. Integrating the binary matrices of R_b, G_b, and B_b vertically leads to matrix P_b with 3H rows and 8W columns [18]; moreover, the size of each color's (R, G, or B) matrix is obtained as $M \times N$.

In this paper, we had a comprehensive review on different categories of image encryption techniques and realized that these categories would be more popular among researchers. Therefore, we focused our attention on describing these ten schemes.

Section 2 presents a brief review of image encryption and its techniques. Then, the proposed categorization for color image encryption schemes has been introduced in Section 3 in addition to the summary of some of the studies which have used these schemes. Accordingly, all common performance metrics in image encryption have been described in Section 4, and then the selected articles and 10 proposed schemes have been compared in the second part of Section 4. Section 5 has discussed the extent of application of the proposed schemes in recent years. Finally, the future directions in the area of color image encryption and conclusion have been introduced in Section 6.

2. Image encryption: a brief review

Image encryption is the process of hiding images from unauthorized access using a secret key. Digital visual data are organized into rectangular array frames. Members of an array are denoted as pixels, each pixel being a numerical value. With the development of information technologies (IT), the digital images, which are a format of information, such as medical images, grayscale images, color images, binary images, etc., have been increasingly applied, stored, and transmitted. Thus, protection of this type of information is a critical challenge [19]. Taking into account the characteristic of the image data, numerous existing image encryption algorithms have been suggested on the basis of different technologies, including SCAN [20,21], circular random grids [22,23], elliptic curve ElGamal [24], gray code [25], wave transmission [26], vector quantization [27], fractional wavelet transform [7,28,29], p-Fibonacci transform [30], and chaos [1,19,31–33].

The studies presented in the field of image encryption have been explained in the following. Table 2 indicates a comparison among various encryption techniques and their performance taking into account various parameters. Security of a cryptographic algorithm is measured and laid into three levels as Low (L), Medium (M), and High (H). If the cryptographic scheme is not secure against cryptanalysis attacks, then security is assessed to be low. If cryptographic scheme is secure against some of the cryptanalysis attacks then its security is evaluated as moderate, and finally, if it is robust against all cryptanalysis and special attacks, then the scheme is assessed to be highly secure.

In this section, a review of the literature on various image encryption techniques has been presented with tabular form. The existing studies on (color) image encryption have been listed in Table 3.

Fig. 1. Color original image of 'Lena' image including (a) Color plain image, (b) Red component, (c) Green component, and (d) Blue component. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

Table 2
Some image encryption techniques.

Author(s)/reference	Year	Encryption algorithm	Security	Advantages
Chen et al. [34]	2015	A dynamic state variables selection	H	• Plain image sensitive, • Efficient.
Chen et al. [35]	2015	Gray-code based permutation	H	• Highly secure, • Efficient.
Chen et al. [36]	2015	Chaos-base using nonlinear inter-pixel computing and swapping based permutation	H	• Highly secure, • Suitable for practical secret applications.
Chen et al. [37]	2015	Multi-beams interference principle and vector composition	H	• No decrypted image can be obtained until all the keys are rightly used.
Murillo-Escobar et al. [16]	2015	Based on total plain image characteristics and 1D logistic map with optimized distribution based on Murillo- Escobar's algorithm	H	• Easy to implement, • Ideal for fast encryption. • Good against attacks. • Useful for real time applications.
Enayatifar et al. [38]	2015	A hybrid model of the Tinkerbelowl chaotic map, deoxyribonucleic acid (DNA) and cellular automata (CA)	H	• Highly secure, • Efficient, • Good against attacks.
Wang et al. [39]	2015	Based on chaotic system and improved gravity model	H	• Good against attacks, • Efficient.
Wang et al. [40]	2015	Hybrid chaotic maps and dynamic random growth technique	H	• Useful for image transmission systems, • Resisting chosen plain text attack.
Wang et al. [41]	2015	Based on DNA (Deoxyribonucleic acid) sequence operations and chaotic system	H	• Good against attacks, • Highly secure.
Zhang et al. [42]	2015	Spatiotemporal non-adjacent coupled map lattices	M	• Good permutation, • Efficient, • Secure.
Luo et al. [43]	2015	Chaos based encryption	H	• Effective coding compression, • Efficient, • Secure.
Hua et al. [44]	2015	Heterogeneous bit-permutation and correlated chaos	H	• Wider chaotic range, • Good ergodicity, • Low cost.
Li et al. [45]	2014	Chinese Reminder Theorem	H	• Helping to clarify positive role of CRT in cryptology.
Mohamed [46]	2014	Reversible one- dimensional cellular automata	H	• Can be computed in parallel, • Highly secure, • Useful for real time applications.
Gu [47]	2014	A chaotic 3D cat map	H	• Good permutation, • Large key space, • Simple, • Efficient.
Zhu et al. [48]	2014	Generalized Arnold Map In Row And Column Direction	H	• Suitable for practical image encryption.
Huang et al. [49]	2014	Self-adaptive model for chaotic image encryption algorithm	H	• High speed, • Good against attacks, • Highly secure, • Efficient.
Zhang et al. [50]	2014	Single round permutation diffusion chaotic cipher	H	• Simple, • Large key space.
Sui et al. [51]	2014	Multiple-image encryption scheme based on the asymmetric technique and using fractional Fourier transform and chaotic diffusion	H	• Secure, • Efficient.
Zhang et al. [52]	2014	Cross chaotic map	M	• Highly secure, • High speed,
Ghebleh et al. [53]	2014	Robust shuffling-masking image encryption scheme based on chaotic maps	H	• Large key space, • Sensitivity to the secret key, • Good against attacks, • Use in secure communication applications, • Secure and reliable.
Boriga et al. [54]	2014	Hyper chaotic map based on parametric equations	H	• Efficient, • Secure.
Xie et al. [55]	2014	Based on DNA sequence operation and hyper-chaotic system	H	• Efficient.
Zhou et al. [19]	2014	1D chaotic maps (seed maps)	H	• Simple, • Efficient, • Good Performance, • Good against attacks.
Zhang et al. [56]	2014	Based on the spatiotemporal chaos of the mixed linear-nonlinear coupled map lattices	H	• Large key space, • Good against attacks, • Efficient, • High sensitivity.

3. Color image encryption schemes

With the development of the effective color image encryption techniques, it is more necessary to review the techniques and select the algorithm which would be applied in a particular situation. The color image encryption algorithms can be divided into two categories based on different domains: one in the spatial domain and the other in the transformed domain. Encryption algorithms in the spatial domain are mainly based on scrambling image pixels or blocks [79]. Encryption algorithms in transformed domain, however, are mainly based on scrambling or encrypting the transform coefficients or blocks [79]. Despite the fact that most of the

Table 3
List of previous surveys on image encryption.

Author(s)/reference	Year	Classification
Kabir et al. [57]	2017	Color image encryption for secure transfer over the internet*
Ranjan et al. [58]	2017	Key(s) and keyless image encryption techniques
Farook M. et al. [59]	2017	Image encryption methods
Kumar et al. [60]	2017	Image encryption security solutions for wireless systems
Singh et al. [61]	2017	Image encryption technique and to extract feature from image
Parameshwaran [62]	2016	Encryption algorithms for color images*
Younes [63]	2016	Different techniques of image encryption
Kaur et al. [64]	2016	Image encryption using DNA based cryptography techniques
Paliwal et al. [65]	2016	Extraction technique from videos and images
Jain et al. [66]	2016	Image encryption schemes
Bose et al. [67]	2015	Image encryption and compression techniques
Jawad et al. [68]	2015	Emerging challenges in color image encryption techniques*
Chand et al. [69]	2015	Image encryption using chaos based techniques
Kumar et al. [70]	2015	Image encryption techniques
Damedhar et al. [71]	2015	Keyless approach to image encryption
Sneha et al. [72]	2014	Image encryption using different approaches
Khan et al. [73]	2014	Image encryption techniques
Naskar et al. [74]	2014	Secured image encryption techniques
Kumar Das et al. [75]	2014	Image cryptography
Sankpal et al. [76]	2014	Image encryption using chaotic maps
Jawad et al. [77]	2013	Color image encryption techniques*
Ephin et al. [78]	2013	Chaos based image encryption and decryption techniques

* Surveys on color image encryption.

encryption techniques proposed based on transformed domains can be executed by optical setups with a high speed in encryption, they lack security strength due to their intrinsic linearity in the overall system. In the meantime, classification of these techniques under some criteria is very difficult.

In the current study, it has been tried to review and classify various color image encryption techniques taking into account their schemes. In the following subsections, these schemes will be shortly reviewed and then some of the algorithms proposed in this field will be presented.

3.1. Color image encryption using chaos-based algorithms

A chaotic system benefits from numerous excellent intrinsic characteristics, including ergodicity, aperiodicity, high sensitivity to initial conditions and control parameters, and pseudorandom behaviors [80]. Therefore, researchers have suggested several image encryption algorithms on the basis of the chaotic systems. The typical chaotic map-based ciphers can be divided into two stages of permutation and diffusion. The permutation operation of some algorithms merely changes the pixel position; however, the chaotic sequence produced by a chaotic system is independent of the plain text and diffusion process. Hence, the ciphertext can be easily deciphered by chosen-plain text and chosen-ciphertext attacks. The diffusion operation can drastically increase the resistance to statistical and differential attacks, in which the histogram of the cipher image is fairly uniform and significantly differs from that of the plain image. For a good diffusion process, we must use a key stream which is strongly related to the plain image. When encrypting different plain images, completely different chaotic sequences can be achieved in the encryption algorithm [80]. The diffusion process has been introduced as the following.

Step 1: Utilizing chaotic sequence to obtain key stream.
Step 2: Encrypting pixel values of the image matrix.
Step 3: Repeating Step 2 until reaching cipher-image.

The conventional chaotic systems utilized in image encryption processes are Lorenz map [81,82], Baker map [83,84], Arnold's cat map [85,86], Hénon map [87,88], Logistic map [51,89], Chee-Lee system [90], Hyper-chaotic system [80,91], Quantum Logistic map [92,93], Multiple coupled map lattices [94], Tent and sine map [95], etc. In the following, some methods proposed for color image encryption using chaotic system will be reviewed.

Aqeel ur Rehman et al. offered a color image encryption technique using exclusive-OR with DNA complementary rules on the basis of the chaos theory and SHA-256 [96]. The SHA-256 hash function was utilized in this study in order to modify the initial conditions and control parameters of the chaotic system. Three channels of a color image have been arranged into a one dimensional vector and sorted based on the chaotic sequence produced by Piecewise Linear Chaotic Map. Then this permuted array has been split into three parts each representing a color channel and permuted independently again using Lorenz's chaotic system. Once the dual permutation was performed, each pixel of every channel is independently encoded into Deoxyribonucleic Acid (DNA) bases chaotically. The novelty of the algorithm is that each pixel of a channel is substituted by Exclusive-OR operation with DNA complementary rules. Multiple DNA rules are exploited to repeat this operation in a sequence to some random number of times. This operation iteration continues cyclically. The selection of DNA rule in the onset of this cyclic operation and the operation continuation are dependent on Chen's chaotic sequence. Based on the extensive simulated experimental results, it has been proved that the proposed algorithm is accompanied by excellent encryption results achieved only in one round.

Seyedzadeh et al. [1] have proposed a new chaos-based image encryption algorithm in order to encrypt color images utilizing a Coupled Two-dimensional Piecewise Nonlinear Chaotic Map (CTPNCM), and a masking process. Computerized simulations verified that the new algorithm was accompanied by a high security level and was very fast in practical color image encryption applications. In this algorithm, a 256-bit long external secret key was employed in order to produce the initial conditions and parameters of the CTPNCM. Experimental results revealed the superiority of the proposed algorithm in yielding better security performance compared to the results of other algorithms.

Tong et al. suggested a fast color image encryption algorithm on the basis of a four-dimensional chaotic system [97]. Initially in this study, in order to enhance the complexity and key space of the encryption algorithm, they proposed a novel method to design four-dimensional chaotic systems considering the classical equations of the three-dimensional chaotic systems. In the second step, given

the dependence of the pixel channel of the color images, they designed a new pseudo-random sequence generator and reused the random sequence to improve the speed of the image encryption operation. Finally, they exploited the row-major and column-major methods in order to diffuse the original image, in addition to using the cat map with parameter to scramble the image pixels and gain the encryption effect. The simulation and security analysis results indicated that the encryption algorithm in this study was accompanied by a good performance in terms of security, robustness, and high speed of encryption.

A Li et al. introduced a hyper-chaos based image encryption algorithm to adopt a 5-D multi-wing hyper-chaotic system, in which the key stream produced by the hyper-chaotic system was related to the original image [80]. Then, the pixel-level and bit-level permutations were utilized to enhance the security of the cryptosystem. Eventually, a diffusion operation was exploited to change pixels. Theoretical analysis and numerical simulations illustrated that the proposed algorithm was of a high security and reliability for image encryption.

A simple and effective chaotic system has been proposed in [19] using a combination of two existing one-dimension (1D) chaotic maps (seed maps). Simulations and performance evaluations revealed the capability of the proposed system in producing several 1D chaotic maps with larger chaotic ranges and better chaotic behaviors in comparison to their seed maps. A novel image encryption algorithm was proposed to examine the applications of this system in multimedia security. Using a similar set of security keys, this algorithm was able to produce a completely different encrypted image each time when applying it to the same original image. Experiments and security analysis showed the great performance of the algorithm in image encryption and against various attacks.

El-Latif et al. [92] proposed a new scheme for encryption of the color images based on quantum chaotic system. First, they obtained a new substitution total automorphism in integer wavelet transform through scrambling only the Y (Luminance) component of L frequency sub band. In the next step, they achieved two diffusion modules by mixing the features of horizontally and vertically adjacent pixels using the adopted quantum chaotic map. Finally, they accomplished substitution/confusion generating an intermediate chaotic key stream image exploiting the quantum chaotic system. Several security and performance analyses performed thoroughly based on the experimental investigations and revealed the excellent characteristics of the proposed color image encryption method including sufficient security and appropriate performance. Comparisons showed that most of the results were in favor of the proposed scheme.

Pak and Huang [98] suggested a method to create a simple and effective chaotic system using difference of the output sequences of two similar existing one-dimension (1D) chaotic maps. Simulations and performance evaluations revealed the ability of the proposed system to generate a one-dimension (1D) chaotic system along with better chaotic performances and larger chaotic ranges in comparison to the previous chaotic maps. A novel encryption system of linear-nonlinear-linear structure was introduced on the basis of total shuffling in order to investigate its uses in the image encryption field. The experiment was indicative of the accuracy of the encryption algorithm. Experiments and security analysis proved the excellent performance of the algorithm in image encryption as well as against various attacks.

Wang et al. [99] suggested another algorithm of color image encryption using alternate chaotic mapping structure. In this study, they exploited the R, G and B components to form a matrix. 1D logistic and two-dimensional (2D) logistic mapping were utilized for generating a chaotic matrix, and then two chaotic mappings were iterated alternately to permute the matrix. *XOR* operation was adopted for each iteration to encrypt plain image matrix, and subsequently to make further transformation for the matrix diffusion. Finally, the encrypted color image was obtained from the confused matrix. Theoretical analysis and experimental results demonstrated the secure and practical characteristics of this cryptosystem, as well as its properness to color images encryption.

Wang et al. [82] presented a new color image encryption algorithm on the basis of complex Chen and complex Lorenz systems. Three step processes were included in this encryption algorithm. In the permutation process, the plain image pixels were individually scrambled through 2D and 1D permutation processes among RGB channels. In addition, in the diffusion process, the *XOR* operation was utilized to conceal the information of pixels. At last, the mixing RGB channels were applied to achieve a multilevel encryption. Based on the security analysis and experimental simulations, the proposed algorithm was large enough to resist the brute-force attack yielding an excellent encryption performance.

In [100], a chaos-based asymmetric color image encryption scheme was designed by Liu and Kadir; the advantage of this design was the distribution of different keys to different receivers through key changing mechanism. The hash value of the plain image was exploited for generating two initial values of the Hénon map to generate two pseudo-random sequences. In the encryption scheme, six pseudo-random arrays were initially generated to circularly shift the R, G, and B components by rows and columns respectively, and then diffuse the three color components by *XOR* operation. In the decryption process, two initial values of Hénon map, the iteration number $m\text{-}n+1$, the iteration times, and the control parameters of Hénon map were served as keys. Numerical results indicated the feasibility and effectiveness of the asymmetric cryptosystem for color image encryption.

Another attempt in this field has been presented in [91] regarding an asymmetric color image encryption scheme based on four-wing hyper chaotic complex system, with initial values, parameter, and step length being dependent on 512-bit hash value of the plain image. The encryption process involved converting the three color components into three 1D arrays, and then using three pairs of chaotic sequences to encrypt the elements of odd number and even number indices, respectively. The encryption and decryption algorithms had different keys. The feasibility and effectiveness of this asymmetric color image encryption scheme were proven based on the numerical results and security analyses.

Liu et al. [101] suggested a chaos-based color image encryption scheme using bijection. In this algorithm, the whole image was diffused by *XOR* operation for random rounds, with each color component being separated into blocks with the same size. A bijective function f: $B \rightarrow S$ was made between block set B and S-box set S. The corresponding 8×8 S-box was generated dynamically by the Chen system with variable conditions. The ciphered image could be obtained after substituting each block with the paired S-box. According to the numerical simulation and security analyses, the scheme was capable of application in image encryption.

In [102], an asymmetric image encryption algorithm was proposed by Wu et al. with the advantages that the key groups and the number of keys in secret information transmission among multiple individuals were very small, and key transmission mode was relatively simple and secure. In this algorithm, the plain image was compressed first, then the encryption was performed on the color image using the improved 4D cat map followed by asymmetric encryption based on elliptic curve ElGamal encryption. Finally, the encrypted image was diffused globally. The performance analysis was carried out on key spaces, key sensitivity, capability of resisting statistical attacks, differential attacks, known plain text attacks and chosen plain text/cipher text attacks, and quality evaluation metrics of the decrypted image. Simulation results indicated

better security of the proposed algorithm in comparison with other algorithms.

In [103], Mazloom et al. have suggested a coupled nonlinear chaotic map (CNCM) and a novel chaos-based image encryption algorithm for encryption of color images using CNCM. The chaotic cryptography technique used in this study was a symmetric key cryptography with a stream cipher structure. In order to increase the security of the proposed algorithm, a 240 bit-long secret key was used to generate the initial conditions and parameters of the chaotic map through performing some algebraic transformations on the key. These transformations and also the nonlinearity and coupling structure of the CNCM have led to the enhanced cryptosystem security. The image size and color components have been employed in cryptosystem in the current study in order to achieve higher security and complexity, thereby significantly increasing the resistance to known/chosen-plain text attacks. The results of various experimental and statistical analyses as well as the key sensitivity tests revealed that the proposed image encryption scheme is capable of providing an efficient and secure way for real-time image encryption and transmission.

In [15], Liu and Wang suggested a stream-cipher algorithm based on one-time keys and robust chaotic maps. In this study, the piecewise linear chaotic map was employed as the generator of a pseudo-random key stream sequence. The initial conditions were generated by the true random number generators, the MD5 of the mouse positions. They applied the algorithm in the color image encryption and gained a satisfactory level of security.

A color image encryption scheme based on coupled hyper chaotic Lorenz systems was proposed by Kadir et al. in [104]. The random injection of the impulse signals into coupled Lorenz system during iterations for enhancing the complexity of trajectory was the novelty of this scheme. Six sequences of state variables were generated in order to encrypt the R, G, and B components using bitwise operations of *XOR* and left or right cyclic shift. Six initial values and indeterminate multiple impulse signals could cause the cryptosystem to include larger variable key space to resist against exhaustive attack, even the attack from a quantum computer. Simulation results were indicative of the stability of the mean encryption speed, that is, the speed depended solely on hardware equipment and algorithm. Statistical analysis illustrated the high effectiveness of the proposed image encryption algorithm.

A novel cryptographic system has been presented by Hsiao et al. in [105] for color image security using chaotic amplitude phase frequency model (APFM) nonlinear adaptive filter. The authors in this study set nine parameters and simulated time interval and initial values for APFM nonlinear adaptive filter in order to generate chaos, in addition to using the chaos property to design a color image encryption algorithm. The proposed scheme was able to encrypt the color image (plain image) and transform it into the color cipher image with histograms of the three components which were distributed almost uniformly. The proposed scheme included a key sensitivity capable of reaching the order of 10 to the power of -10 in order to get sufficient security strength needed for color images protection. Furthermore, the encryption algorithm suggested in this study passed the NIST SP 800-22a tests successfully, verifying that the proposed scheme was a safe cryptographic system. The experimental results and security analyses indicated an appropriate security performance of the proposed method.

As stated in [78], chaos methods have unique characteristics such as sensitivity to the primary values and parameters and mixing; and their main difference with encryption methods is in the fact that encryption methods are defined on a limited set of integers while chaos methods are defined on real numbers. Chaos-based methods are a combination of speed, complexity, high security, reasonable computational overhead, and computational power that can be used independently or in combination in the encryption of images.

3.2. Color image encryption using permutation

During the past few years, multiple image encryption techniques have been introduced in transform domain. The common levels of permutation are bit level [56,106,107], pixel level [108,109], and block–level permutation [101,110], in addition, row-shuffling and column-shuffling are classified as block-level permutation. Bit level permutation (BLP) is a new method that was first proposed in 2011 and is exploited at the confusion stage of image encryption. In BLP, an image is considered to consist of a bit matrix to which all the encryption effects are applied; hence, the cipher-image should ultimately reflect the bit distribution of these encryption effects. In contrast, previous image encryption algorithms were used to perform the encryption process at the pixel level, whereas BLP acts directly on each bit in the plain image, rather than on a bit group at the pixel level [110]. Most of the previously reported image encryption algorithms perform several rounds of 2D and 3D permutations among the different bit planes of the plain image, following which the different permuted bit planes are combined to generate the confused (encrypted) color image.

Patro and Acharya in [108] have proposed a secure multiple color image encryption technique based on multi-level permutation operation; this technique was totally different from the currently used multiple image encryption techniques. Three levels of permutation operation were used in the proposed encryption technique with the first, second, and third levels of permutation operation performing pixel-shuffling operations in R, G, and B components, row-shuffling operations between the pixel-shuffled R, G, and B components, and column-shuffling operations between the row-shuffled components, respectively. Finally, the proposed encryption algorithm was used to perform block-diffusion operations in order to achieve the final encrypted images. Moreover, the secret keys employed in this algorithm depended not only on the original key values, but also on the original color images. This supported the algorithm against known-plain text and chosen-plain text attacks. The simulation results and the security analyses were indicative of the good encryption results, large secret-key space, higher sensitivity to secret keys and the plain text, weaker correlation of adjacent pixels, greater randomness of pixels, and enough resistance against various common attacks of the proposed algorithm.

The study by Zhang et al. [110] on combining the aspects of the Chen system with a 3D cat map in the permutation stage was another attempt in this field. In this study, an image was considered to be as a natural three-dimensional (3D) bit matrix (width, height, and bit length), and a new 3D bit matrix permutation was suggested. The results of the simulations carried out verified the security and efficiency of the new cryptosystem discussed in this study.

In [106], Wang and Zhang presented a novel color image encryption with heterogeneous bit-permutation and correlated chaos. Taking into account the difference in volumes of information between bit planes, they employed heterogeneous bit-permutation for reducing the computation costs and improving permutation efficiency, followed by conducting expanded *XOR* operation for R, G, B components of color images, thus achieving cipher color images. The introduced correlated chaos provided a new way of initialization for chaotic maps, in addition to fully exploiting the chaotic maps. The architecture of permutation and diffusion was utilized in this method, and 1D WPLCW chaotic maps were used to produce pseudo-random sequences during the entire encryption process. The results of the experiments and analyses proved the secu-

rity and effectiveness of the proposed color image encryption algorithm.

Ying-Qian et al. [56] introduced a new image encryption algorithm on the basis of the spatiotemporal chaos of the mixed linear-nonlinear coupled map lattices; the strategy of bit level pixel permutation was employed in this algorithm, enabling the lower bit planes and higher bit planes of pixels to permute mutually without any extra storage space. The simulation results indicated the superior security and high efficiency of the proposed algorithm.

In [111], a new confusion scheme based on paired interpermuting planes was suggested by Zhang et al.. In the new confusion operation proposed in this investigation, "an exchange and random access strategy" was utilized in order to replace the traditional confusion operations. The simulation results were indicative of the superior security and computation speed of the scheme proposed in this study in comparison with other comparable algorithms.

Another investigation in this field has been offered by Liu [107] regarding a bit-level permutation and high-dimension chaotic map for color image encryption. In this investigation, the plain color image of size ($M \times N$) was first converted into a grayscale image of size ($M \times 3\,\mathrm{N}$), then it was transformed into a binary matrix, and the matrix at bit-level was permuted by the scrambling mapping produced by piecewise linear chaotic map (PWLCM). In the next step, the Chen system was exploited to confuse and diffuse the R, G, and B components at the same time. The results of tests and security analyses illustrated not only the capability of the scheme to achieve good encryption results, but also the sufficient large size of the key space to resist against common attacks.

In [109], a novel pixel shuffling method was proposed by Huang et al. for image encryption. The output trajectory of chaotic system was very unpredictable. Therefore, due to the unpredictable character of this method, the chaotic sequences generated by chaotic systems were utilized as encryption codes. Then the digital-color image encryption was implemented with high confidential security. The proposed method along with four differential chaotic systems and pixel shuffling were capable of thoroughly banishing the outlines of the original image, disordering the distributive characteristics of RGB levels, and dramatically decreasing the probability of exhaustive attacks. Finally, empirical images were regarded as illustrations, showing great encryption performance for the proposed method and achieving a high confidential security.

Therefore, due to simplicity and speed in implementation [112], permutation algorithm is used in the form of double or multiple combination with other encryption methods; sometimes, different levels of permutation can be combined in order to promote security level [108].

3.3. Optical color image encryption

In this part, some of the optical image encryption techniques proposed in the literature inspired by the architecture of the classic optical double random phase encoding (DRPE) system were reviewed. The optical DRPE method and its numerical simulation algorithm were first examined in association with the sampling considerations at various stages of the system based on the spread of the input signal. Then, various well-known optically inspired encryption techniques were investigated and classified into optical techniques and image scrambling techniques. Each method was implemented numerically and compared with the optical DRPE scheme, where random phase diffusers (masks) were applied after different transformations. First, the optical system exploited for each method was demonstrated, and then the implementation of the corresponding unitary numerical algorithm was examined in order to maintain the properties of the optical counterpart. The common optical image encryptions included Fresnel transform (FST) [113,114], polarization [115,116], gyrator transform (GT) [117,118], Hartley transform [119,120], double random phase encoding [121,122], and fractional Fourier transform (FFT) [51,123]. In the following, some algorithms will be introduced using the optical image encryptions for color image encryption.

In [113], a technique has been proposed by Hwang based on a modified Gerchberg-Saxton algorithm (MGSA) in the Fresnel-transform (FST) domain in order to encode a color image into three phase-only functions (POFs) for three separated channels. The computerized simulations of the partial color encryption and decryption validated the feasibility of the proposed scheme.

In [114], a color image encryption was suggested by Wang et al. using a phase-truncated FST and random amplitude mask (RAM) without the risk of information disclosure. In this design, an image was first separated into three channels, and then the risk of information disclosure encountered in previous encryption methods was removed using an additional RAM channel. Robustness of the proposed scheme was analyzed against attacks and the numerical simulations were indicative of the feasibility and effectiveness of the proposed system.

Rajput et al. [115] presented a single-channel color image encryption scheme based on amplitude- and phase-truncated FRT and interference of polarized light using structured phase masks (SPM). Their scheme, secured a color image with multiple levels of security. Amplitude and phase truncation help generate unique decryption keys and make the cryptosystem asymmetric. This technique used polarization selective diffractive optical element (PSDOE) to generate the desired polarized wavefronts. So knowledge of PSDOE, fractional orders, decryption keys, and construction parameters of SPM are essential for the successful retrieval of plain image.

Abuturab introduced a new method using discrete cosine transform in GT domain structured-phase encoding, similar to [124] but to secure color images in [117]. In the technique proposed in this study, the input color image to be encrypted was separated into three channels each being independently encrypted through changing its spatial distribution of pixel value using discrete cosine transform, and they were then encoded with structured phase mask. The GT was conducted on resultant spectrum. In this proposed method, the structured phase mask, discrete cosine transform, and GT were utilized twice. In addition, the construction parameters of the structured phase mask and angle parameters of GT in each channel were principal encryption keys. Moreover, the schematic electro-optical implementation was presented in this method and the proposed architecture did not require axial movements. The effectiveness of the proposed algorithm was demonstrated against the selected and known plain text attacks; in addition, the numerical simulations verified the security, validity, and capability of this method.

Liu et al. [119] suggested an algorithm to encrypt color image with the use of the rotation of color vector on the basis of discrete Hartley transform. The three component images of the color image were taken into account as the axes of Cartesian coordinates. Two random angle shifts were introduced in order to rotate the color vectors consisting of the three color components in discrete Hartley transform domains in the process of image encryption. The corresponding rotation shifts of the two angles were capable of performing as the scheme key. Some numerical simulations showed the feasibility of the proposed scheme.

In [121] a single-channel color image encryption system is proposed using a double-phase encoding. In their algorithm, at first the input RGB image is converted to an indexed image, and then the encryption is performed by using a typical optical security system. The proposed method transforms a RGB color image into a complex-amplitude stationary white noise, and needs only one channel for encryption. It can add color information to verification

in addition to the shape information, reduce the complexity, and increase the reliability of the corresponding optical color image encryption systems.

In this regard, another study was introduced by Chen et al. in [123]. A single channel optical asymmetric cryptosystem was presented in this investigation for color image in FFT domain. The color image was encoded into grayscale format and encrypted in a single optical channel system instead of the commonly used encryption system of the RGB channels. The effective trapdoor one-way function was calculated to design asymmetric approach utilizing the equal modulus decomposition (EMD). The Ushiki chaotic system was performed to enhance the security of the proposed cryptosystem in order to produce the random phase mask in FFT as well as a random sequence in order to scramble the private key. The sensitive initial values and chaotic data could be considered as the additional keys and public key. Various numerical experiments were performed, confirming the validity and capability of the proposed color cryptosystem.

In addition to high speed [125] and security [126] of optical image encryption algorithms, they have a key advantage compared to other encryption methods which is capability of massive parallelism in a two-dimensional space [127].

3.4. DNA based color image encryption

As discussed in [128], encoding of an image into DNA bases is simple using Table 4. The R, G, and B channels have been encoded using four DNA rules. Some of the studies accomplished in the area of the DNA-based color image encryption have been presented in the following.

In [129], Wu et al. offered a new scheme for the encryption of color images on the basis of the DNA sequence operations and multiple improved 1D chaotic systems with excellent performance. In this study, the key streams were first produced from three improved 1D chaotic systems using the secret keys and the plain image and the key streams; in addition, the plain image were transformed randomly into the DNA matrices by the DNA encoding rules, respectively. Secondly, the DNA complementary and *XOR* operations were performed on the DNA matrices to obtain the scrambled DNA matrices. In the third step, the scrambled DNA matrices were decomposed equally into blocks, and then these blocks were shuffled randomly.

Finally, the DNA *XOR* and addition operations were implemented on the DNA matrices obtained from the previous step and the key streams. Then, the encrypted DNA matrices were converted into the cipher-image by the DNA decoding rules. Experimental results and security analyses illustrated a good encryption effect and high security for the proposed encryption scheme in addition to a strong robustness for the common image processing operations and geometric attack.

A color image encryption algorithm has been presented based on DNA sequence addition operation in [131] by Wei et al. In this algorithm, three DNA sequence matrices were first obtained through encoding the original color image which could be transformed into three matrices of R, G and B. Then, the chaotic sequences generated by Chen's hyper-chaotic maps were employed in order to scramble the locations of elements from three DNA sequence matrices, and then divide these matrices into some equal blocks, respectively. In the third step, these blocks were added using DNA sequence addition operation and Chen's hyper-chaotic maps. Eventually, the encrypted color image was achieved by decoding the DNA sequence matrices and recombining the three channels of R, G, and B. The simulation results and security analyses revealed that the algorithm of this study not only had a suitable encryption effect, but was also able to resist exhaustive, statistical, and differential attacks.

Table 4
Encoding and decoding map rules for DNA sequences [130].

	A	T	C	G
Rule 1	00	11	10	01
Rule 2	00	11	01	10
Rule 3	11	00	10	01
Rule 4	11	00	01	10
Rule 5	10	01	00	11
Rule 6	01	10	00	11
Rule 7	10	01	11	00
Rule 8	01	10	11	00

In [132], Kalpana et al. proposed an improved color image encryption on the basis of multiple DNA sequence operations with DNA synthetic; three modifications were suggested in this study: (1) adoption of multiple DNA encoding rules for each pixel of the color image, (2) Diffusion of pixels by either DNA addition/subtraction rather than a single DNA operation, and (3) addition/subtraction for each pixel with a synthesized image rather than the same image. The simulation results and security analysis of this algorithm demonstrated not only a better encryption effect but also a higher ability of resisting statistical and differential attacks compared with the original proposal.

In [133], a novel improved color image encryption algorithm based on DNA sequence *XOR* operation and complex chaotic systems was introduced by Li et al. In the first step, three DNA sequence matrices were obtained by encoding the original color image which could be converted into three matrices of R, G, and B. Then, the new chaotic sequences which acted to retain the decimal part and remove the integer part from six chaotic sequences, Key 2 gotten by Key 1 and hamming distance were exploited to scramble locations of elements of the three DNA sequence matrices. In addition, the three DNA sequence matrices were divided into some equal blocks, respectively. In the third step, the *XOR* operation was applied between these blocks by DNA *XOR* operation and complex hyper-chaotic map; moreover, the pseudo-DNA sequences were controlled by quaternary chaotic sequences from the wavelet function. At last, the encrypted color image was obtained through decoding the DNA sequence matrices and recombining the three channels of R, G, and B. The simulations and security analysis revealed that the proposed algorithm was capable of improving the encoding efficiency and enhancing the security of the cipher text, in addition to the capability of resistance to exhaustive, statistical, and differential attacks.

In a study, a novel color image encryption algorithm was offered by Wu et al. [134] based on DNA sequence operations, one-time keys, and the spatiotemporal chaos. In this algorithm, the key streams were firstly generated by the NCA map-based CML, in which the hash function SHA-256 was employed to update the system parameters and initial conditions in combination with the plain image and the secret keys. In the second step, the plain image was decomposed into three channels, and they were converted randomly into three DNA matrices by the DNA encoding rules. Furthermore, the three DNA matrices were combined into a new DNA matrix, and then the row-wise and column-wise permutations were performed on it. In the third step, the shuffled DNA matrix was divided into three equal blocks and the DNA addition, subtraction, and *XOR* operations were implemented on these DNA blocks. Finally, the DNA matrices were separately transformed into the decimal matrices according to the DNA decoding rules. A diffusion process was further carried out using the key streams in order to enhance the cryptosystem security, hence attaining the resulting cipher-image. Experimental results and security analysis illustrated the good encryption effect and resistance of the presented encryption algorithm to various typical attacks.

Wang et al. proposed an encryption algorithm for color images using chaotic system and DNA sequence operations in [135]. The three components of the color plain image were utilized to construct a matrix, and then to perform confusion operation on the pixel matrix produced by the spatiotemporal chaos system, i.e., the coupled map lattice (CML). DNA encoding and decoding rules were introduced in the permutation phase and the extended Hamming distance was suggested to generate new initial values for CML iteration combining color plain image. Then, the rows and columns of the DNA matrix were permuted and the color cipher image was then attained from this matrix. Theoretical analysis and experimental results proved the security and applicability of the cryptosystem, as well as its suitability to encrypt color images of any size.

As mentioned above, one of the most successful methods of image encryption is the DNA-based encryption method [136] which is interested by researchers due to its low cost [3], capability of massive parallelism [131], having large key space and saving the storage space [137].

3.5. Frequency domain based color image encryption

The watermarked techniques have been categorized into two types in terms of domain, spatial domain, and frequency domain [133]. The spatial domain procedures are the oldest techniques that consider the modification of pixels in the image for the insertion of water-mark. The spectrum and least significant bit are the commonly used approaches. However, the spatial domain techniques are not robust against all types of attacks. On the other hand the frequency domain techniques are employed to insert the watermark by transforming the original image using discrete wavelet transform (DWT) [138,139], Ridgelet transform [140,141], discrete cosine transform (DCT) [142,143], discrete Hadamard transform (DHT) [144,145], and discrete Fourier transform (DFT) [146,147]. Then, the watermark insertion procedure is performed. These techniques are widely acceptable and more robust against all types of attacks. Some of the studies in the field of the color image encryption based on the frequency domain are as follows.

A color image encryption algorithm has been designed by Liu et al. using Arnold transform and DCT [143]. In this algorithm, the RGB components of the color image were scrambled by Arnold transform at the aspect of pixel sequence. The scrambled RGB components were exchanged and mixed randomly under the control of a matrix defined by random angle. DCT was employed to change the pixel values of the color image. In this encryption scheme, the above-mentioned operations were performed twice continuously. The Arnold transform and the random angle parameters served as the color image encryption method key. Some numerical simulations were carried out to examine the validity and capability of the color encryption algorithm.

Wu et al. proposed a new lossless encryption algorithm for color images considering a six-dimensional (6D) hyper chaotic system and the two-dimensional (2D) discrete wavelet transform (DWT) [139]. In this algorithm, the plain image was firstly divided into four image sub-bands by the 2D DWT. Then, the sub-bands were permutated by a key stream, and then their size was decreased by a constant factor. In the third stage, the 2D inverse DWT was employed to reconstruct an intermediate image using the four encrypted image sub-bands. Finally, the pixel values of the intermediate image were modified using another key stream to further enhance the security. Experimental results and security analysis demonstrated the high security and fast speed of the proposed algorithm as well as its resistance to various attacks.

In a study, utilizing the characteristics of the human visual system (HVS), spread transform technique, and statistical information measure, Maity et al. [145] introduced a digital image watermarking scheme. Spread transform (ST) scheme was implemented using the transform coefficients of both the host and the watermark signals. Watermark embedding strength was adaptively adjusted using frequency sensitivity, luminance, contrast, and entropy masking of the HVS model. The selection of Hadamard transform as watermark embedding domain brought about several advantages, including low loss in image information (higher image fidelity), greater watermark detection reliability, and higher data hiding capacity in a high degree of compression. The proposed method was compared with some of the recently reported watermarking schemes in terms of performance based on the spread spectrum and quantization index modulation.

Another study was proposed in this ground by Tsui et al. [146]. Two vector watermarking schemes were proposed in this study based on the use of complex and quaternion Fourier transforms. For the first time in this study, it was shown how to embed watermarks into the frequency domain, which is consistent with human visual system discussed in this study. The most interesting characteristic of the scheme was the possibility of performing watermarking in the frequency domain of chromatic components. Robustness was attained through embedding a watermark in the coefficient with positive frequency, spreading it to all color components in the spatial domain. Moreover, the invisibility was satisfied modifying the coefficient with negative frequency, such that the combined effects of the two were insensitive to human eyes. Experimental results indicated better performance of the two proposed algorithms in comparison to the two existing algorithms.

Therefore, the advantage of Frequency Domain based Image Encryption algorithms is the presence of a simple structure and its easy implementation [146]; but the most important reason for the use of these algorithms is minimization of the computational costs [148].

3.6. Hash based color image encryption

Hash function is commonly exploited to generate the fixed-length output bits acting as a shortened digest to the original data. Since the collision of MD5 has been revealed, SHA-2 has become more suitable for cryptosystem designing, which consists of a set of hash functions with digests of 224, 256, 384, or 512 bits, however no collision has been found up to now [149]. On October 2, 2012, Keccak [150] was selected as the winner of the NIST hash function competition [151] to become SHA-3.

Some hash functions like [152] have been designed for gray images, in addition, some others like the following methods have been designed for RGB color images.

Dong [153] designed a chaos-based asymmetric color image encryption scheme. The plain image hash value was converted into three initial values for the piecewise linear chaotic map (PWLCM), which was iterated to generate three pseudo-random sequences to respectively diffuse the R, G, and B components. The hash value and the initial iteration number m were served as keys in the encryption process; moreover, three initial values for PWLCM and the initial iteration number n were served as keys in the decryption process. Numerical results were indicative of the feasibility and effectiveness of the proposed asymmetric cryptosystem for color image encryption.

In [149], a novel algorithm was suggested for image encryption based on SHA-512. Employing one half of the image data for encryption of the other half of the image reciprocally was the main idea behind the algorithm. The high security, sensitivity, and speed included the distinct characteristics of the algorithm that could be employed for encryption of gray-level and color images. The algorithm accounted for two main sections: the first part performing the preprocessing operation to shuffle one half of the image and the second part exploiting the hash function to produce a random

number mask. The mask was then *XOR*ed with the other part of the image to be encrypted. This was conducted in order to increase the image entropy. Analysis was performed on both aspects of security and performance of the proposed algorithm and satisfactory results were obtained in various rounds.

Hence, although hash-based image encryption methods are mostly used to hash the security key, due to high security and large key space [126] in this kind of algorithm, some researchers have used them dependently or in combination with other image encryption methods.

3.7. Color image encryption using evolutionary methods

Currently, evolutionary algorithms (EAs) are significantly considered by the scientists and are used in numerous applications [154]. EA-based methods, as the name suggests, have an iterative nature and this special characteristic helps the algorithm improve its results in each iteration [38]. The main advantage of EAs is their capability to treat the problem with only minimal information on them without leaving any detail on the intermediate calculations leading to results. This last point perfectly required the domain of data encryption to complicate or even penalize any cryptanalysis attempt. Thus, the data encryption problem can be solved by an optimization procedure, holding the detailed general structure through the following subsections, going from the coding operation until the achievement of the final results [155]. In an investigation, Enayatifar et al. [154] suggested an encryption method based on the weighted discrete imperialist competitive algorithm (WDICA) or a hybrid model consisting of a genetic algorithm (GA) and a chaotic function proposed by Abdullah et al. in [130]. A partial image encryption optimization scheme was proposed by Kuppusamy et al. in [156] using high energy coefficients of the transformed image which was selected employing the particle swarm optimization (PSO) technique within the daubechies 4 domain for encryption. In addition, some evolutionary-based methods such as the following algorithm were designed for color image encryption.

A novel color image encryption algorithm has been introduced in [157]. In this study, the 24-bit planes of the color plain image RGB components were obtained and recombined into 4 compound bit planes; this could make the three components affect each other. A four-dimensional (4D) memristive hyperchaotic system generated the pseudorandom key streams and its initial values came from the SHA 256 hash value of the color plain image. The compound bit planes and key streams were confused based on the principles of genetic recombination, then confusion and diffusion were applied as a union to the bit planes, then the color cipher image was obtained. Experimental results and security analyses indicated the security and effectiveness of the proposed algorithm; hence it can be adopted for secure communication.

Considering the above examples, it is concluded that evolutionary methods in image encryption are raised in terms of their innovation, but the main advantage of these algorithms is their high sensitivity and security [155].

3.8. Color image encryption using bit plane decomposition

Each pixel in gray scale image may be represented as an 8-bit binary value, distributed by Eq. (2).

$$P(x,y) = K(8), K(7), K(6), K(5), K(4), K(3), K(2), K(1) \tag{2}$$

Typically, the upper four bit planes of an 8-bit gray scale image (i.e. 8th, 7th, 6th, and 5th) include significant volume of information, whereas the lower four bit planes (4th, 3rd, 2nd, and 1st) contain less information as illustrated in Fig. 2. The pixel information percentage is distributed as Eq. (3).

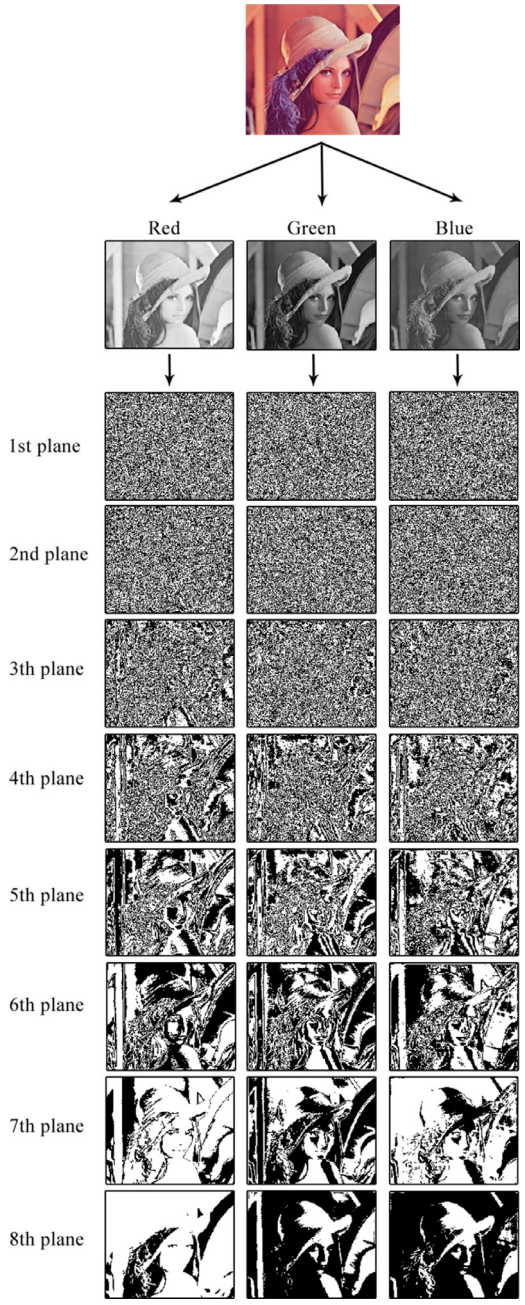

Fig. 2. Bit planes of the color 'Lena' image.

$$\boldsymbol{K(I)} = \frac{2^i}{\sum_{i=0}^{7} 2^i} \tag{3}$$

Therefore, the bit plane technique is exploited to decompose the image into subparts, moreover, binary bit-plane decomposition is used to separate the gray scale image into 8-bit binary planes, which is demonstrated in Fig. 2; where the *nth* bit-plane is in fact composed of all *n*th bits of binary representation of each pixel. A non-negative decimal number N may be illustrated with a binary sequence ($b_{n-1}\ldots\ b_1,\ b_0$) as shown in Eq. (4).

$$N = \sum_{i=0}^{n-1} b_i 2^i \ = \ b_0 2^0 + b_1 2^1 + \ldots + b_{n-1} 2^{n-1} \tag{4}$$

Some of the studies in the color image encryption field using bit plane decomposition have been introduced in the following.

A useful image encryption algorithm has been proposed in [158] for multiple gray-scale images. This algorithm was exploited to decompose input images into bit planes, randomly swap bit-blocks among different bit planes, and perform *XOR* operation between the scrambled images and secret matrix controlled by chaotic map. Finally, an encrypted PNG image was achieved through viewing four scrambled gray-scale images as its red, green, blue, and alpha components. Many simulations have been performed to show the efficiency of the algorithm.

Another image encryption technique has been offered by Sravanthi et al. taking into account the bit plane operation using piecewise linear chaotic map (PWLCM) and 2-D logistic-adjusted-sine map [159]. Initially, the bit plane diffusion operation was performed using the PWLCM system, then the row-shuffling and column-shuffling operations were conducted with the use of the 2-D logistic-adjusted-sine map. Besides, the secure hash algorithm SHA-256 was utilized to update the secret keys of the proposed cryptosystem to resist known-plain text and chosen-plain text attacks. The bit plane operation was the main significance of this algorithm. This operation confuses the pixels in addition to diffusing the pixels simultaneously. The simulation results were indicative of the better encryption results of the proposed cryptosystem with the security analysis showing the stronger resistance to the most known common attacks.

A chaos-based image encryption algorithm for color images has been introduced in [160] based on the 3D bit plane permutation. In this algorithm, the color plain image was first transformed into 24-bit planes using RGB splitting and bit plane decomposition; in the next step, the 3D bit plane permutation was performed on bit planes, and the position sequences for permutation were obtained from the 3D Chen chaotic system, and then the three confused components were attained. Secondly, three key matrices were generated by a 1D chaotic system and a multilevel discretization method. Ultimately, the color cipher image was obtained diffusing the confused components using key matrices. The SHA 256 hash function value of the plain image was obtained and combined with the given parameters to calculate the parameters and initial values of the chaotic system. In this way, the proposed scheme highly relied on the plain image and it could effectively withstand known-plain text and chosen-plain text attacks. Simulation results and security analyses demonstrated the good encryption effect of the algorithm in addition to resistance to common attacks, indicating its reliability for application in image secure communications.

So, Image Encryption using Bit plane Decomposition methods have two significant features including having large key space [137], and efficiency [161].

3.9. Double (multiple)-image encryption for color images

Encryption algorithms using iterative phase retrieval technique for double gray images include a series of forward and backward iterations [162]. In order to examine the double color images, three groups of gray images (the color image being decomposed into R, G, and B channels with each component considered as a gray image) will be respectively encrypted. However, the interrelationships between color components are not used in this approach. It also leads to three-times-larger iteration loops and phase functions. To reduce the image communication overload on the Internet, the double (multiple)-image encryption has attracted great interest in recent years [163]. The advantage of the multiple-image encryption is its capability to encrypt many images synchronously [164]. Some researchers have presented various encryption algorithms [165–169], including double (multiple)-image encryption; some of the studies on double color image encryption have been listed in the following.

Wei et al. proposed a double color image encryption scheme based on off-axis holography and maximum length cellular automata (MLCA) [170]. The original image was separated into three channels of red, green, and blue, and each channel was encrypted independently using the MLCA mask to alter the intensity values in the spatial domain. Then the reference waves with different incident angles were introduced into the off-axis Fourier transform hologram in order to accomplish double color image encryption. The system parameters of the off-axis Fourier transform in each channel were also keys in image encryption and decryption. The reference wave with certain incident angle and corresponding MLCA mask were exploited when decrypting one of the original images. Some numerical simulations demonstrated the effectiveness of the proposed scheme, and the authors in this study present the results of the preliminary experiments performed.

An optical double color image cipher was proposed in [171] using 2D chaotic Arnold transform (AT) as a preprocessing scrambling stage and 2D chaotic logistic adjusted sine map (LASM) phase masks in the Fresnel (Fr)-based Hartley transform (HT). In this optical double color image cipher, the 2D chaotic LASM was employed to create chaotic phase masks. The color plain image RGB channels were first scrambled with 2D chaotic AT. In the next step, the scrambled color plain image R-G-B channels were modulated using the 2D chaotic LASM phase mask and transformed with the Fr-based HT. The distributions of the transformed complex R-G-B channels were then scrambled with the 2D chaotic AT, modulated with the 2D chaotic LASM phase mask, and then transformed with Fr-based HT. The utilization of 2D chaotic LASM phase masks, in addition to the 2D chaotic AT, provided efficient key administration and communication. Moreover, optical geometric parameters were considered as extra additional keys enhancing the secrecy of the proposed scheme. A comprehensive security study was exploited for the proposed scheme and test results verified and ensured the high security and resistance of the proposed scheme against most potential attacks.

Another method was proposed by Shao et al. in [162], describing an algorithm for encryption of the double color images into a single undistinguishable image in quaternion gyrator domain. In this algorithm, the phase masks used for encryption were obtained using an iterative phase retrieval algorithm. The encrypted image was then generated through cascaded quaternion GTs with different rotation angles. In quaternion GTs, the parameters and phases serve as encryption keys. Knowing these keys, the original color images can be fully restituted. Numerical simulations have demonstrated the validity of the proposed encryption system as well as its robustness against loss of data and additive Gaussian noise.

Therefore, the Double (Multiple)-image Encryption methods have high speed and sensitivity that can lead to saving in the storage space [164].

3.10. Color image encryption using scrambling transform

Image scrambling is an image encryption or auxiliary encryption technique [172], as well as an important method of preprocessing and post-processing in image hiding, sharing, and digital watermarking. Arnold transform [86,173], Jigsaw transform [174,175], Fibonacci transform [30,176], Knight's tour [177,178], Lucas transform [179], magic square transform [180,181], gray code [25,35], cellular automata [170,182], Baker map [32,84], and sub affine transform [183] are the popular image scrambling methods in image encryption. Some of the studies accomplished in the color image encryption area using scrambling transform are as follows.

A color image encryption scheme has been proposed in [173] using GT and Arnold transform; this scheme includes two security levels. In the first level of the scheme, the color image was separated into three components of red, green, and blue, which

are normalized and scrambled using the Arnold transform. The green component was combined with the first random phase mask and transformed to an interim using the GT. The encryption result was along with stationary white noise distribution and camouflage property to some extent. In the encryption and decryption processes, the rotation angle of GT, the iterative numbers of Arnold transform, the parameters of the chaotic map, and the produced accompanied phase function served as encryption keys, hence enhancing the security of the system. Simulation results and security analysis confirmed the security, validity, and feasibility of the proposed scheme.

Another algorithm for encryption and decryption of RGB images was proposed by Mishra et al. using scrambling based on chaotic system combined with reality preserving 2D discrete fractional Fourier transform (RP2DFRFT) and Arnold transform (AT) [86]. The proposed cryptosystem provided security of color images based on the keys as well as the arrangement of the algorithms and parameters employed. Furthermore, the use of reality preserving method alleviated the complexity of dealing with imaginary data in addition to improving the efficiency of the technique through decreasing the domain space to its half, at least for all the calculations involved in the 2D DFRFT. The sensitivity analysis on the proposed technique indicated the high sensitivity of the encryption keys. Results based on the standard examples and their security and statistical analyses for color images revealed the robustness and suitability of the proposed technique.

In [180], a color image encryption algorithm has been introduced by Shen et al. based on magic cube transformation, in addition to designing a new modular arithmetic operation. First, a natural number chaotic sequence was created with the secret key. For a higher security, all secret keys were generated by different chaotic maps, thus increasing the decryption security. Then, the position permutation algorithm was implemented by magic cube transformation with chaotic sequences. In the third step, the pixel-substitution algorithm was realized through changing the image pixel value, with a *XOR* plus mod diffuse operation and a modular arithmetic operation. Finally, experimental results performed demonstrated the efficiency and high security of the novel algorithm.

Niat et al. suggested an image encryption scheme according to cellular automata (CA) [112]. CA is a self-organizing structure with a set of cells in which each cell is updated by certain rules that are dependent on a limited number of neighboring cells. The limited number of reversal rules and inability to produce long sequences of states by these rules were the major drawbacks of cellular automata in cryptography. In this study, a non-uniform cellular automata framework was proposed to solve this problem. This proposed scheme included confusion and diffusion steps. In the confusion step, the positions of the original image pixels were replaced by chaos mapping. The key image was created using non-uniform cellular automata and then the hyper-chaotic mapping was exploited to select random numbers from the image key for encryption. The main contribution of the paper included the application of hyper chaotic functions and non-uniform CA for robust key image generation. Security analysis and experimental results indicated that the proposed method was accompanied by a very large key space as well as resistance to noise and attacks.

In another investigation, a novel image encryption scheme was presented by Chai et al. employing the memristive hyper-chaotic system, cellular automata (CA), and DNA sequence operations, consisting of diffusion process [182]. SHA 256 hash function was applied in order to yield the secret key and compute the initial values of the chaotic system. Moreover, a dynamic DNA encoding scheme was introduced. Two DNA rule matrices for encoding the plain image and 2D CA were generated from chaotic sequences, which were controlled by the plain image; therefore, there are different DNA encoding rules for different original images. In addition, the block diffusion encryption method was manipulated to the plain image to save time. The previous diffused block image and 2D CA were combined to affect the encryption effect of the current block image. Among them, the 2D CA was updated by the local rule computed from the previous diffused sub image, and its initial configuration was determined by the chaotic sequences. Simulation results and security analyses both confirmed the extraordinary encryption performance of the proposed image encryption scheme in addition to resistance to various attacks. This scheme can be used in secure image and video communication fields.

Chen et al. [184] have designed a color image encryption algorithm employing the affine transform in the GT domains. The RGB components of the color image were transformed into the real part and the imaginary part of a complex function through the affine transform. Then, the complex function was encoded and transformed in gyrator domain. To increase the security of this encryption algorithm, the GT was performed twice. The parameters in the affine transform and the GT were regarded as the key in the encryption algorithm. Some numerical simulations have been carried out to test the validity and capability of the proposed color encryption algorithm.

According to the studies on the use of Scrambling Transform Image Encryption methods, it is concluded that these algorithms have a large key space [185], and in addition to high run speed, they have a simple implementation [186] leading to more use of these methods in different studies.

4. Performance evaluation measures

A good (gray or color) image encryption algorithm should resist all known attack types, including exhaustive attack, statistical attack, and chosen-plain text/cipher text attack. In the following subsection, all common performance metrics have been demonstrated in Fig. 3 and each of the metrics have been described in detail manner respectively. In Sections 4.2, 54 selected papers and 10 proposed schemes will be compared.

4.1. Performance metrics

Various parameters have been exploited to thoroughly examine the techniques. All the parameters have been comprehensively investigated in the current subsection and the existing relations between performance metrics and evaluation parameters in image encryption have been summarized in Table 5 at the end of this subsection. For instance, regarding the evaluation of an image encryption technique against “Brute-force attack”, the “key length” of the proposed image encryption technique will be evaluated.

Histogram Analysis: the histogram demonstrates the gray level intensity and the statistical information of an image as well as distribution of the pixel intensity values, in addition to providing information about the plain image to be used in a histogram attack. However in case of a uniform histogram, the information becomes unpredictable and a histogram attack can be avoided [16].

Correlation Analysis: Two adjacent pixels in a plain image are strongly correlated vertically and horizontally. This is the property of an image, with the maximum and minimum values of the correlation coefficient being 1 and 0, respectively; an image robustly encrypted to statistical attacks should have a correlation coefficient value of 0 [187]. The following Eqs. (5)–(8) indicate the calculation of the correlation coefficients in horizontal, vertical, and diagonal directions.

$$R_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{5}$$

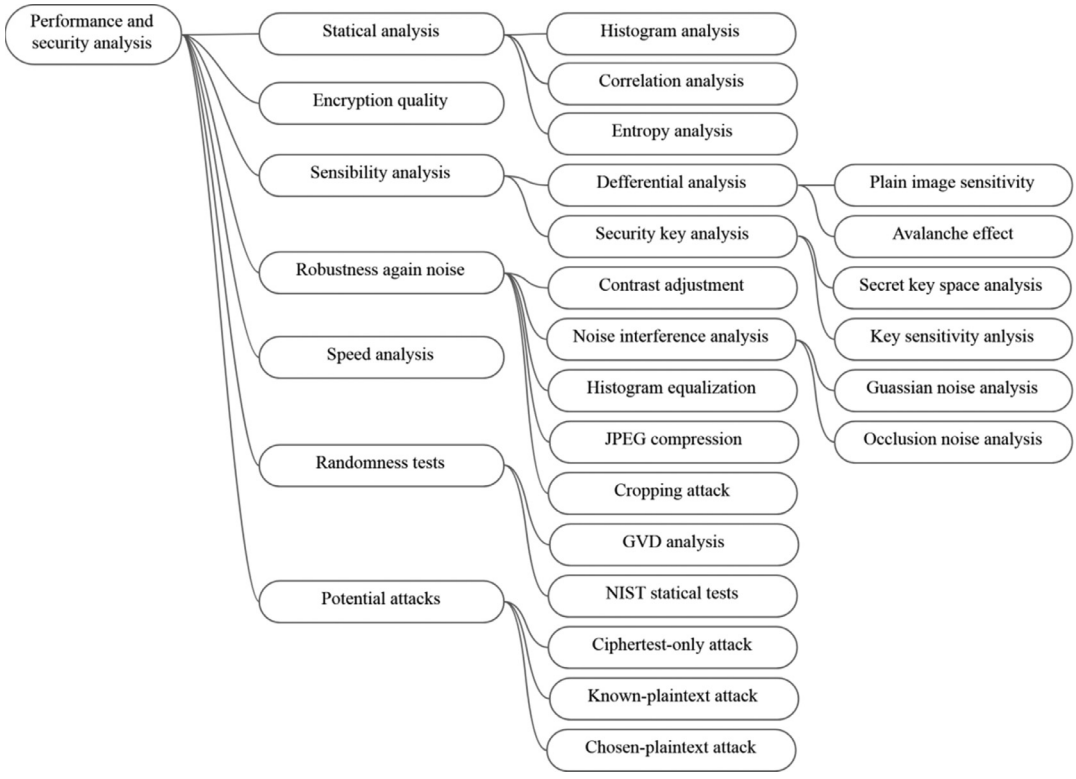

Fig. 3. All common security analysis techniques in image encryption.

Table 5
Performance metrics and evaluation parameters relation in image encryption analysis.

	Metric								
Parameters	Correlation Coefficient	Entropy Value	Histogram of Image	Key Length	MSE Value	NPCR Value	PSNR Value	UACI Value	GVD Score
Histogram Analysis			√						
Correlation Analysis	√								
Inf. Entropy Analysis		√							
Plain Image Sensitivity						√		√	
Avalanche Effect						√		√	
Key Sensitivity Analysis						√		√	
Contrast Adjustment							√		
Gaussian Noise Analysis	√				√	√	√	√	
Occlusion Noise Analysis					√	√	√	√	
Histogram Equalization							√		
JPEG Compression							√		
Cropping Attack							√		
Randomness Tests									√
Cipher text-only Attack				√					
Known-plain text Attack				√					
Chosen-plain text Attack				√					
Brute-force Attack				√					

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{6}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{7}$$

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{8}$$

In the above relations, y is the horizontal adjacent pixel of x, N is the total number of pixels in $N \times N$ image, $cov(x, y)$ is covariance at pixels positions x and y, $\sqrt{D(x)}$ is standard deviation, $D(x)$ is variance, also $E(x)$ is mean.

Information Entropy Analysis: Entropy analysis is a measure of randomness of a message computing the spread of the pixels for each gray level of each color channel. In case of a better uniform distribution, it will be stronger against statistical attacks. For color images, R-G-B channels with intensities between 0 and 255 and the ideal entropy score of encrypted message as 8 in higher, the value higher will have a uniform distribution. It can be defined as Eq. (9) [96],

$$H(m) = -\sum_{i=0}^{N-1} P(m_i) log_2 P(m_i) \tag{9}$$

In which $P(m_i)$ and log refer to the probability of occurrence of symbol m_i and the base 2 logarithm, respectively. The randomness

concept has been proposed because of the occurrence of 256 likely results of the message m with the same probability. In this case, $H(m) = 8$ which is considered to be an ideal value. The security of the encryption algorithm against entropy attack is highlighted when the entropy value is close to 8.

Encryption Quality: The encryption quality (EQ) indicates the average number of changes to each gray level L. The image EQ may be determined by the following equation in which $E(i, j)$ and $I(i, j)$ are the gray value of the pixels at *grid (i, j)* in cipher and plain image, each of size M × N pixels with L gray levels, respectively [130]. It is evident that $I(i, j)$ and $E(i, j) \in \{0, 1, \ldots, L\text{-}1\}$. *HL (I)* and *HL (E)* will be defined as the number of occurrences for each gray level L in the plain image and cipher image, respectively.

The larger the EQ value, the better the encryption security. The EQ is calculated using Eq. (10).

$$\boldsymbol{EQ} = \sum_{\boldsymbol{L}=0}^{255} (\boldsymbol{H_L}(\boldsymbol{E}) - \boldsymbol{H_L}(\boldsymbol{I}))^2 / 256 \tag{10}$$

Sensitivity: means that changing a single bit in the clear image must lead to at least a change in 50% of the bits in the encrypted image [188]. The sensitivity is evaluated using two parameters: the number of pixels change rate (NPCR) and the unified average changing intensity (UACI). NPCR and UACI indicate the number of changing pixels between two encrypted images and the number of averaged changed intensity between two encrypted images, respectively. The ideal value of NPCR and UACI are 99.61% and 33.46%, respectively [188] and NPCR is calculated using Eq. (11).

$$NPCR = \frac{\sum_{i,j} D(i, j)}{M \times N} \times 100\% \tag{11}$$

Where, M and N are respectively the width and height of two random images and $D(i, j)$ is defined as Eq. (12) where *C1* and *C2* denote the cipher images before and after one pixel of the plain image is changed.

$$D(i, j) = f(x) = \begin{cases} 1, & if\ C1(i, j) \neq C2(i, j) \\ 0, & otherwise \end{cases} \tag{12}$$

Moreover, UACI can be exploited to measure the average of intensity for contrast in color component, calculated using Eq. (13).

$$UACI = \frac{1}{\mathrm{M} \times \mathrm{N}} \left[\sum_{\mathrm{i,j}} \frac{\mathrm{C1(i,j)} - \mathrm{C2(i,j)}}{255} \right] \times 100\% \tag{13}$$

Avalanche Effect: The avalanche effect is the proportion of the bits changed in the cipher text while changing a bit in the plain text [97]. The ideal value of avalanche effect is 0.5 and it is often used to indicate the ratio of the bits changed in the cipher text while having a slight change in the system.

Secret Key Space Analysis: refers to the set of all possible keys capable of being used for producing a key, and is one of the most important features determining the strength of a cryptosystem. The number of attempts to find directly refers to key space of the cryptosystem growing exponentially with increasing key size. That is, doubling the key size for an algorithm does not simply double the required number of operations, rather squares them. An encryption algorithm with a 128-bit in key size defines a key space of 2^{128}, which takes about 1021 years to check all the possible keys using modern high performance computers. Therefore, a cryptosystem with key size of 128 bits looks computationally robust against a brute-force attack [189]. A secure algorithm should be completely sensitive to secret key, i.e., the encrypted image cannot be decrypted by slight changes in the secret key [189].

Key Sensitivity Analysis: an ideal multimedia encryption should be sensitive with respect to the secret key, i.e., the change of a single bit in the secret key should be along with generating a completely different encrypted result, called key sensitivity. In general, key sensitivity of a chaotic cipher refers to the sensitivity of the initial states as well as sensitivity of the control parameters of the chaotic map [61].

Contrast Adjustment: A suitable level of brightness and contrast must be available in an image for comfortable viewing, in which former indicates the lightness or darkness of a whole image, however the latter defines the difference of brightness to identify clear separation of different regions [96].

Thus, contrast adjustment is an image processing mechanism in which the input intensities are mapped to a desired level in order to enhance the area or region of interest. This contrast enhancement is applied on the encrypted image at two different levels of 70% and 30%, with the lower value meaning higher contrast, and then the decrypted and original images are compared.

Gaussian Noise Analysis: distortion, degradation, and contamination with communication noises are common in physical world [96]. Thus, in order to test the robustness of the algorithm in such scenarios, a figure is polluted by Gaussian noise with mean zero and variances of 0.0001, 0.0003, and 0.0005 and once again salt and pepper noise was added in encrypted images with densities 1%, 5%, 10% and 25%. The noisy encrypted images were decrypted and the results were compared with each other. Therefore, the robustness against noise is an important index for testing the performance of the encryption scheme [182].

Occlusion Noise Analysis: While communicating over the Internet, a portion of an image can be cropped or even lost, hence the proposed cipher must be capable of handling ciphering of lossy image in an appropriate way [96]. In order to show the strength of the proposed cipher against such a situation, a block of pixels of red channel, a block of pixels of green channel, and a block of pixels of all channels were removed from a figure and they were then encrypted; if the original information was retained after decryption and it was possible to visualize the contents of the original image, the proposed cipher would be capable of handling deciphering of the lossy images.

Histogram Equalization: Histogram of an image includes the range of gray levels and occurrences of each gray level [96]. After decrypting the noisy encrypted image, if the visual information stays intact, the proposed cipher will be able to counterattack the histogram equalization. The parameter peak signal to noise ratio (PSNR) is utilized in order to assess the histogram equalization. PSNR is the ratio of peak signal power to noise power. Basically, mean square error (MSE) indicates a collective squared error between stego and the original image. There is a proportional relation between MSE and error in which Ler value of MSE is the same as the Ler error. The relation of the $m \times n$ monochrome images has been presented below. Thus, *MAX* is indicative of the maximum value of the image pixel. Overall, for a pixel of 8 bits per sample, the value of image is 255; the formulas employed for calculation of PSNR are given based on Eqs. (14) and (15) [96].

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \tag{14}$$

$$PSNR = 10.log_{10} \frac{MAX_I^2}{MSE} \tag{15}$$

JPEG Compression: It is also a common manipulation in image processing [129]. In the simulations, the encrypted image is first compressed with different quality factors; a large quality factor means a small compression rate, yielding a better image quality after JPEG compression. The PSNR values are compared between the decrypted and original images. If recognizing the decrypted images is still possible, so the presented algorithm is robust against JPEG compression attacks.

Cropping Attack: Image cropping is a very common manipulation in real applications, and such operation can cause data loss

Table 6
Classification of the proposed color image encryption schemes on 'Lena' image.

Author(s)/Reference	Year	Used Techniques	Average Correlation Analysis$_{R, G, B}$			Average Entropy	Key Space	Average NPCR (%)	Average UACI(%)
			Horizontal	Vertical	Diagonal				
Chen et al. [123]	2019	1, 3	–	–	–	–	–	–	–
Sravanthi et al. [159]	2019	1, 2, 8	0.0125	−0.0174	−0.0065	7.9993	1.1×2^{377}	99.6098	33.4707
ur Rehman et al. [96]	2018	1, 4, 10	−0.0041	0.0016	0.0021	7.6635	10^{94}	99.5999	33.3848
Patro et al. [108]	2018	2	0.0002	0.0004	0.0002	7.9998	1.9×2^{426}	99.6128	33.4621
Wu et al. [134]	2018	1, 4, 6	−0.0082	−0.0128	−0.0012	7.9896	10^{88}	99.6090	33.4727
Gan et al. [160]	2018	1, 8	0.0101	0.0169	−0.0130	7.9993	2^{470}	99.6000	33.4400
Faragallah [171]	2018	1, 9, 10	−0.0015	−0.0015	−0.0015	7.5907	–	99.7400	0
Li et al. [80]	2017	1, 2	−0.0015	−0.0032	0.0008	7.9972	2^{273}	99.6100	33.4600
Pak et al. [98]	2017	1	−0.0026	−0.0038	0.0017	–	2^{138}	99.6236	33.3441
Wu et al. [102]	2017	1, 10	−0.0001	0.0089	0.0091	7.9912	10^{117}	100.000	33.4720
Kadir et al. [104]	2017	1	0.0019	−0.0015	0.0018	7.9973	$10^{14\times(6+1)}$	99.6022	33.4634
Wei et al. [170]	2017	9, 10	0.0039	0.0004	−0.0046	–	–	–	–
Mishra et al. [86]	2017	1, 5, 10	−0.0238	−0.0238	−0.0238	–	–	–	–
Niyat et al. [112]	2017	1, 10	0.0052	0.0018	0.0010	7.9973	2^{128}	99.6525	33.4331
Chai et al. [182]	2017	1, 4, 6, 10	−0.0016	−0.0033	0.0130	7.9971	2^{128}	99.6100	33.4200
Wang et al. [99]	2016	1	0.0017	0.0016	0.0012	7.9928	10^{165}	99.6300	33.4433
Wang et al. [82]	2016	1	0.0061	0.0049	0.0042	–	10^{194}	–	–
Liu et al. [91]	2016	1, 6	0.0020	−0.0022	−0.0007	7.9891	2×10^{101}	99.6307	33.4460
Zhang et al. [110]	2016	1, 2, 10	−0.0042	0.0005	−0.0004	7.9992	–	99.6155	33.4988
Li et al. [133]	2016	1, 4, 6	0.0046	0.0040	0.0017	7.9954	10^{182}	–	–
Wang et al. [135]	2016	1, 4	−0.0031	−0.0047	−0.0010	7.9973	5.1×10^{66}	99.6100	33.4333
Wu et al. [139]	2016	1, 5	−0.0065	0.0006	0.0054	7.9909	10^{169}	99.6126	33.4668
Chai et al. [157]	2016	1, 6, 7	0.0083	−0.0046	0.0050	7.9993	2^{128}	99.6000	33.2800
Tong et al. [97]	2015	1, 10	0.0017	0.0023	0.0077	7.9997	10^{56}	99.6919	33.3298
Liu et al. [100]	2015	1	0.0019	0.0007	0.0038	7.9895	10^{58}	99.6246	33.4604
Hsiao et al. [105]	2015	1	0.0110	0.0110	0.0110	7.9993	10^{196}	99.6110	33.4585
Wang et al. [106]	2015	1, 2	−0.0098	−0.0050	−0.0013	7.9972	10^{108}	99.6150	33.4893
Zhang et al. [111]	2015	2	0.0052	−0.0002	−0.0002	7.9993	–	99.6199	33.4829
Wang et al. [114]	2015	3	–	–	–	–	–	–	–
Wu et al. [129]	2015	1, 4	0.0084	0.0004	0.0015	7.9897	10^{90}	99.6097	33.4819
Kalpana et al. [132]	2015	1, 4	−0.0177	−0.0094	−0.0042	7.9983	10^{-230}	99.6231	33.6698
Dong [153]	2015	1, 6	0.0025	0.0017	−0.0020	7.9896	10^{50}	99.6155	33.4422
Zhou et al. [19]	2014	1	-0.9×10^{-5}	-5.7×10^{-6}	-7.2×10^{-4}	7.9993	10^{84}	–	–
Liu et al. [101]	2014	1	−0.0018	0.0003	0.0043	7.2476	4.2×10^{59}	99.6180	33.6069
Zhang et al. [56]	2014	2	0.0013	−0.0002	−0.0003	–	10^{120}	99.8726	33.4964
Shao et al. [162]	2014	3, 9	–	–	–	–	–	–	–
El-Latif et al. [92]	2013	1, 5	–	–	–	7.9997	–	99.6389	33.4189
Sui et al. [173]	2013	1, 3, 10	–	–	–	–	–	–	–
Chen et al. [184]	2013	3, 10	–	–	–	–	–	–	–
Seyedzadeh et al. [1]	2012	1	0.0006	0.0008	0.0011	7.9992	2^{256}	99.6828	33.4898
Hwang [113]	2012	3	–	–	–	–	–	–	–
Abuturab [117]	2012	3, 5	–	–	–	–	–	–	–
Wei et al. [131]	2012	1, 4	0.0042	0.0033	0.0024	7.9967	2^{233}	99.2172	33.4055
Liu et al. [107]	2011	1, 2	−0.0574	−0.0035	0.0578	7.9807	1.1×10^{114}	>99.000	>33.000
Liu et al. [143]	2011	5, 10	–	–	–	–	–	–	–
Maity et al. [145]	2011	5	–	–	–	–	–	–	–
Seyedzade et al. [149]	2011	1, 6	−0.0006	−0.0030	0.0061	–	–	–	–
Zhu et al. [158]	2011	1, 2, 8	0.0008	0.0012	0.0036	7.9993	10^{42}	99.6273	33.4815
Liu et al. [15]	2010	1, 6	0.0965	−0.0318	0.0362	7.9845	3.9×10^{341}	99.5799	33.4342
Liu et al. [119]	2010	3	–	–	–	–	–	–	–
Mazloom et al. [103]	2009	1	0.0118	0.0002	0.0148	–	1.8×10^{72}	99.6410	33.3620
Huang et al. [109]	2009	1, 2	0.1257	0.0581	0.0504	–	10^{180}	99.5200	27.7933
Tsui et al. [146]	2008	5	–	–	–	–	–	–	–
Shen et al. [180]	2005	1, 10	0.0143	0.0134	0.0258	–	2^{192}	–	–

[139]. Cropping is deleting some pixel values intentionally in the encrypted image and passing it over the decryption algorithm. Then the decrypted image can be analyzed to test the robustness of the adopted encryption scheme.

Speed Analysis: Analysis of the computation cost of the image encryption algorithm is necessary. Compared with texts, the capacity of the multimedia data is horrendously large. If a cryptographic system encrypts all of the multimedia data bits equally in terms of importance, the computational complexity may be *H*, which has often proved unnecessary [19]. The speed of an encryption scheme is also an important issue in real-time applications [139].

Randomness Tests: For the security of a cryptosystem, the cipher must include some characteristics including good distribution, long period, high complexity, and efficiency. The main objective in these tests is to concentrate on various types of possible randomness in the sequence. Some of these tests include a number of subtests [1]. Recently, the NIST has designed a set of different statistical tests with the aim to justify randomness of binary sequences generated by either hardware- or software-based cryptographic random or pseudo-random number generators [1]. The degree of gray difference is another statistical measure of randomness comparing original and ciphered image and can be defined through Eq. (16) [96];

$$GN(x,y) = \frac{\sum\left[G(x,y) - G\left(x',y'\right)\right]^2}{4} \; here \; \left(x',y'\right) = \begin{cases} (x-1,y) \\ (x+1,y) \\ (x,y+1) \\ (x,y-1) \end{cases} \tag{16}$$

Whereas G(x, y) indicates the gray score at position (x, y). The average neighborhood Gray difference of the whole image can be computed by Eqs. (17) and (18).

$$GVD = \frac{AN'[GN(x,y)] - AN[GN(x,y)]}{AN'[GN(x,y)] + AN[GN(x,y)]} \tag{17}$$

$$AN[GN(x,y)] = \frac{\sum_{x=2}^{M-1}\sum_{y=2}^{N-1} GN(x,y)}{(M-2)(N-2)} \tag{18}$$

In Eqs. (17) and (18), AN and AN' represent average neighborhood gray value; with the former and latter representing before and after encryption, respectively. The final result of the above equations is called GVD score, which will be 0 if the two images are completely the same, otherwise it will be 1.

Cipher text-only Attack: it is an attack with an attempt to decrypt cipher text when only the cipher text itself is available. The opponent tries to recover the corresponding plain text or the encryption key [93].

Known-plain text Attack: the opponent attempts to recover the key in case of access to the cipher text and an associated piece of plain text [190].

Chosen-plain text Attack: An image encryption algorithm with the excellent diffusion property is capable of resisting against the chosen-plain text attack. However, when several existing image encryption algorithms employ the same security keys to encrypt an original image, their encrypted image are duplicate. The attackers exploit this security weakness to break the encryption algorithms using the chosen plain text attack [19].

4.2. Comparison

Each of the proposed schemes is accompanied by the advantages and limitations investigated in Table 7. In recent years, most of the researchers have merged these techniques to eliminate the limitations of a particular technique, and to obtain a more secure encryption algorithm. In these methods, one scheme is always specified to be as the main algorithm, taking the advantages of other schemes to remove the available drawbacks.

In this subsection, the selected studies and proposed schemes will be compared in terms of correlation, entropy, key space, and sensitivity analyses. All the schemes suggested in the current study are along with some strengths and limitations, however the chaos-based techniques are more popular in comparison to other schemes. Among 75.9% of all 54 selected studies using chaotic schemes, 24.1% and 18.5% have employed scrambling transform methods and various techniques of permutation, respectively, in addition, 14.8% of these investigations used optical, DNA based, and hash based schemes, with 11.1% of the selected papers using frequency domain based schemes and also less than 6% using evolutionary techniques, bit plane decomposition, and double (multiple)-image encryption in the encryption process.

A brief insight into each study chosen for color image encryption and the techniques used in each encryption scheme have been presented in Table 6. In this table, the column entitled “used techniques”, included short (1) chaos-based, (2) permutation, (3) optical, (4) DNA-based, (5) frequency, (6) hash-based, (7) evolutionary, (8) bit plane, (9) double (Multiple)-image, and (10) scrambling techniques.

As it is clear in this table, studies in which the hybrid encryption algorithms have been used with chaos-based techniques have lower correlation rate and higher shanon’s entropy, NPCR, and UACI, hence having higher security and sensitivity level.

Each of the ten schemes has been introduced in Section 4, and a number of studies employing the technique to encrypt color images, have been described briefly.

Table 7
Comparison of the proposed schemes.

	Scheme	Chaos based	Permutation	Optical	DNA based	Frequency	Hash based	Evolutionary	Bit plane	Multiple-image	Scrambling
Advantages	High speed	[98]	–	[125]	–	–	–	–	–	[164]	[186]
	Simple structures	[98]	–	–	–	[146]	–	–	–	–	–
	Easy implementation	[98]	[112]	–	–	[146]	–	–	–	–	[186]
	Low cost	[98]	–	–	[3]	–	–	–	–	–	–
	High randomness	[98]	–	–	–	–	–	–	–	–	–
	High sensitivity	[98]	–	–	–	–	–	[155]	–	[164]	–
	Highly secure	[98]	–	[126]	–	–	[191]	[155]	–	–	–
	Timely implementation	–	[112]	–	–	–	–	–	–	–	–
	Large key space	–	–	[192]	[137]	–	[191]	–	[185]	–	[161]
	Storage saving	–	–	–	[137]	–	–	–	–	[164]	–
	Efficient	–	–	–	–	–	–	–	[193]	–	–
	Massive parallelism	–	–	[127]	[131]	–	–	–	–	–	–
Drawbacks and limitations	High time complex	–	–	–	–	–	–	[194]	–	–	–
	High complex	[98]	–	[195]	[196]	–	–	–	–	[197]	–
	High cost	–	–	–	[196]	–	–	–	–	–	–
	Low-quality or missing output	–	–	–	–	[198]	–	–	–	–	–
	Dependent on diffusion step	–	[112]	–	–	–	–	–	–	–	–
	Small keys pace	[109]	[158]	–	–	–	–	–	–	–	–
	Limited behaviors	[98]	–	–	–	–	–	–	–	–	–
	Poor efficiency	[109]	–	–	–	–	–	–	–	–	–
	Potential for redundancy or breaking	–	–	–	–	–	[199]	–	[200]	–	–
	Limited number of reversal rules and	–	–	–	–	–	–	–	–	–	[112]
	Inability to produce long sequences of states										

Table 8
Number of studies using the proposed schemes in color image encryption (2012–2018).

Scheme/Year	Total	ACM DL.	Elsevier	Google Scholar	IEEE Xplore	Scopus	Springer link	Wiley online
Chaos based	**14,095**	**10,156**	**374**	**2381**	**275**	**490**	**414**	**5**
2018	**2488**	1531	94	525	55	140	142	1
2017	**2353**	1576	60	480	70	64	101	2
2016	**2079**	1466	52	357	51	69	82	2
2015	**1855**	1333	58	317	29	78	40	0
2014	**1884**	1430	51	285	21	69	28	0
2013	**1728**	1358	41	243	32	46	8	0
2012	**1708**	1462	18	174	17	24	13	0
Permutation	**2959**	**443**	**248**	**1474**	**163**	**316**	**311**	**4**
2018	**715**	69	62	354	38	83	108	1
2017	**579**	74	34	314	43	38	75	1
2016	**504**	73	38	246	29	48	68	2
2015	**365**	58	38	179	10	51	29	0
2014	**317**	52	35	159	11	39	21	0
2013	**284**	55	28	136	23	39	3	0
2012	**195**	62	13	86	9	18	7	0
Optical	**3805**	**1532**	**285**	**1286**	**104**	**387**	**211**	**0**
2018	**788**	262	61	284	21	81	79	0
2017	**693**	270	48	237	28	67	43	0
2016	**591**	241	36	196	19	44	55	0
2015	**493**	195	48	164	7	66	13	0
2014	**480**	199	42	164	9	55	11	0
2013	**391**	159	34	137	11	47	3	0
2012	**369**	206	16	104	9	27	7	0
DNA based	**1815**	**448**	**153**	**748**	**73**	**200**	**190**	**3**
2018	**515**	61	45	252	25	49	83	0
2017	**402**	69	27	194	29	37	44	2
2016	**285**	57	27	125	10	34	31	1
2015	**211**	57	23	78	4	31	18	0
2014	**174**	52	19	62	2	27	12	0
2013	**136**	78	9	28	3	17	1	0
2012	**92**	74	3	9	0	5	1	0
Frequency	**7199**	**4999**	**239**	**1289**	**140**	**299**	**230**	**3**
2018	**1332**	761	54	312	33	70	101	1
2017	**1335**	880	41	265	38	48	63	0
2016	**1048**	772	28	168	14	35	29	2
2015	**1018**	730	38	170	16	48	16	0
2014	**927**	654	33	167	16	44	13	0
2013	**833**	613	32	128	17	39	4	0
2012	**706**	589	13	79	6	15	4	0
Hash based	**2290**	**1315**	**88**	**577**	**62**	**125**	**121**	**2**
2018	**526**	235	23	166	15	29	58	0
2017	**455**	220	19	139	24	25	27	1
2016	**349**	208	12	88	9	14	17	1
2015	**247**	148	12	57	4	18	8	0
2014	**252**	176	8	46	1	15	6	0
2013	**266**	177	10	52	8	17	2	0
2012	**195**	151	4	29	1	7	3	0
Evolutionary	**7653**	**6890**	**78**	**433**	**50**	**105**	**95**	**2**
2018	**1271**	1022	26	135	11	33	44	0
2017	**1163**	1029	9	83	13	13	15	1
2016	**1000**	840	16	87	9	24	23	1
2015	**1145**	1051	13	52	8	15	6	0
2014	**1054**	1000	7	31	2	8	6	0
2013	**1042**	990	6	32	6	8	0	0
2012	**978**	958	1	13	1	4	1	0
Bit plane	**401**	**6**	**34**	**240**	**29**	**49**	**43**	**0**
2018	**116**	0	11	62	5	15	23	0
2017	**82**	3	5	52	9	7	6	0
2016	**52**	2	3	30	4	7	6	0
2015	**48**	1	6	29	0	8	4	0
2014	**49**	0	5	33	4	5	2	0
2013	**34**	0	3	20	5	5	1	0
2012	**20**	0	1	14	2	2	1	0
Multiple-image	**752**	**3**	**104**	**411**	**34**	**131**	**69**	**0**
2018	**203**	0	25	110	7	27	34	0
2017	**156**	1	18	84	12	24	17	0
2016	**102**	0	14	54	7	18	9	0
2015	**100**	1	19	50	2	24	4	0
2014	**87**	0	14	50	2	19	2	0
2013	**67**	1	10	39	2	13	2	0
2012	**37**	0	4	24	2	6	1	0

(*continued on next page*)

Table 8 (*continued*)

Scheme/Year	Total	ACM DL.	Elsevier	Google Scholar	IEEE Xplore	Scopus	Springer link	Wiley online
Scrambling	**3036**	**235**	**341**	**1594**	**145**	**426**	**293**	**2**
2018	**728**	32	71	382	35	83	125	0
2017	**589**	47	52	323	35	60	72	0
2016	**462**	39	47	240	28	60	46	2
2015	**389**	35	57	190	11	76	20	0
2014	**366**	24	51	199	10	61	21	0
2013	**321**	27	43	167	18	61	5	0
2012	**181**	31	20	93	8	25	4	0

In this section, comparison of the above schemes is applicable in the form of a table, as shown in Table 7. This table indicates the advantages and limitations of the proposed schemes based on the founded resources.

In the studies conducted on different image encryption methods, two factors that have been used regardless of the method leading to distinction between all the 10 proposed algorithms, are (1) dimensions and (2) color of the plain image (colorful or gray). As it is shown in Table 7, in addition to multiple advantages such as randomness, chaos functions have disadvantages such as weak efficiency and complexity; combining these functions in the algorithms based on optical, DNA, hash, bit plane, and scrambling, the researchers remove their highlighted limitation which is their small key space, in order to receive better efficiency. In addition to being added to other encryption methods as an improvement phase, due to simplicity and short time of implementation, permutation algorithms can be used for the encryption of colorful images. Optical and evolutionary algorithms are so complicated, but they can provide a high security for the encrypted images. Due to low cost and having large key space, using DNA-based methods has always been a complementary step in diffusion phase. Frequency algorithms have a simple implementation and structure, but low quality. Multiple-image and scrambling algorithms are high speed algorithms in image encryption. Hash- and bit plane-based algorithms are considered to be highlight in the creation of large key space; both of them have potential for redundancy and breaking, and are used as an inbuilt method to improve the image encryption.

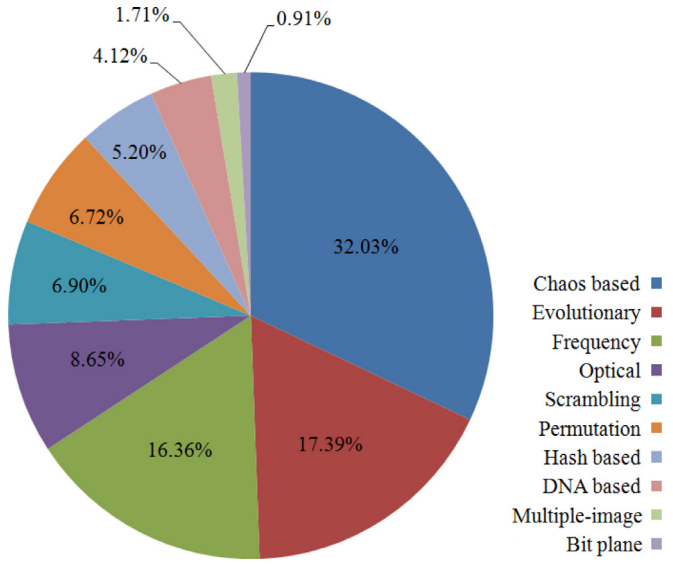

Fig. 4. Percentage of studies using the proposed schemes in color image encryption (2012–2018).

5. Discussion

The rest of this section focuses on the presentation of a complete comparison of the various features of the proposed schemes.

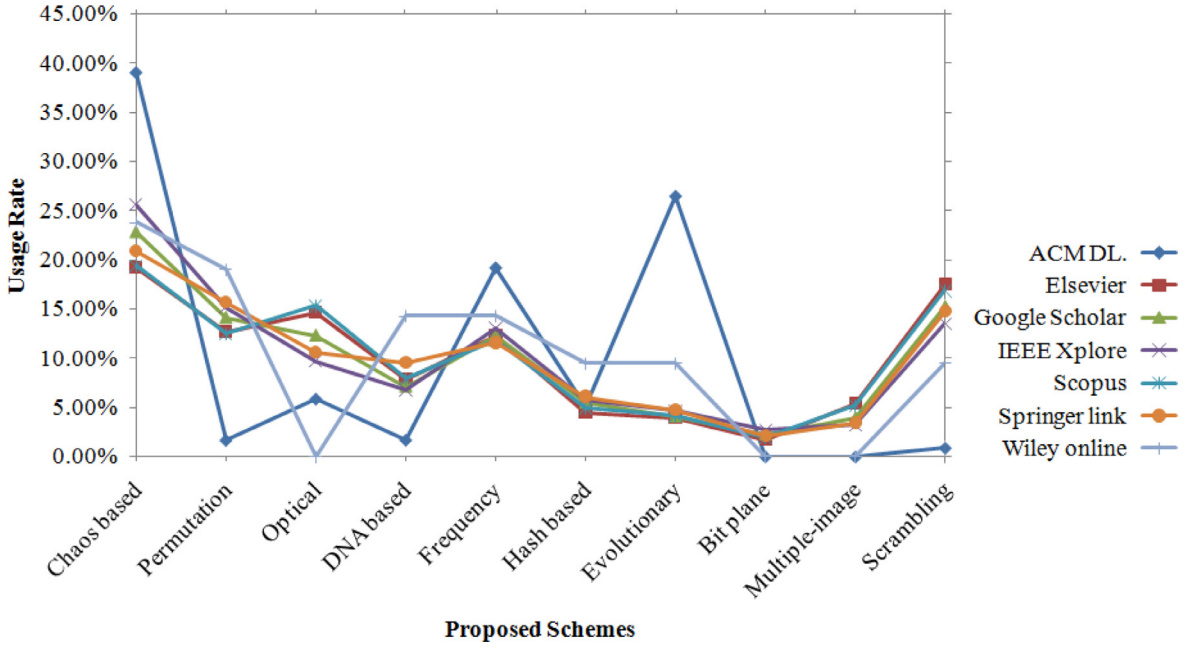

Fig. 5. Comparison of the percentage of studies using the proposed schemes in color image encryption (2012–2018).

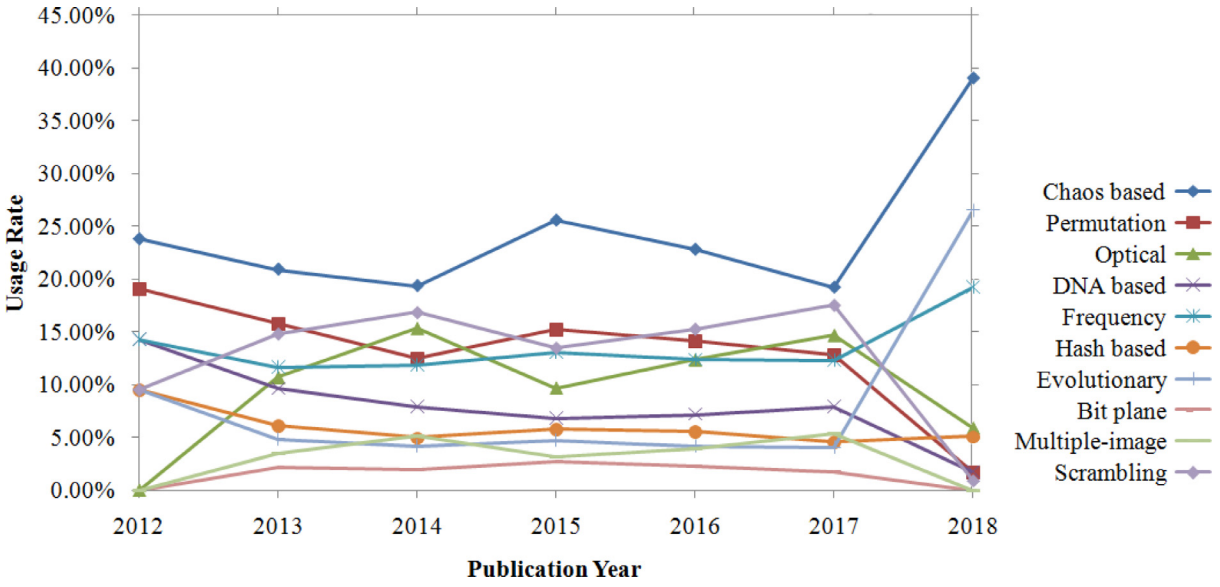

Fig. 6. Timeline diagram of the percentage of published studies using the proposed schemes in color image encryption.

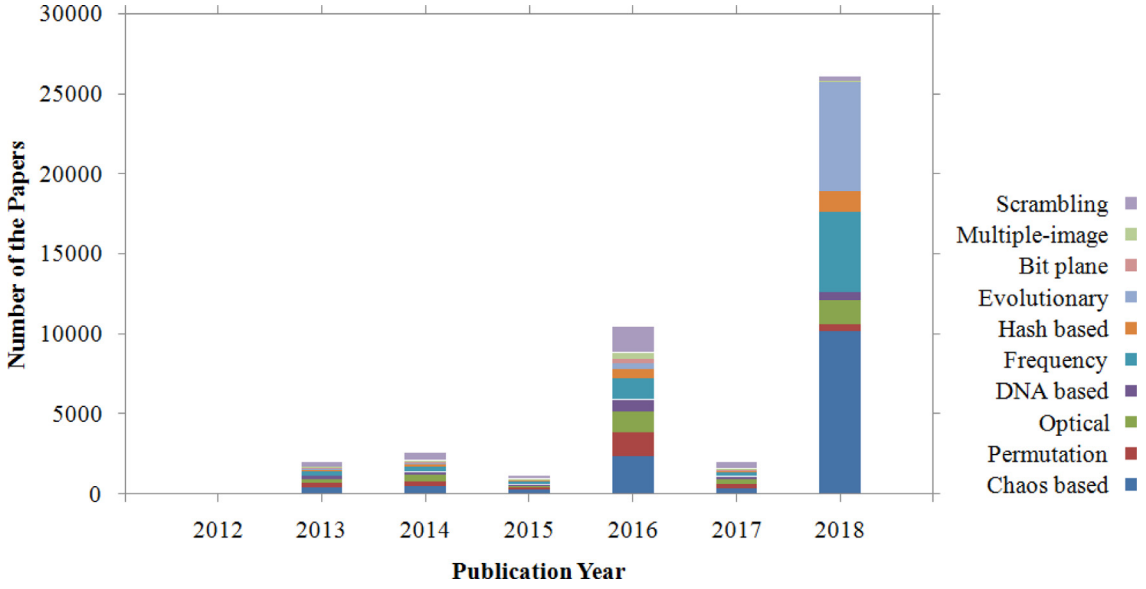

Fig. 7. Timeline diagram of the number of studies using the proposed schemes in color image encryption.

The rate of use of the proposed schemes in published studies can be a good measure for the optimality and application of a technique. In September 2018, a search was performed by the researchers in the present study in ACM Digital Library, Elsevier, Google Scholar, IEEE Xplore, Scopus, Springer link, and Wiley online, with the results for the period of 2012–2018 shown in Table 8.

Fig. 4 exhibits the number of published papers using each scheme in color image encryption as percentage. As demonstrated in this figure, chaotic methods have been used by most of the researchers for image encryption. Based on Fig. 4, the number of articles using the chaos-based, scrambling, and permutation methods for color image encryption is much higher in comparison to the number of studies using other image encryption schemes. As illustrated in this figure, the use of chaos based, evolutionary, and frequency schemes in the published papers have accounted for the highest rates, and the DNA-based, double (multiple)-image, and bit plane decomposition in these papers were with the least rate of use; the details of the search results for each scheme have been listed in Table 8.

As it can be observed in Fig. 4, the chaotic scheme has been used as the main algorithm in more than 32% of all the published studies, with 17.39% of the studies using evolutionary methods, and 16.36% of the studies employing various techniques of frequency domain based color image encryption. In addition, other schemes of the encryption process was exploited in 34.22% of these studies.

Figs. 5 and 6 demonstrate the percentage of using different color image encryption schemes in studies (2012–2018). As shown in these figures, chaos-based, frequency domain-based, and evolutionary schemes have been more focused in recent years. Fig. 7 indicates the upward trend in the total number of papers published between 2012 and 2018 using the proposed schemes; the use of encryption methods has been increased significantly in 2018.

6. Conclusion and future directions

Security of images has become an important agenda of the present era. Network and communication technologies provide

several modes for transferring images worldwide. Images are frequently used in various fields including online learning, engineering services, defense services, scientific experiments, medical imaging, art exhibition, or advertising. With the increased use of digital techniques for transmitting and storing images, the fundamental issue of protecting images for confidentiality, integrity, authentication, and non-repudiation are of major concerns. Since the color images carry richer information compared to the gray-level ones, color image security has become an important issue in the field of information security. Several approaches have been proposed for encrypting images. The color image encryption schemes have been outlined and examined in the present study in terms of usage. Several image encryption techniques have been proposed in the literature. Moreover, a complete list of the common security analysis techniques was presented in the current study for (gray or color) image encryption and discussed, and the potential resistance of the methods to different possible attacks was assessed. Moreover, a complete comparison of these proposed schemes was provided, which can be very useful in designing the future image encryption algorithms for color images.

The ongoing direction in the color image encryption is designing a secure method with the least possible factors for resistance against the security attacks and inclusion of the ideal properties specified in Section 5. Furthermore, considering the privacy of the secret keys is very important in image encryption; however in all of the studies employing the proposed schemes, various methods have been used for scrambling the secret keys. Therefore, designing secure color image encryption should be taken into account in the future investigations. In addition, the use of evolutionary and chaotic methods is highly necessary in all encryption applications, so that they need to be integrated with other schemes to compensate for their deficiencies.

Declaration of Competing Interest

None.

References

[1] S.M. Seyedzadeh, S. Mirzakuchaki, A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, Signal Process. 92 (2012) 1202–1215.
[2] L. Chen, G. Zheng, Multimedia Security Handbook, CRC Press, 2005.
[3] X. Chai, Y. Chen, L. Broyde, A novel chaos-based image encryption algorithm using DNA sequence operations, Opt. Lasers Eng. 88 (2017) 197–213.
[4] L. Zhang, X. Liao, X. Wang, An image encryption approach based on chaotic maps, Chaos Solitons Fractals 24 (2005) 759–765.
[5] I. Mehra, N.K. Nishchal, Wavelet-based image fusion for securing multiple images through asymmetric keys, Opt. Commun. 335 (2015) 153–160.
[6] I. Mehra, N.K. Nishchal, Optical asymmetric watermarking using modified wavelet fusion and diffractive imaging, Opt. Lasers Eng. 68 (2015) 74–82.
[7] I. Mehra, N.K. Nishchal, Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding, Opt. Express 22 (2014) 5474–5482.
[8] A.U. Rehman, J.S. Khan, J. Ahmad, S.O. Hwang, A new image encryption scheme based on dynamic s-boxes and chaotic maps, 3D Res. 7 (2016) 1–8.
[9] J.S. Khan, J. Ahmad, Chaos based efficient selective image encryption, Multidimension. Syst. Signal Process. 30 (2019) 943–961.
[10] J.S. Khan, J. Ahmad, M.A. Khan, Td-ercs map-based confusion and diffusion of autocorrelated data, Nonlinear Dyn. 87 (2017) 93–107.
[11] J. Khan, J. Ahmad, S.O. Hwang, An efficient image encryption scheme based on: Henon map, skew tent map and S-Box, in: 2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), IEEE, 2015, pp. 1–6.
[12] F.A. Khan, J. Ahmed, J.S. Khan, J. Ahmad, M.A. Khan, A novel image encryption based on Lorenz equation, Gingerbreadman chaotic map and S 8 permutation, J. Intell. Fuzzy Syst. 33 (2017) 3753–3765.
[13] J. Ahmad, M.A. Khan, S.O. Hwang, J.S. Khan, A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices, Neural Comput. Appl. 28 (2017) 953–967.
[14] H. Liu, X. Wang, Image encryption using DNA complementary rule and chaotic maps, Appl. Soft Comput. 12 (2012) 1457–1466.
[15] H. Liu, X. Wang, Color image encryption based on one-time keys and robust chaotic maps, Comput. Math. Appl. 59 (2010) 3320–3327.
[16] M. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gutiérrez, O.A. Del Campo, A RGB image encryption algorithm based on total plain image characteristics and chaos, Signal Process. 109 (2015) 119–131.
[17] B. Norouzi, S. Mirzakuchaki, A fast color image encryption algorithm based on hyper-chaotic systems, Nonlinear Dyn. 78 (2014) 995–1015.
[18] L. Teng, X. Wang, J. Meng, A chaotic color image encryption using integrated bit-level permutation, Multimed. Tools Appl. 77 (2018) 6883–6896.
[19] Y. Zhou, L. Bao, C.P. Chen, A new 1D chaotic system for image encryption, Signal Process. 97 (2014) 172–182.
[20] R.-J. Chen, S.-J. Horng, Novel SCAN-CA-based image security system using SCAN and 2-D von Neumann cellular automata, Signal Process. Image Commun. 25 (2010) 413–426.
[21] S. Maniccam, N.G. Bourbakis, Lossless image compression and encryption using SCAN, Pattern Recognit. 34 (2001) 1229–1245.
[22] S.J. Shyu, Image encryption by multiple random grids, Pattern Recognit. 42 (2009) 1582–1596.
[23] T.-H. Chen, K.-C. Li, Multi-image encryption by circular random grids, Inf. Sci. 189 (2012) 255–265.
[24] L. Li, A.A.A. El-Latif, X. Niu, Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images, Signal Process. 92 (2012) 1069–1078.
[25] Y. Zhou, K. Panetta, S. Agaian, C.P. Chen, (n, k, p)-Gray code for image systems, IEEE Trans. Cybern. 43 (2013) 515–529.
[26] X. Liao, S. Lai, Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission, Signal Process. 90 (2010) 2714–2722.
[27] T.-H. Chen, C.-S. Wu, Compression-unimpaired batch-image encryption combining vector quantization and index compression, Inf. Sci. 180 (2010) 1690–1701.
[28] G. Bhatnagar, Q.J. Wu, B. Raman, A new fractional random wavelet transform for fingerprint security, IEEE Trans. Syst. Man Cybern.-Part A 42 (2012) 262–275.
[29] G. Bhatnagar, Q.J. Wu, B. Raman, Discrete fractional wavelet transform and its application to multiple encryption, Inf. Sci. 223 (2013) 297–316.
[30] Y. Zhou, K. Panetta, S. Agaian, C.P. Chen, Image encryption using P-Fibonacci transform and decomposition, Opt. Commun. 285 (2012) 594–608.
[31] C.-K. Chen, C.-L. Lin, C.-T. Chiang, S.-L. Lin, Personalized information encryption using ECG signals with chaotic functions, Inf. Sci. 193 (2012) 125–140.
[32] X. Tong, M. Cui, Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator, Signal Process. 89 (2009) 480–491.
[33] Y. Zhang, D. Xiao, Y. Shu, J. Li, A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations, Signal Process. Image Commun. 28 (2013) 292–300.
[34] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, L.-B. Zhang, A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism, Commun. Nonlinear Sci. Numer. Simul. 20 (2015) 846–860.
[35] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, L.-B. Zhang, An efficient image encryption scheme using gray code based permutation approach, Opt. Lasers Eng. 67 (2015) 191–204.
[36] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, Y. Zhang, An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach, Commun. Nonlinear Sci. Numer. Simul. 23 (2015) 294–310.
[37] L. Chen, J. Liu, J. Wen, X. Gao, H. Mao, X. Shi, Q. Qu, A new optical image encryption method based on multi-beams interference and vector composition, Opt. Laser Technol. 69 (2015) 80–86.
[38] R. Enayatifar, H.J. Sadaei, A.H. Abdullah, M. Lee, I.F. Isnin, A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata, Opt. Lasers Eng. 71 (2015) 33–41.
[39] X.-Y. Wang, N. Wei, D.-D. Zhang, A novel image encryption algorithm based on chaotic system and improved Gravity Model, Opt. Commun. 338 (2015) 209–217.
[40] X. Wang, L. Liu, Y. Zhang, A novel chaotic block image encryption algorithm based on dynamic random growth technique, Opt. Lasers Eng. 66 (2015) 10–18.
[41] X.-Y. Wang, Y.-Q. Zhang, X.-M. Bao, A novel chaotic image encryption scheme using DNA sequence operations, Opt. Lasers Eng. 73 (2015) 53–61.
[42] Y.-Q. Zhang, X.-Y. Wang, A new image encryption algorithm based on non-adjacent coupled map lattices, Appl. Soft Comput. 26 (2015) 10–20.
[43] Y. Luo, M. Du, J. Liu, A symmetrical image encryption scheme in wavelet and time domain, Commun. Nonlinear Sci. Numer. Simul. 20 (2015) 447–460.
[44] Z. Hua, Y. Zhou, C.-M. Pun, C.P. Chen, 2D Sine Logistic modulation map for image encryption, Inf. Sci. 297 (2015) 80–94.
[45] C. Li, Y. Liu, L.Y. Zhang, K.-W. Wong, Cryptanalyzing a class of image encryption schemes based on Chinese remainder theorem, Signal Process. Image Commun. 29 (2014) 914–920.
[46] F.K. Mohamed, A parallel block-based encryption schema for digital images using reversible cellular automata, Eng. Sci. Technol. Int. J. 17 (2014) 85–94.
[47] G. Gu, J. Ling, A fast image encryption method by using chaotic 3D cat maps, Optik-Int. J. Light Electr. Opt. 125 (2014) 4700–4705.
[48] H. Zhu, C. Zhao, X. Zhang, L. Yang, An image encryption scheme using generalized Arnold map and affine cipher, Optik-Int. J. Light Electr. Opt. 125 (2014) 6672–6677.
[49] X. Huang, G. Ye, An efficient self-adaptive model for chaotic image encryption algorithm, Commun. Nonlinear Sci. Numer. Simul. 19 (2014) 4094–4104.

[50] L.Y. Zhang, X. Hu, Y. Liu, K.-W. Wong, J. Gan, A chaotic image encryption scheme owning temp-value feedback, Commun. Nonlinear Sci. Numer. Simul. 19 (2014) 3653–3659.
[51] L. Sui, K. Duan, J. Liang, Z. Zhang, H. Meng, Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain, Opt. Lasers Eng. 62 (2014) 139–152.
[52] M. Zhang, X. Tong, A new chaotic map based image encryption schemes for several image formats, J. Syst. Software 98 (2014) 140–154.
[53] M. Ghebleh, A. Kanso, H. Noura, An image encryption scheme based on irregularly decimated chaotic maps, Signal Process. Image Commun. 29 (2014) 618–627.
[54] R. Boriga, A.C. Dăscălescu, I. Priescu, A new hyperchaotic map and its application in an image encryption scheme, Signal Process. Image Commun. 29 (2014) 887–901.
[55] T. Xie, Y. Liu, J. Tang, Breaking a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system, Optik-Int. J. Light Electr. Opt. 125 (2014) 7166–7169.
[56] Y.-Q. Zhang, X.-Y. Wang, A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice, Inf. Sci. 273 (2014) 329–351.
[57] F. Kabir, J. Kaur, Color image encryption for secure transfer over internet: a survey, Int. Res. J. Eng. Technol. 4 (2017) 860–863.
[58] K.H. Ranjan, S.S. Fathimath, G. Aithal, S. Shetty, A survey on key and keyless image encryption techniques, Cybern. Inf. Technol. 17 (2017) 134–164.
[59] O.F. Mohammad, M.S.M. Rahim, S.R.M. Zeebaree, F.Y. Ahmed, A survey and analysis of the image encryption methods, Int. J. Appl. Eng. Res. 12 (2017) 13265–13280.
[60] P. Praveenkumar, K. Thenmozhi, J.B.B. Rayappan, R. Amirtharajan, Inbuilt image encryption and steganography security solutions for wireless systems: a survey, Res. J. Inf. Technol. 9 (2017) 46–63.
[61] S. Singh, H. Mandoria, A review on image encryption technique and to extract feature from image, Int. J. Comput. Appl. 163 (2017) 19–23.
[62] A.P. Parameshwaran, W.-Z. Song, Encryption algorithms for color images: a brief review of recent trends, Int. J. Adv. Comput. Sci. Appl. 7 (2016) 1–11.
[63] M.A.B. Younes, Literature survey on different techniques of image encryption, Int. J. Scient. Eng. Res. 7 (2016) 93–98.
[64] S. Kaur, S. Malhotra, A review on image encryption using DNA based cryptography techniques, Int. J. Adv. Res. Comput. Sci. Manag. Stud. 4 (2016) 5–8.
[65] S. Paliwal, R. Singh, M. HL, A survey on various text detection and extraction techniques from videos and images, Int. J. Comput. Sci. Eng. Inf. Technol. Res. 6 (2016) 1–10.
[66] Y. Jain, R. Bansal, G. Sharma, B. Kumar, S. Gupta, Image encryption schemes: a complete survey, Int. J. Signal Process. Image Process. Pattern Recognit. 9 (2016) 157–192.
[67] J.S. Bose, G. Gopinath, A survey based on image encryption then compression techniques for efficient image transmission, J. Industr. Eng. Res. 1 (2015) 15–18.
[68] L.M. Jawad, G. Sulong, A survey on emerging challenges in selective color image encryption techniques, Ind. J. Sci. Technol. 8 (2015) 1–12.
[69] S. Chand, R. Aggarwal, E. Dubey, A review of image encryption using chaos based techniques, Int. J. Sci. Res. 7 (2015) 1871–1875.
[70] S. Kumar, M. Kumar, A survey on image encryption techniques, Vivekananda J. Res. (2015) 57.
[71] V.A. Damedhar, V. Nandedkar, A review on keyless approach to image encryption, Int. J. Eng. Res. Gen. Sci. 3 (2015) 316–319.
[72] C.S. Sneha, H. Jose, J.K. Jacob, D. Davis, A survey of image encryption using different approaches, Int. J. Comput. Technol. (IJCAT) 1 (2014) 75–79.
[73] M. Khan, T. Shah, A literature review on image encryption techniques, 3D Res. 5 (2014) 5–29.
[74] P.K. Naskar, S. Majumdar, P. Das, A. Bose, An analytical survey on different secured image encryption techniques, Int. J. Comput. Technol. (IJCAT) 1 (2014) 397–403.
[75] P.K. Das, M.P. Kumar, M. Sreenivasulu, Image cryptography: a survey towards its growth, Adv. Electr. Electr. Eng. 4 (2014) 179–184.
[76] P.R. Sankpal, P. Vijaya, Image encryption using chaotic maps: a survey, Signal and Image Processing (ICSIP), in: 2014 Fifth International Conference on, IEEE, 2014, pp. 102–107.
[77] L.M. Jawad, G.B. Sulong, A review of color image encryption techniques, Int. J. Comput. Sci. Issues (IJCSI) 10 (2013) 266.
[78] M. Ephin, J.A. Joy, N. Vasanthi, Survey of Chaos based Image encryption and decryption techniques, Amrita international conference of women in computing (AICWIC'13), Int. J. Comput. Appl. (IJCA) (2013) 81–85.
[79] I.F. Akyildiz, D. Pompili, T. Melodia, State-of-the-art in protocol research for underwater acoustic sensor networks, in: Proceedings of the 1st ACM international workshop on Underwater networks, ACM, 2006, pp. 7–16.
[80] Y. Li, C. Wang, H. Chen, A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation, Opt. Lasers Eng. 90 (2017) 238–246.
[81] M. Kumar, A. Iqbal, P. Kumar, A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography, Signal Process. 125 (2016) 187–202.
[82] L. Wang, H. Song, P. Liu, A novel hybrid color image encryption algorithm using two complex chaotic systems, Opt. Lasers Eng. 77 (2016) 118–125.
[83] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, Optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains, Opt. Commun. 341 (2015) 263–270.
[84] Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on 3D chaotic baker maps, Int. J. Bifurc. Chaos 14 (2004) 3613–3624.
[85] A. Vaish, M. Kumar, Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain, Optik-Int. J. Light Electr. Opt. 145 (2017) 273–283.
[86] D. Mishra, R. Sharma, S. Suman, A. Prasad, Multi-layer security of color image based on chaotic system combined with RP2DFRFT and Arnold transform, J. Inf. Secur. Appl. 37 (2017) 65–90.
[87] Y. Su, C. Tang, X. Chen, B. Li, W. Xu, Z. Lei, Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map, Opt. Lasers Eng. 88 (2017) 20–27.
[88] R.C. Hilborn, Chaos and Nonlinear Dynamics: an Introduction For Scientists and Engineers, Oxford University Press on Demand, 2000.
[89] L. Sui, B. Liu, Q. Wang, Y. Li, J. Liang, Color image encryption by using Yang-Gu mixture amplitude-phase retrieval algorithm in gyrator transform domain and two-dimensional Sine logistic modulation map, Opt. Lasers Eng. 75 (2015) 17–26.
[90] G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos Solitons Fractals 21 (2004) 749–761.
[91] H. Liu, A. Kadir, Y. Li, Asymmetric color pathological image encryption scheme based on complex hyper chaotic system, Optik-Int. J. Light Electr. Opt. 127 (2016) 5812–5819.
[92] A.A.A. El-Latif, L. Li, N. Wang, Q. Han, X. Niu, A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces, Signal Process. 93 (2013) 2986–3000.
[93] A. Akhshani, A. Akhavan, S.-C. Lim, Z. Hassan, An image encryption scheme based on quantum logistic map, Commun. Nonlinear Sci. Numer. Simul. 17 (2012) 4653–4661.
[94] X. Wang, H. Zhao, M. Wang, A new image encryption algorithm with nonlinear-diffusion based on Multiple coupled map lattices, Opt. Laser Technol. 115 (2019) 42–57.
[95] M. Alawida, A. Samsudin, J.S. Teh, R.S. Alkhawaldeh, A new hybrid digital chaotic system with applications in image encryption, Signal Process. 160 (2019) 45–58.
[96] A. ur Rehman, X. Liao, R. Ashraf, S. Ullah, H. Wang, A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2, Optik 159 (2018) 348–367.
[97] X.-J. Tong, M. Zhang, Z. Wang, Y. Liu, H. Xu, J. Ma, A fast encryption algorithm of color image based on four-dimensional chaotic system, J. Visual Commun. Image Represent. 33 (2015) 219–234.
[98] C. Pak, L. Huang, A new color image encryption using combination of the 1D chaotic map, Signal Process. 138 (2017) 129–137.
[99] X. Wang, Y. Zhao, H. Zhang, K. Guo, A novel color image encryption scheme using alternate chaotic mapping structure, Opt. Lasers Eng. 82 (2016) 79–86.
[100] H. Liu, A. Kadir, Asymmetric color image encryption scheme using 2D discrete-time map, Signal Process. 113 (2015) 104–112.
[101] H. Liu, A. Kadir, Y. Niu, Chaos-based color image block encryption scheme using S-box, AEU-Int. J. Electron. Commun. 68 (2014) 676–686.
[102] J. Wu, X. Liao, B. Yang, Color image encryption based on chaotic systems and elliptic curve ElGamal scheme, Signal Process. 141 (2017) 109–124.
[103] S. Mazloom, A.M. Eftekhari-Moghadam, Color image encryption based on coupled nonlinear chaotic map, Chaos Solitons Fractals 42 (2009) 1745–1754.
[104] A. Kadir, M. Aili, M. Sattar, Color image encryption scheme using coupled hyper chaotic system with multiple impulse injections, Optik-Int. J. Light Electr. Opt. 129 (2017) 231–238.
[105] H.-I. Hsiao, J. Lee, Color image encryption using chaotic nonlinear adaptive filter, Signal Process. 117 (2015) 281–309.
[106] X. Wang, H.-l. Zhang, A color image encryption with heterogeneous bit-permutation and correlated chaos, Opt. Commun. 342 (2015) 51–60.
[107] H. Liu, X. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Opt. Commun. 284 (2011) 3895–3903.
[108] K.A.K. Patro, B. Acharya, Secure multi–level permutation operation based multiple colour image encryption, J. Inf. Secur. Appl. 40 (2018) 111–133.
[109] C. Huang, H. Nien, Multi chaotic systems based pixel shuffle for image encryption, Opt. Commun. 282 (2009) 2123–2127.
[110] W. Zhang, H. Yu, Y.-l. Zhao, Z.-l. Zhu, Image encryption based on three-dimensional bit matrix permutation, Signal Process. 118 (2016) 36–50.
[111] W. Zhang, H. Yu, Z.-l. Zhu, Color image encryption based on paired interpermuting planes, Opt. Commun. 338 (2015) 199–208.
[112] A.Y. Niyat, M.H. Moattar, M.N. Torshiz, Color image encryption based on hybrid hyper-chaotic system and cellular automata, Opt. Lasers Eng. 90 (2017) 225–237.
[113] H.-E. Hwang, Optical color image encryption based on the wavelength multiplexing using cascaded phase-only masks in Fresnel transform domain, Opt. Commun. 285 (2012) 567–573.
[114] Y. Wang, C. Quan, C. Tay, Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask, Opt. Commun. 344 (2015) 147–155.
[115] S.K. Rajput, N.K. Nishchal, Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask, Appl. Opt. 51 (2012) 5377–5386.
[116] S.K. Rajput, N.K. Nishchal, Image encryption using polarized light encoding and amplitude and phase truncation in the Fresnel domain, Appl. Opt. 52 (2013) 4343–4352.

[117] M.R. Abuturab, Securing color image using discrete cosine transform in gyrator transform domain structured-phase encoding, Opt. Lasers Eng. 50 (2012) 1383–1390.
[118] L. Yao, C. Yuan, J. Qiang, S. Feng, S. Nie, An asymmetric color image encryption method by using deduced gyrator transform, Opt. Lasers Eng. 89 (2017) 72–79.
[119] Z. Liu, J. Dai, X. Sun, S. Liu, Color image encryption by using the rotation of color vector in Hartley transform domains, Opt. Lasers Eng. 48 (2010) 800–805.
[120] M.R. Abuturab, An asymmetric single-channel color image encryption based on Hartley transform and gyrator transform, Opt. Lasers Eng. 69 (2015) 49–57.
[121] S. Zhang, M.A. Karim, Color image encryption using double random phase encoding, Microwave Opt. Technol. Lett. 21 (1999) 318–323.
[122] Y. He, Y. Cao, X. Lu, Color image encryption based on orthogonal composite grating and double random phase encoding technique, Optik-Int. J. Light Electr. Opt. 123 (2012) 1592–1596.
[123] H. Chen, Z. Liu, L. Zhu, C. Tanougast, W. Blondel, Asymmetric color cryptosystem using chaotic Ushiki map and equal modulus decomposition in fractional Fourier transform domains, Opt. Lasers Eng. 112 (2019) 7–15.
[124] Z. Hua, Y. Zhou, H. Huang, Cosine-transform-based chaotic system for image encryption, Inf. Sci. 480 (2019) 403–419.
[125] J. Lang, Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain, Opt. Commun. 338 (2015) 181–192.
[126] N. Zhou, Y. Wang, L. Gong, H. He, J. Wu, Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform, Opt. Commun. 284 (2011) 2789–2796.
[127] A. Alfalou, C. Brosseau, Optical image compression and encryption methods, Adv. Opt. Photon. 1 (2009) 589–636.
[128] X. Liao, A. Kulsoom, S. Ullah, A modified (Dual) fusion technique for image encryption using SHA-256 hash and multiple chaotic maps, Multimed. Tools Appl. 75 (2016) 11241–11266.
[129] X. Wu, H. Kan, J. Kurths, A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps, Appl. Soft Comput. 37 (2015) 24–39.
[130] A.H. Abdullah, R. Enayatifar, M. Lee, A hybrid genetic algorithm and chaotic function model for image encryption, AEU-Int. J. Electron. Commun. 66 (2012) 806–816.
[131] X. Wei, L. Guo, Q. Zhang, J. Zhang, S. Lian, A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system, J. Syst. Software 85 (2012) 290–299.
[132] J. Kalpana, P. Murali, An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos, Optik-Int. J. Light Electr. Opt. 126 (2015) 5703–5709.
[133] X. Li, L. Wang, Y. Yan, P. Liu, An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems, Optik-Int. J. Light Electr. Opt. 127 (2016) 2558–2565.
[134] X. Wu, K. Wang, X. Wang, H. Kan, J. Kurths, Color image DNA encryption using NCA map-based CML and one-time keys, Signal Process. 148 (2018) 272–287.
[135] X.-Y. Wang, H.-L. Zhang, X.-M. Bao, Color image encryption scheme using CML and DNA sequence operations, Biosystems 144 (2016) 18–26.
[136] R. Enayatifar, A.H. Abdullah, I.F. Isnin, Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence, Opt. Lasers Eng. 56 (2014) 83–93.
[137] J. Wu, X. Liao, B. Yang, Image encryption using 2D Hénon-sine map and DNA approach, Signal Process. 153 (2018) 11–23.
[138] Y. Gangadhar, V.G. Akula, P.C. Reddy, An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation, Biomed. Signal Process. Control 43 (2018) 31–40.
[139] X. Wu, D. Wang, J. Kurths, H. Kan, A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system, Inf. Sci. 349 (2016) 137–153.
[140] P. Campisi, D. Kundur, A. Neri, Robust digital watermarking in the ridgelet domain, IEEE Signal Process Lett. 11 (2004) 826–830.
[141] H.-Y. Yu, J.-L. Fan, X.-L. Zhang, A robust watermark algorithm based on ridgelet transform and fuzzy c-means, in: Information Engineering and Electronic Commerce, 2009. IEEC'09. International Symposium on, IEEE, 2009, pp. 120–124.
[142] H. Liu, H. Nan, Color image security system using chaos-based cyclic shift and multiple-order discrete fractional cosine transform, Opt. Laser Technol. 50 (2013) 1–7.
[143] Z. Liu, L. Xu, T. Liu, H. Chen, P. Li, C. Lin, S. Liu, Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains, Opt. Commun. 284 (2011) 123–128.
[144] E.E. Abdallah, A.B. Hamza, P. Bhattacharya, Improved image watermarking scheme using fast Hadamard and discrete wavelet transforms, J. Electron. Imaging 16 (2007) 033020.
[145] S.P. Maity, M.K. Kundu, Perceptually adaptive spread transform image watermarking scheme using Hadamard transform, Inf. Sci. 181 (2011) 450–465.
[146] T.K. Tsui, X.-P. Zhang, D. Androutsos, Color image watermarking using multidimensional Fourier transforms, IEEE Trans. Inf. Forensics Secur. 3 (2008) 16–28.
[147] V. Solachidis, L. Pitas, Circularly symmetric watermark embedding in 2-D DFT domain, IEEE Trans. Image Process. 10 (2001) 1741–1753.
[148] L. Krikor, S. Baba, T. Arif, Z. Shaaban, Image encryption using DCT and stream cipher, Eur. J. Scient. Res. 32 (2009) 47–57.
[149] S.M. Seyedzade, S. Mirzakuchaki, R.E. Atani, A novel image encryption algorithm based on hash function, in: Machine Vision and Image Processing (MVIP), 2010 6th Iranian, IEEE, 2010, pp. 1–6.
[150] G. Bertoni, D. Joan, P. Michaël, V.A. Gilles, The Keccak sponge function family: Specifications summary, 2011.
[151] C. Boutin, NIST selects winner of secure hash algorithm (SHA-3) Competition-competition, 2012.
[152] A. Kanso, M. Ghebleh, A fast and efficient chaos-based keyed hash function, Commun. Nonlinear Sci. Numer. Simul. 18 (2013) 109–123.
[153] C.E. Dong, Asymmetric color image encryption scheme using discrete-time map and hash value, Optik-Int. J. Light Electr. Opt. 126 (2015) 2571–2575.
[154] R. Enayatifar, A.H. Abdullah, M. Lee, A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption, Opt. Lasers Eng. 51 (2013) 1066–1077.
[155] I. Souici, H. Seridi, H. Akdag, Images encryption by the use of evolutionary algorithms, Analog Integr. Circuits Signal Process. 69 (2011) 49–58.
[156] K. Kuppusamy, K. Thamodaran, Optimized partial image encryption scheme using PSO, in: Pattern Recognition, Informatics and Medical Engineering (PRIME), 2012 International Conference on, IEEE, 2012, pp. 236–241.
[157] X.-L. Chai, Z.-H. Gan, Y. Lu, M.-H. Zhang, Y.-R. Chen, A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system, Chin. Phys. B 25 (2016) 10050301–10050313.
[158] Z.-L. Zhu, W. Zhang, K.-W. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, Inf. Sci. 181 (2011) 1171–1186.
[159] D. Sravanthi, K.A.K. Patro, B. Acharya, S. Majumder, A secure chaotic image encryption based on bit-plane operation, in: Soft Computing in Data Analytics, Springer, Singapore, 2019, pp. 717–726.
[160] Z.-H. Gan, X.-L. Chai, D.-J. Han, Y.-R. Chen, A chaotic image encryption algorithm based on 3-D bit-plane permutation, Neural Comput. Appl. 29 (2018) 1–20.
[161] G. Zhu, W. Wang, X. Zhang, M. Wang, ZGW-1 digital image encryption algorithm based on three levels and multilayer scramble, in: Network Infrastructure and Digital Content, 2010 2nd IEEE International Conference on, IEEE, 2010, pp. 939–943.
[162] Z. Shao, H. Shu, J. Wu, Z. Dong, G. Coatrieux, J.L. Coatrieux, Double color image encryption using iterative phase retrieval algorithm in quaternion gyrator domain, Opt. Express 22 (2014) 4932–4943.
[163] L. Sui, K. Duan, J. Liang, Double-image encryption based on discrete multiple–parameter fractional angular transform and two-coupled logistic maps, Opt. Commun. 343 (2015) 140–149.
[164] X.W. Li, S.J. Cho, S.T. Kim, Combined use of BP neural network and computational integral imaging reconstruction for optical multiple-image security, Opt. Commun. 315 (2014) 147–158.
[165] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, H. Yu, Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains, Opt. Lasers Eng. 66 (2015) 1–9.
[166] R. Kumar, J.T. Sheridan, B. Bhaduri, Nonlinear double image encryption using 2D non-separable linear canonical transform and phase retrieval algorithm, Opt. Laser Technol. 107 (2018) 353–360.
[167] L. Sui, B. Liu, Q. Wang, Y. Li, J. Liang, Double-image encryption based on Yang-Gu mixture amplitude-phase retrieval algorithm and high dimension chaotic system in gyrator domain, Opt. Commun. 354 (2015) 184–196.
[168] Z. Zhong, J. Chang, M. Shan, B. Hao, Double image encryption using double pixel scrambling and random phase encoding, Opt. Commun. 285 (2012) 584–588.
[169] Z. Liu, Y. Zhang, S. Li, W. Liu, W. Liu, Y. Wang, S. Liu, Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains, Opt. Laser Technol. 47 (2013) 152–158.
[170] R. Wei, X. Li, Q.-H. Wang, Double color image encryption scheme based on off-axis holography and maximum length cellular automata, Optik-Int. J. Light Electr. Opt. 145 (2017) 407–417.
[171] O.S. Faragallah, Optical double color image encryption scheme in the Fresnel-based Hartley domain using Arnold transform and chaotic logistic adjusted sine phase masks, Opt. Quantum Electr. 50 (2018) 1–27.
[172] G. Xiong, S. Zheng, J. Wang, Z. Cai, D. Qi, Local negative base transform and image scrambling, Math. Probl. Eng. (2018) (2018) 1–18.
[173] L. Sui, B. Gao, Color image encryption based on gyrator transform and Arnold transform, Opt. Laser Technol. 48 (2013) 530–538.
[174] A. Sinha, K. Singh, Image encryption using fractional Fourier transform and 3D Jigsaw transform, Opt. Eng. 9 (2013) 158–166.
[175] N.K. Nishchal, G. Unnikrishnan, J. Joseph, K. Singh, Optical encryption using a localized fractional Fourier transform, Opt. Eng. 42 (2003) 3566–3572.
[176] R.K.W. Jiancheng Zou, Qi Dongxu, A new digital image scrambling method based on fibonacci number, in: Proceeding of the IEEE Inter Symposium On Circuits and Systems, Vancouver,Canada, 2004, pp. 965–968.
[177] M. Singh, A. Kakkar, M. Singh, Image encryption scheme based on Knight's tour problem, Procedia Comput. Sci. 70 (2015) 245–250.
[178] L. Hong, F. Yi, Modified Knight's tour image encryption algorithm based on Arnold transform, Commun. Technol. 7 (2018) 1663–1670.
[179] T. Zhang, S. Li, R. Ge, M. Yuan, Y. Ma, A novel 1D hybrid chaotic map-based image compression and encryption using compressed sensing and Fibonacci–Lucas transform, Math. Probl. Eng. (2016) (2016) 1–15.

[180] J. Shen, X. Jin, C. Zhou, A color image encryption algorithm based on magic cube transformation and modular arithmetic operation, in: Pacific-Rim Conference on Multimedia, Springer, 2005, pp. 270–280.
[181] S. Sowmiya, I.M. Tresa, A.P. Chakkaravarthy, Pixel based image encryption using magic square, algorithms, methodology, models and applications in emerging technologies (ICAMMAET), in: 2017 International Conference on, IEEE, 2017, pp. 1–4.
[182] X. Chai, Z. Gan, K. Yang, Y. Chen, X. Liu, An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations, Signal Process. Image Commun. 52 (2017) 6–19.
[183] A. Nag, J.P. Singh, S. Khan, S. Biswas, D. Sarkar, P.P. Sarkar, Image encryption using affine transform and XOR operation, Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), in: 2011 International Conference on, IEEE, 2011, pp. 309–312.
[184] H. Chen, X. Du, Z. Liu, C. Yang, Color image encryption based on the affine transform and gyrator transform, Opt. Lasers Eng. 51 (2013) 768–775.
[185] Y. Zhou, W. Cao, C.P. Chen, Image encryption using binary bitplane, Signal Process. 100 (2014) 197–207.
[186] O. Watanabe, A. Nakazaki, H. Kiya, A fast image-scramble method using public-key encryption allowing backward compatibility with JPEG2000, in: Image Processing, 2004. ICIP'04. 2004 International Conference on, IEEE, 2004, pp. 3435–3438.
[187] S.S. Raja, V. Mohan, A review on various image encryption techniques for secure image transmission, Int. J. Adv. Eng. Res. 8 (2014) 1–14.
[188] E.-H. Bensikaddour, Y. Bentoutou, N. Taleb, Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher, J. King Saud Univ. -Comput. Inf. Sci. 3 (2018) 1–7.
[189] Z. Su, S. Lian, G. Zhang, J. Jiang, in: Chaos-based Video Encryption algorithms, Chaos-Based Cryptography, Springer, 2011, pp. 205–226.
[190] Z. Su, G. Zhang, J. Jiang, Multimedia security: a survey of chaos-based encryption technology, in: Multimedia-a Multidisciplinary Approach to Complex Issues, InTech, 2012, pp. 99–124.
[191] R. Guesmi, M. Farah, A. Kachouri, M. Samet, A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2, Nonlinear Dyn. 83 (2016) 1123–1136.
[192] D.S. Monaghan, G. Situ, U. Gopinathan, T.J. Naughton, J.T. Sheridan, Analysis of phase encoding for optical encryption, Opt. Commun. 282 (2009) 482–492.
[193] H.H. Yu, X. Yu, Progressive and scalable encryption for multimedia content access control, in: Communications, 2003. ICC'03. IEEE International Conference on, IEEE, 2003, pp. 547–551.
[194] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Digital image steganography: survey and analysis of current methods, Signal Process. 90 (2010) 727–752.
[195] C. Han, Y. Shen, W. Ma, Iteration and superposition encryption scheme for image sequences based on multi-dimensional keys, Opt. Commun. 405 (2017) 101–106.
[196] L. Liu, Q. Zhang, X. Wei, A RGB image encryption algorithm based on DNA encoding and chaos map, Comput. Electr. Eng. 38 (2012) 1240–1248.
[197] N. Zhou, H. Li, D. Wang, S. Pan, Z. Zhou, Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform, Opt. Commun. 343 (2015) 10–21.
[198] J. Wu, X. Luo, N. Zhou, Four-image encryption method based on spectrum truncation, chaos and the MODFrFT, Opt. Laser Technol. 45 (2013) 571–577.
[199] A. Akhavan, A. Samsudin, A. Akhshani, Hash function based on piecewise nonlinear chaotic map, Chaos, Solitons Fractals 42 (2009) 1046–1053.
[200] P. Dahake, S. Nimbhorkar, Review on various methods for secure transmission of images for maintaining image integrity, IJCSN J. 3 (2014) 450–454.