Archives of Computational Methods in Engineering (2020) 27:15–43
https://doi.org/10.1007/s11831-018-9298-8

ORIGINAL PAPER

A Comprehensive Review on Image Encryption Techniques

Manjit Kaur[1] · Vijay Kumar[1]

Received: 11 April 2018 / Accepted: 12 November 2018 / Published online: 24 November 2018

Abstract
Image encryption techniques play a significant role in multimedia applications to secure and authenticate digital images. This paper presents a comprehensive study of various image encryption techniques. This paper covers the most significant developments in meta-heuristic based image encryption techniques. The various attacks and performance measures related to image encryption techniques have also been studied. The existing techniques are analyzed with respect to differential, statistical, and key analyses. The main goal of this paper is to give a broad perspective on characteristics of image encryption techniques. The paper concludes by discussing significant advancements in the field of image encryption and highlighting future challenges.

1 Introduction

Due to advancement in distributed computer networks, storage devices, and imaging tools, the digital images have been extensively used in various fields [1]. As images are communicated over public networks, they are prone to various security threats such as eavesdropping, illegal modification, duplication, etc. Therefore, securing the image in an efficient manner has received much attention in last few years. Figure 1 shows the classification of information security techniques. The security system is divided into two parts namely information hiding techniques and cryptography. The information hiding techniques are further decomposed into watermarking and steganography.

In case of cryptography, the actual data is converted into meaningless form before communicating over public networks. Image encryption algorithms are the most important strategies to protect the images [2]. Steganography injects given information into a cover media like digital images, audio signals or videos, to hide its existence. Thus, steganography achieves information hiding in such a way that no one can recognize the existence of data except the intended receiver. Whereas, in case of cryptography, the existence of information is not hidden but its values are obscured [3]. In digital watermarking, the digital contents are embedded with a unique identification signal known as watermark. To authenticate the digital contents, watermark will be extracted from the watermarked image at receiver end. The digital contents can be audio, image, video, and text. Whenever the watermarked images are found to be illegally reused, the embedded watermark can be extracted to verify the ownership claims [4, 5].

1.1 General Framework

Figure 2 illustrates the general framework of image encryption techniques. An input image that needs to be encrypted is called a plain-image and encrypted image is known as a ciphered image. The plain and ciphered images are represented by P and C, respectively. The encryption process is demonstrated as

$$C = EF_{EK}(P) \tag{1}$$

where $EF()$ is the encryption function that applied on P using encryption key (EK). Similarly, at receiver end, the decryption process retrieves the original image using decryption key (DK) and decryption function ($DF()$) as follows:

$$P = DF_{DK}(C) \tag{2}$$

The image encryption techniques can be divided as symmetric and asymmetric techniques. In case of symmetric image encryption, the encryption and decryption keys are same, *i.e.*, $EK = DK$. The keys are to be kept secret during

✉ Manjit Kaur
dr.kaurmgill@gmail.com

[1] Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala, Punjab 147001, India

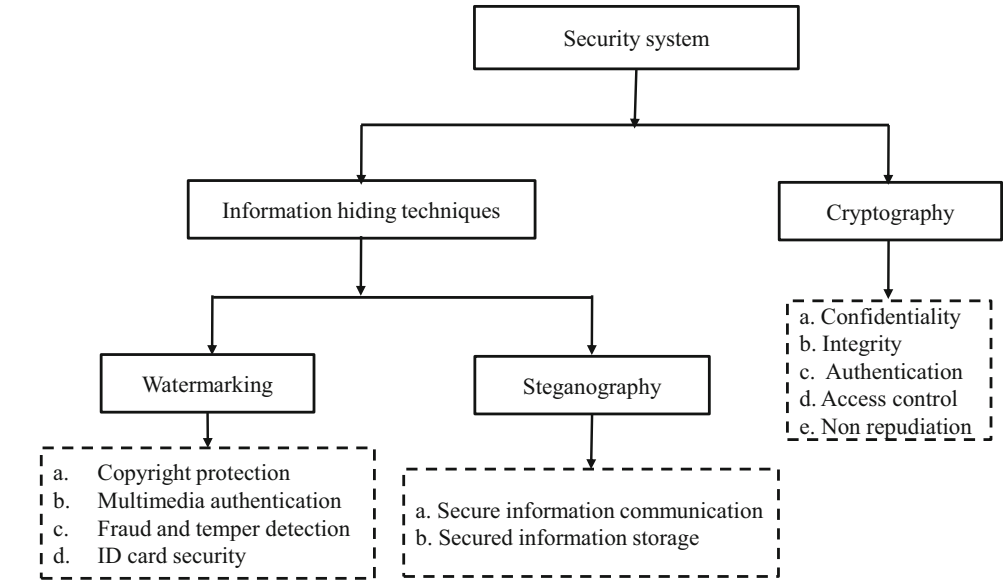

Fig. 1 Classification of information security techniques

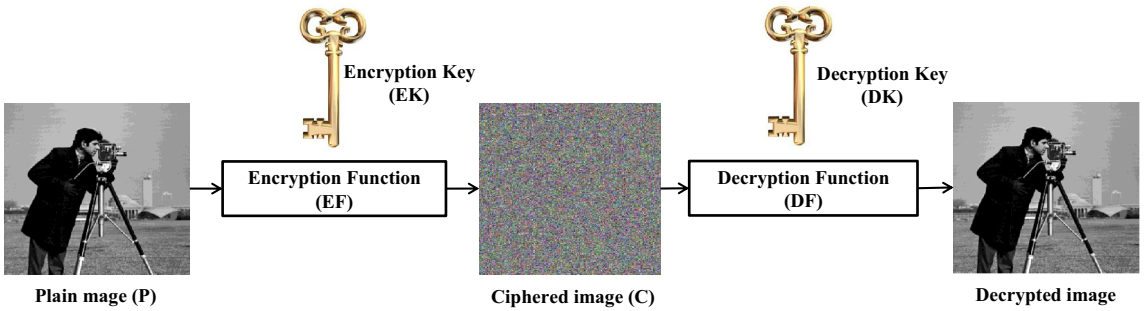

Fig. 2 Generic framework of image encryption techniques

the communication. When different keys are used for encryption and decryption, the image encryption is known as asymmetric image encryption, i.e., $EK \neq DK$. In this system, EK is taken as public whereas DK is kept private.

The motivation behind this study is to explore various issues associated with the existing image encryption techniques. This paper provides a survey of current image encryption techniques with their pros and cons. The purpose of this paper is three folds:

(i) There is hardly any literature found on meta-heuristic based image encryption techniques. This is the reason that we decided to do a systematic study of existing image encryption techniques.
(ii) Meta-heuristic based image encryption techniques outperform existing techniques especially against various cryptanalysis. Therefore, it becomes necessary to study the existing cryptanalysis techniques.
(iii) Each image encryption technique has its own benefits and limitations. Some techniques are robust against various attacks but suffer from computational speed. Therefore, it is necessary to study the trade-off between computational speed and performance against various security attacks.

The main contributions of this paper are:

(i) A comprehensive study has been conducted to explore various image encryption techniques, especially meta-heuristic encryption techniques.
(ii) The various attacks and performance measures related to image encryption techniques have also been studied.
(iii) The existing techniques have been analyzed with respect to differential, statistical, and key analyses.
(iv) The future research directions which inhibit the design of efficient image encryption techniques have been explored.

The remaining structure of this paper is as follows: The performance metrics of image encryption techniques are explained in Sect. 2. Section 3 presents the brief description of existing image encryption techniques. Section 4 discusses

comparative analyses based on quality metrics. The study of various cryptanalysis techniques is presented in Sect. 5. Section 6 demonstrates the various applications of image encryption. Sections 7 and 8 discuss the applications and future research directions of image encryption. The concluding remarks are presented in Sect. 9.

2 Evaluation Measures

Evaluation measures are very necessary to confirm the effectiveness of image encryption technique. The various characteristics of an image encryption algorithm are explored using these parameters.

2.1 Differential Analysis

Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) parameters are used to analyze the differential attacks. The differential attack is used to tests the sensitivity of encryption algorithm toward slightest changes in plain image. Attackers often make a slight change in the original image. Then, encrypt the original and modified images using same secret key. Afterwards, try to find the relationship between encrypted images of original and modified images.

2.1.1 Number of Pixel Change Rate (NPCR)

It is defined as the percentage of different pixel numbers between two encrypted images, whose plain images have only one pixel difference. If any technique provides high value of NPCR, then the algorithm is better against differential attacks [6]. NPCR can be computed as follows [6]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100 \tag{3}$$

Here,

$$D(i,j) = \begin{cases} 0 & \text{if } E(i,j) = E'(i,j) \\ 1 & \text{if } E(i,j) \neq E'(i,j) \end{cases} \tag{4}$$

where W and H represent width and height of image, respectively. $D(i, j)$ indicates the difference between corresponding pixels of encrypted image of original image ($E'(i, j)$) and encrypted image of changed image ($E(i, j)$). The range of NPCR $\in$ [0, 100]. NPCR value of an encrypted image should be close to 100.

2.1.2 Unified Average Changing Intensity (UACI)

It measures the average intensity of difference between two encrypted images, corresponding to plain images that have one pixel difference [7]. It can be defined as follows [8]:

$$UACI = \frac{\sum_{i,j} E(i,j) - E'(i,j)}{255 \times W \times H} \times 100 \tag{5}$$

where $E(i, j)$ and $E'(i,j)$ are the encrypted images of original and changed images, respectively. The values of NPCR and UACI need to be maximized.

2.2 Statistical Analysis

The encryption techniques can also be broken using the statistical analysis of an encrypted image. Histogram Analysis (HA) and Correlation Coefficient (CC) are used to analyze the adjacent pixels of an encrypted image to confirm the robustness of an encryption technique against statistical attacks.

2.2.1 Histogram Analysis (HA)

It reveals the distribution of pixel values of an image. The histogram of original image should be totally different from the histogram of an encrypted image. The histograms of plain images are non-uniform in nature. While the histograms of encrypted images should be uniform in nature [2]. It means that all pixels are distributed equally in the space. Figure 3 shows the histograms of plain and encrypted Lena images. Figure 3b shows the histogram of plain Lena image in which pixels are not uniform. From Fig. 3d, it can be observed that pixels of an encrypted image are uniformly distributed.

2.2.2 Correlation Coefficient (CC)

It is used to find the similarity between corresponding pixels of an original and encrypted image. The values of adjacent pixels of an original image are strongly correlated in three directions, *i.e.,* horizontal, diagonal, and vertical. The good image encryption technique is one which reduces this relationship in ciphered image [9]. Correlation coefficient can be computed as follows [10]:

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}} \tag{6}$$

Here,

$$C(x,y) = \frac{\sum_{i=1}^{K} (x_i - E(x))(y_i - E(y))}{K} \tag{7}$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K} (x_i - E(x))^2 \tag{8}$$

$$D(y) = \frac{1}{K}\sum_{i=1}^{K} (y_i - E(y))^2 \tag{9}$$

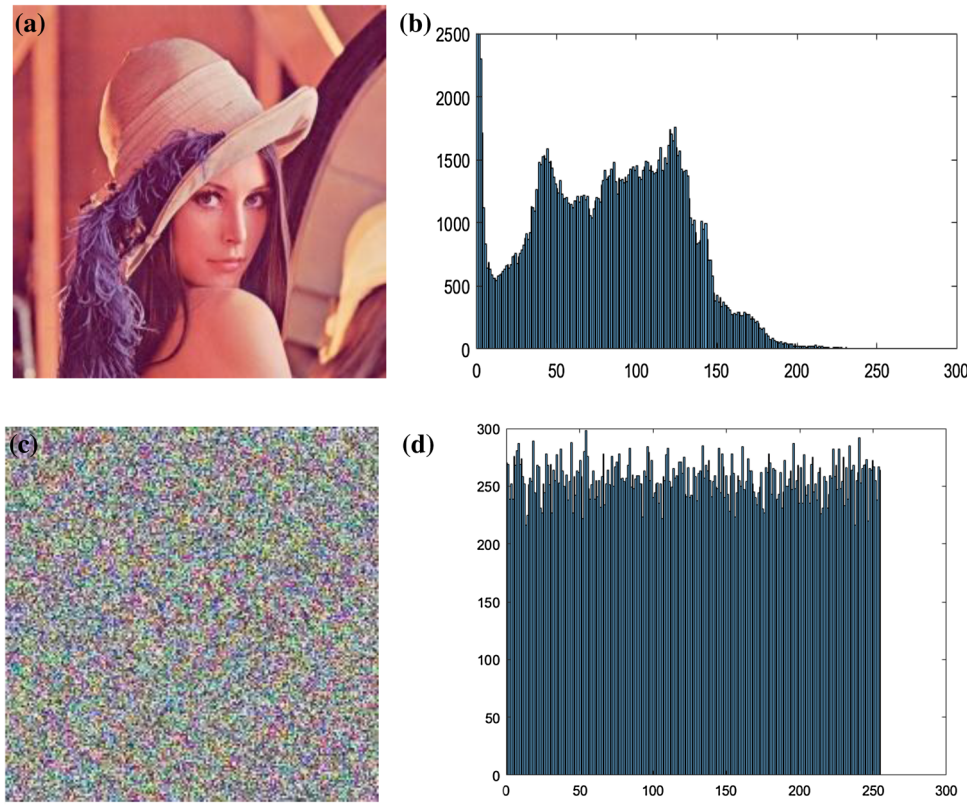

Fig. 3 **a** Plain Lena image, **b** histogram of plain image, **c** encrypted Lena image, and **d** histogram of encrypted image

where $C(x, y)$ is the covariance between samples x and y. x and y are the coordinates of an image. K is the number of pixel pairs (x_i, y_i). $D(x)$ and $D(y)$ are the standard deviation of x and y, respectively. $E(x)$ is the mean of x_i pixel values. The range of CC$\in [-1, 1]$. The CC value of an encrypted image should be near to 0.

2.3 Information Entropy (IE)

It measures the average information per bit in an image. It contains the possible information available in the given image. Each pixel has different value. Therefore, the entropy of an encrypted image means each pixel has equal probability with uniform distribution [11]. It can be computed as:

$$H(S) = -\sum_{s}(P(s_i) \times \log_2 P(s_i)) \tag{10}$$

where $H(S)$ represents the entropy of message source (S). $P(s_i)$ denotes the probability of occurrence of s_i. The value of $IE \in [0, 8]$. It should be close to 8 for 8-bit image.

2.4 Key Analysis (KA)

Security keys are the core part of any encryption algorithm as the strength of algorithm depends on it. The secret keys should be strong enough to resist all types of attacks. The desirable properties of strong secret keys are large key space and high sensitivity [1]. The key space depends on the size of secret key. If the size is large, then it is harder for an attacker to estimate the same key. Key sensitivity means that if attacker modify even a single pixel in the original key, then the original image remains unrecoverable.

2.5 Noise Attack (NA)

To destroy the useful information, attacker may introduce noise in the encrypted image. Due to this, the intended user cannot recover the original image successfully after decryption. The attacker introduce additive, Gaussian, Poisson noise, etc. in the encrypted image [2]. Therefore, an efficient image encryption technique should be resistant to noise attacks.

2.6 Execution Time (ET)

Execution time (ET) is measured as the time required to execute a given image encryption technique. It is the aggregation of compile and run time. For practical implementation of image encryption, ET should be minimum. It is generally measured in seconds, milliseconds or minutes [12].

2.7 Bit Correct Ratio (BCR)

BCR is used to estimate the difference between an original image and decrypted image. It checks the correctness of decrypted image [13]. It can be calculated as [13] follows:

$$BCR = \left(1 - \frac{\sum_{x,y}^{M\times N} O(x,y) \oplus R(x,y)}{M \times N}\right) \tag{11}$$

where x and y are the pixel coordinates of images having size of $M \times N$ pixels. O is an original image and R is the decrypted image. $\oplus$ represents the XOR operation. The range of $BCR \in [0, 1]$.

2.8 Mean Squared Error (MSE)

MSE helps to compare the "true" pixel values of an original image to decrypted image. The error is amount by which the values of an original image differ from decrypted image [14]. MSE can be defined as follows:

$$MSE = \frac{1}{MN}\sum_{x=1}^{x=M}\sum_{y=1}^{y=N}[O(x,y) - R(x,y)]^2 \tag{12}$$

where x and y are the pixel coordinates of images with size of $M \times N$ pixels. O and R are the original and decrypted images, respectively. The value of $MSE \in [0, \infty]$. The value of MSE between original and decrypted should be minimum.

2.9 Peak Signal to Noise Ratio (PSNR)

PSNR is used as a quality measurement between the original and decrypted images [15]. PSNR can be mathematically computed as follows:

$$PSNR = 10\log_{10}\frac{(2^n - 1)^2}{MSE} \tag{13}$$

where n represents the number of bits per pixel. $PSNR$ is measured in decibel (dB). The value of $PSNR \in [0, \infty]$. The value of PSNR should be maximum between original and decrypted images.

2.10 Signal to Distortion Ratio (SDR)

SDR measures the rate of distortion between the pixel values of an original and decrypted images [16]. It is calculated as:

$$SDR = 10\log_{10}\frac{\sum_{x,y} O(x,y)^2}{\sum_{x,y}(O(x,y) - D(x,y))^2} \tag{14}$$

where $O(x, y)$ and $D(x, y)$ represent the original and decrypted images, respectively. x and y are the pixel coordinates of images with size of $M \times N$. SDR is measured in decibel units. The value of $SDR \in [0, \infty]$. The SDR value between original and decrypted images should be minimum.

2.11 Structural SIMilarity Index (SSIM)

SSIM reveals the similarity between original and decrypted images. It is quality assessment parameter of decrypted image. It is calculated between various windows of images having same size [16]. It can be defined as follows:

$$SSIM = \frac{(2\mu_I\mu_D + C_1)(2\sigma_{ID} + C_2)}{(\mu_I^2 + \mu_D^2 + C_1)(\sigma_I^2 + \sigma_D^2 + C_2)} \tag{15}$$

where μ_I and μ_D represent the average of an input (I) and decrypted (D) images, respectively. σ_I^2 and σ_D^2 represent the variance of I and D, respectively. σ_{ID} represents the covariances of I and D. C_1 and C_2 are the regularization constants with value $(0.01P)^2$ and $(0.03P)^2$. where P is the specified dynamic range value. The range of $SSIM \in [-1, 1]$.

2.12 Root Mean Squared Error (RMSE)

RMSE evaluates the root of MSE to give more precise and accurate data [17]. It can be mathematically computed as:

$$RMSE = \sqrt{\frac{\sum_{x=1}^{M}\sum_{y=1}^{N}[O(x,y) - D(x,y)]^2}{MN}} \tag{16}$$

where x and y are the pixel coordinates of images with size of $M \times N$. O and D are the original and decrypted images. The range of $RMSE \in [0, \infty]$.

2.13 Mean Absolute Error (MAE)

MAE measures the difference between encrypted and original images [18]. It can be evaluated as:

$$MAE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}|O(x,y) - E(x,y)| \tag{17}$$

where $O(x, y)$ and $E(x, y)$ denote original and encrypted images, respectively. x and y are the pixel coordinates of image with size of $M \times N$. The range of $MAE \in [0, 2^n - 1]$, where n is number of bits per pixel. It should be maximum between original and encrypted images.

2.14 Signal to Noise Ratio (SNR)

SNR evaluates the results of an encryption algorithm quantitatively [19]. It can be computed as:

$$SNR = \frac{\sum_{m,n}[O(m,n)]^2}{\sum_{m,n}[O(m,n) - D(m,n)]^2} \quad (18)$$

where $O(m, n)$ and $D(m, n)$ represent original and decrypted images, respectively, with pixel coordinates m and n. The range of $SNR \in [1, \infty]$. The value of SNR should be maximum between original and decrypted images.

3 Image Encryption Techniques

In this section, the classification of image encryption techniques is presented. Image encryption techniques are broadly classified into four categories, i.e., optical, spatial, transform domain, and compressive sensing. Figure 4 shows the classification of image encryption techniques. The above-mentioned image encryption techniques are described in the preceding subsections.

Comparison between these image encryption techniques is also carried out using certain performance metrics. These metrics are NPCR, UACI, KA, HA, CC, IE, NA, KCPA and speed. Here, ✔ means given technique has considered the corresponding metric. In the same way, ✗ states that given technique has not considered the respective metric.

3.1 Spatial Domain Based Image Encryption Techniques

The term spatial domain refers to the image plane itself which is direct manipulation of pixels. Spatial domain based techniques are those techniques which are directly applied on these pixels. The various spatial domain based techniques have been discussed in subsequent sections.

3.1.1 Chaos Based Image Encryption Techniques

Chaotic maps are studied in dynamic environment as they exhibit chaotic behaviour. It means that small change in initial conditions can produce drastic change in outputs. These maps are categorized as discrete maps and continuous maps. Chaotic maps are extensively utilized in secure

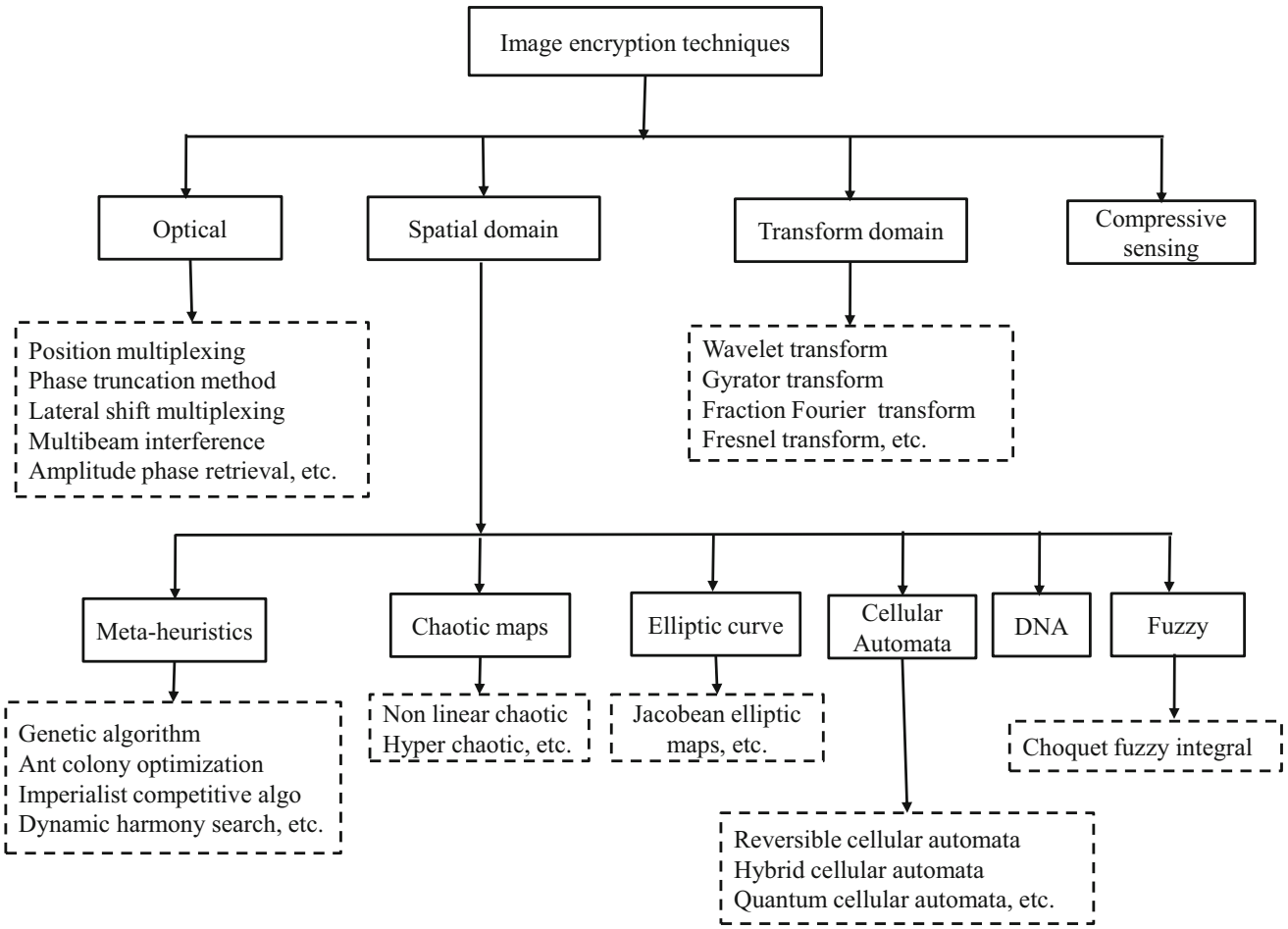

Fig. 4 Classification of image encryption techniques

communication and considered favorable trade-off between security and computational speed. The chaos-based encryption technique possesses several features such as sensitivity to initial circumstances, determinacy, and ergodicity [20].

The chaotic maps divide an image into dual phases, i.e., diffusion and permutation to generate a cipher. In real time, cryptosystems developers may integrate permutation and diffusion to attain a significant computational security.

Figure 5 depicts the process of chaos-based image encryption technique. The permutation or confusion phase shuffles the image circularly using pseudo-random sequence based on plain image. It resolves key dependent problem. In diffusion phase, scrambled image is decomposed into several blocks. It selects preceding block in order to update the pre-conditions of chaotic map. Therefore, the key sequence relies on the given image [21].

Table 1 shows the variants of chaotic map that have been used in the field of image encryption. The categorization of these variants have been done by considering the time domain, spatial domain, number of dimensions (Dim.) and number of parameters (Para.). It has been observed that each map requires different number of parameters to develop a secure key.

Thus, chaotic maps have been widely used in different applications. The overview of chaos-based image encryption techniques has been discussed below.

Pareek et al. [31] used two logistic maps and one external key to encrypt an image. The initial conditions of logistic maps are derived from external key. The secret key is modified every time after encrypting the block of sixteen pixels of an image. Therefore, it is difficult for an attacker to discover the secret key. However, it is not sensitive toward the input images.

Behnia et al. [36] combined one-dimensional chaotic map with coupled map lattice to encrypt an image. This combination provides a large key space and high-level security. However, this method has low sensitivity towards input image as initial conditions of chaotic maps are not dependent on the input image.

Gao et al. [29] implemented the hyper-chaotic map in image encryption to reduce the prediction time than simple chaotic maps based image encryption techniques. In this technique, shuffling of matrix is utilized to permute the pixels of an input image. Thereafter, hyper-chaotic map is used to diffuse the pixel values of shuffled image. This technique provides better key space and high security.

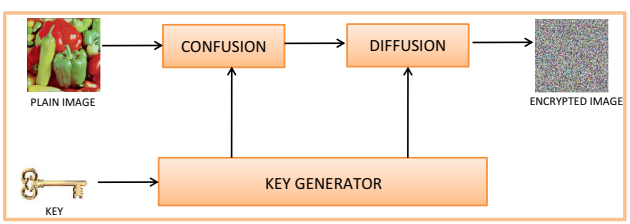

Fig. 5 Image encryption using chaotic maps [21]

Ye et al. [37] used logistic map to encrypt the images. In this technique, permutation is performed at bit level. This technique is robust against various security attacks. However, this technique suffers from known-plaintext and chosen-plaintext attacks [38].

Zhu et al. [39] proposed an image encryption technique that performs permutation and diffusion at bit-level. In this technique, Arnold map and logistic map are utilized to perform permutation and diffusion operations. This method is computationally efficient than the other image encryption techniques. However, permutation based image encryption techniques are prone to known-plaintext and known-ciphertext attacks [40, 41].

Mirzaei et al. [42] implemented an image encryption technique in parallel fashion. In this technique, an image is sub-divided into four blocks. Thereafter, chaotic map is used to shuffle these blocks. Then, each block is encrypted in parallel scheme by changing the pixel values of each block. This technique has better computational speed.

Kanso et al. [43] utilized three dimensional Arnold transform to generate secret keys to encrypt the images. This technique is divided into three phases such as shuffling, scrambling, and masking. This technique is highly sensitive towards an input image. It provides better security against known-plaintext and chosen-plaintext attacks. Wang et al. [44] designed an image encryption technique that performs selective encryption using spatial chaotic maps. It chooses first 4-bits of each pixel for encryption. It shows that encrypting only 50 % pixels of an input image provides better encryption results.

Khan and Shah [19] implemented the S-box in a chaotic manner using affine and Lorenz transforms to improve the algebraic and statistical properties of S-box. S-box is mainly used in block encryption to create confusion among pixels. It provides better confusion and diffusion to protect the input image against security attacks.

Zhang and Wang [45] proposed an image encryption technique based on mixed linear-nonlinear coupled map lattices. The mixed linear and nonlinear coupled map lattices overcome the issues of large periodic windows in bifurcations and small range of parameters. These maps are used to permute and diffuse an input image at bit level to generate an encrypted image.

Wang et al. [46] proposed an image encryption technique based on random integer cycle shift and one-dimensional chaotic map. In this technique, cycle shift technology is used to change the pixel values of an input image. It is used in image encryption because of its easy

Table 1 Variants of chaotic map

References	Chaotic maps	Time domain	Space domain	Dim.	Para.
[22]	2D Rational map	Discrete	Rational	2	2
[23]	3-cells CNN system	Continuous	Real	3	4
[24]	Arnold's cat map	Discrete	Real	2	0
[25]	Baker's map	Discrete	Real	2	0
[26]	Chen attractor	Continuous	Real	3	2
[27]	Circle map	Discrete	Real	1	2
[28]	Exponential map	Discrete	Complex	2	1
[29]	Hyper logistic map	Discrete	Real	2	3
[30]	Hnon map	Discrete	Real	2	2
[31]	Logistic map	Discrete	Real	1	1
[32]	Lorenz attractor	Continuous	Real	3	3
[33]	Tent map	Discrete	Real	1	1
[34]	Tinkerbell map	Discrete	Real	2	4
[35]	Zaslavskii map	Discrete	Real	2	4

implementation; and it can be extended to any size of image.

Belazi et al. [6] improved scrambling technique using permutation-substitution arrangement and chaotic techniques. This technique has better security analysis and good key space. It consists of four cryptographic phases such as diffusion, substitution, diffusion, and permutation. These phases are carried out by enhanced chaotic map, S-box, logistic map, and permutation function to enhance the performance.

Liu et al. [47] improved the key space of [48] using two-dimensional Sine map and iterative chaotic map with infinite collapse modulation map (2D-SIMM). The permutation and diffusion processes are combined into one step to reduce the computational time.

To overcome the problem of fixed-point and dynamic key space of one-dimensional chaotic systems, Farajallah et al. [49] proposed three chaotic systems for image encryption. It is very effective against various security attacks and has good computational speed.

Chen et al. [50] designed a four-dimensional discrete chaotic map using sine function with one-line equilibrium to encrypt the images. The key space generated by chaotic map is greater than 2^{1170}. It provides significant avalanche effect as compared to other image encryption techniques.

Hua et al. [51] used the concept of image filtering in image encryption to enhance security. The image filtering can spread little change of plain-images to entire pixels of cipher-images. This technique provides better results than the existing image encryption techniques in terms of statistical and differential attacks.

Pak and Huang [52] developed a new chaotic system using the difference of output sequences of two same chaotic systems which removes the drawbacks of a single chaotic map. The image encryption is performed by permutation-diffusion-permutation architecture. However, the authors have not discussed the strength of image encryption technique against known-plaintext attacks.

Li et al. [53] discussed a permutation and diffusion architecture in which permutation is performed at pixel level as well as bit level to encrypt an image. This technique used 5-D chaotic map to overcome the drawbacks of low dimensional chaotic maps.

Table 2 shows the performance comparison of chaos-based image encryption techniques. From the table, it has been observed that not even a single technique fulfills all the performance criteria.

3.1.2 DNA Based Image Encryption Techniques

In recent years, Deoxyribonucleic Acid (DNA) technology has impacted the various domains such as medical system, information science, *etc.* DNA molecules contain genetic code which store the data and can transform from one genetic code into another. In recent times, researchers have designed a simulation environment of biological experiments on DNA technology named as pseudo-DNA technology. This idea has been promoted the development of DNA in the field of encryption [59].

Figure 6 shows the block diagram of DNA-based image encryption process. Initially, the image is decomposed into Red (R), Green (G) and Blue (B) color channels. These three channels are transferred into binary matrices. DNA encoding rules are then applied to encode these matrices. To scramble the similarity between pixel values, DNA operations are applied on the encoded matrices. The decoding rules are then applied to convert them again into binary matrices. Finally, three color channels are combined to attain a cipher colored image [60].

Table 2 Comparison between chaos based image techniques

References	NPCR	UACI	KA	HA	CC	IE	NA	KCPA	Speed
[54]	✗	✗	✔	✔	✔	✗	✗	✔	Poor
[31]	✔	✗	✔	✔	✔	✗	✗	✗	Good
[36]	✔	✔	✔	✔	✔	✔	✗	✗	Good
[29]	✗	✗	✔	✔	✔	✗	✗	✗	Poor
[55]	✔	✔	✔	✔	✔	✔	✗	✔	Good
[39]	✔	✔	✔	✔	✔	✔	✗	✗	Good
[42]	✗	✗	✔	✔	✔	✔	✔	✗	Good
[43]	✔	✔	✔	✔	✔	✔	✗	✔	Good.
[44]	✔	✔	✔	✔	✔	✔	✗	✗	Good
[45]	✔	✔	✔	✔	✔	✔	✗	✗	Good
[46]	✔	✔	✔	✔	✔	✔	✗	✗	Avergae
[56]	✗	✗	✔	✔	✔	✗	✔	✗	Average
[6]	✔	✔	✔	✔	✔	✔	✗	✗	Average
[57]	✗	✗	✔	✔	✔	✗	✔	✔	Average
[58]	✔	✔	✔	✔	✔	✔	✗	✔	Good
[47]	✔	✔	✔	✔	✔	✔	✗	✗	Good
[49]	✔	✔	✔	✔	✔	✔	✗	✔	Good
[50]	✗	✗	✔	✔	✔	✔	✗	✗	Good
[52]	✔	✔	✔	✔	✔	✔	✔	✗	Average
[53]	✔	✔	✔	✔	✔	✔	✗	✗	Good

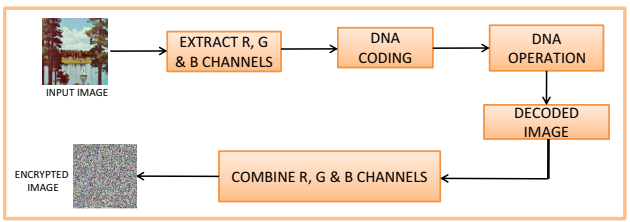

Fig. 6 Block diagram of DNA based encryption scheme [60]

The main reason for using DNA in image encryption are massive parallelism, ultra-low power consumption, and huge storage [46].

Wu et al. [61] proposed three improved one-dimensional chaotic maps with DNA sequences for color images cryptosystem. The input image and key stream are converted into matrices using DNA encoding rule. Thereafter, XOR and complementary operations are applied to scramble the matrices. The scrambled matrices are divided into equal blocks and shuffle them randomly. DNA addition and XOR operations performed on these matrices to get encrypted image. This technique resists against chosen and known-plain text attacks because three chaotic maps are used to generate a key stream that depends on both input image and secret keys.

Wang et al. [46] proposed an image encryption algorithm based on DNA sequence and coupled map lattice. The initial conditions for coupled map lattice are generated through extended hamming distance. The same key can be used to encrypt more than one images. Initially, XOR operation is performed on the pixels of input image by using coupled map lattice. DNA encoding rules are used to encode the confused image to obtain DNA matrix. Furthermore, the shuffled DNA matrix is diffused using coupled map lattice. The final encrypted image is attained by decoding the DNA rule. However, this technique is not sensitive toward the input image.

Kumar et al. [62] used combination of DNA encoding rules and Elliptic Curve Diffie-HEllman (ECDHE) for efficient image cryptography. First, the colored image is encoded using DNA encoding rules to obtain confused RGB matrices and then DNA operations are applied on these matrices. Finally, asymmetric ECDHE cryptography is applied on the image for encryption. The main benefit of this technique is to provide perfect forward secrecy and generate same security with small key size.

Li et al. [60] developed an improved image encryption technique for color images. The quaternary coding is used in DNA sequence to improve the encoding efficiency and enhance the security of keys by using complex and real chaotic maps. The hamming distance is used to generate one-time pad which further scramble the input image. This technique enhances the encoding efficiency of DNA based image encryption techniques.

Wang et al. [63] developed a DNA matrix by utilizing three color channels. Then, spatiotemporal chaos system is used to scramble the image. The hamming distance is

utilized to permute DNA matrix. This technique has an ability to encrypt large size color images.

Mondal and Mandal [65] discussed a light weight image encryption technique by using pseudo random number and DNA. Two level encryption strategy is utilized. The encrypted technique have the ability to handle any kind of attack. However, the noise attack analysis has not been done in this technique.

Chai et al. [7] utilized complex chaotic systems and DNA rules to encrypt the plain images. Initially, color image is encoded using DNA rules. Thereafter, complex chaotic map is used to encrypt the encoded image. This technique is very effective against noise a and known-plaintext attacks.

Table 3 shows the comparison of DNA based image encryption techniques. DNA based image encryption techniques satisfy almost all of the performance metrics (can be seen from Table 3). However, these techniques have poor computational speed as compared to chaos based image encryption techniques.

3.1.3 Cellular Automata Based Image Encryption Techniques

Cellular Automata (CA) consists of cells which reside on grid with different form of structures. These structures evolve through some finite time steps according to the specified rules based on states of neighboring cells. Therefore, CA simulates the complex structures. The huge amount of CA regulations allow several techniques to develop sequences. It evolves through straightforward logic calculations, with pseudo-random and difficult behaviors. The reversible CA is extensively utilized by developers to execute block encryption technique. The main benefits of CA in encryption are huge amount of rules space and parallelism [65]. With the use of CA, image encryption techniques become lossless and adaptive for real-time applications. It also provides high security and fast operation [66]. Figure 7 shows the image encryption using cellular automata.

Wang and Luan [67] proposed a new scheme for image encryption using the combination of chaotic map and reversible CA. The confusion stage uses the chaotic map to generate key stream which permutes the bits of an image. In this scheme, an image is divided into units and each unit contains 4 bits. The diffusion stage considers only higher 4 bits of each pixel because these higher bits provide all information about an image. The diffusion is achieved by applying reversible CA.

Bakhshandeh and Eslami [68] developed a new technique for image encryption based on chaotic maps, CA, and permutation-diffusion architecture. A piecewise linear chaotic map is used to permute the image in permutation phase. The diffusion phase uses logistic map and reversible memory CA to diffuse the permuted image to obtain a secure image. This technique has an authentication ability.

Ping et al. [69] proposed an image encryption scheme in which diffusion and confusion processes are done with the help of CA. CA generates good random sequences to create a scrambled image. Diffusion process uses the interaction between the local cells whereas confusion process is achieved through CA rules by applying on these cells.

Li et al. [13] proved that the integral imaging based encryption procedures have an ability to implement secure and strong image cryptography. It focuses on depth-adaptation integral images and Hybrid Cellular Automata (HCA). Initially, the actual image is divided into an elemental array by utilizing the depth-transformed integral technique. The evaluated elemental images are scrambled by utilizing HCA based chaotic maps. The superiority of this technique is its depth-transformed characteristic which consequently minimizes the magnification factor.

Mohamed [70] used CA to realize parallelization in image cryptography. The reversible CA is used to construct pseudo-random permutation which is used on different blocks independently. The plain image is decomposed into blocks.Thereafter, the secret keys and nonce are applied to encrypt each block independently. This technique is computationally fast as compared to other techniques.

Table 3 Comparison between DNA based image encryption techniques

References	NPCR	UACI	KA	HA	CC	IE	NA	KCPA	Speed
[61]	✔	✔	✔	✔	✔	✔	✔	✔	Poor
[46]	✔	✔	✔	✔	✔	✔	✗	✔	Average
[62]	✗	✗	✔	✔	✔	✗	✔	✔	Poor
[60]	✗	✗	✔	✔	✔	✔	✔	✗	Average
[63]	✔	✔	✔	✔	✔	✔	✗	✗	Poor
[64]	✔	✔	✔	✔	✔	✔	✗	✗	Good
[7]	✔	✔	✔	✔	✔	✔	✔	✔	Poor

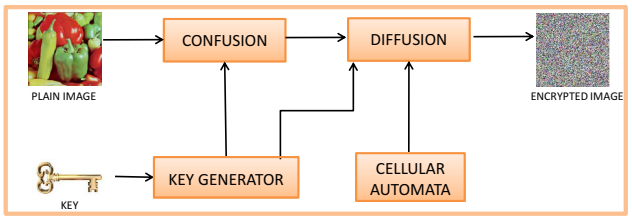

Fig. 7 Image encryption using cellular automata [65]

Enayatifar et al. [71] introduced a hybrid model for image encryption which contains chaotic map, DNA, and CA. The input image is encrypted by using the sequences and operators of DNA with the help of CA. The rule number is selected through chaotic map. It suffers from poor computational speed.

Yang et al. [72] utilized a quantum CA in image encryption. The primary benefit of this technique is that it has time complexity of $O(n)$ which is less than the traditional quantum encryption technique $O(n^2)$.

Li et al. [73] designed an image encryption technique that uses depth-conversion integral imaging and CA to enhance the security. Depth-converted integral imaging technique is used to decompose the input image into an elemental image array. Thereafter, CA and chaotic map is utilized to encrypt the image. This technique reduces the magnification factor that degrades the reconstruction process.

Chai et al. [10] employed the memristive hyper-chaotic system, CA, and DNA sequence operations for image encryption. SHA-256 hash function is used to generate the secret key and compute the initial values of chaotic system. Moreover, a dynamic DNA encoding scheme is introduced. This method has an ability to resist known-plaintext and noise attacks.

Yaghouti Niyat et al. [74] proposed a non-uniform CA framework for image encryption to solve the problems of limited number of reversal rules. The key image is created using non-uniform CA and then hyper-chaotic mapping is used to select random numbers for encryption.

The image encryption techniques based on 2D CA masks provide encryption results with horizontal patterns. To overcome this issue, Li et al. [66] proposed an image encryption algorithm based on CA. In this technique, CA pixel-permutation is used to break the established orders of pixels. It provides large key space and highly sensitive towards secret keys.

The comparison between cellular automata based image encryption techniques has been depicted in Table 4. The most of techniques provide better results in terms of performance measures. The speed of these techniques is comparable to DNA-based image encryption techniques.

Table 4 Performance comparison of cellular automata based image encryption techniques

Ref.	NPCR	UACI	KA	HA	CC	IE	NA	KCPA	Speed
[67]	✔	✔	✔	✔	✔	✔	✗	✗	Average
[68]	✔	✔	✔	✔	✔	✔	✗	✔	Poor
[69]	✔	✔	✔	✔	✔	✔	✗	✔	Good
[70]	✗	✗	✔	✔	✔	✔	✗	✔	Average
[13]	✗	✗	✗	✗	✗	✗	✔	✗	Good
[71]	✔	✔	✔	✔	✔	✔	✗	✗	Average
[72]	✔	✔	✔	✔	✔	✔	✔	✗	Good
[73]	✗	✗	✔	✔	✔	✗	✔	✗	Good
[10]	✔	✔	✔	✔	✔	✔	✔	✔	Good
[74]	✔	✔	✔	✔	✔	✔	✔	✗	Average
[66]	✗	✗	✔	✔	✗	✗	✔	✔	Good

3.1.4 Meta-heuristics Based Image Encryption Techniques

Meta-heuristic techniques play a significant role to optimize the NP-Hard problems. The advantage of these techniques is to optimize the constant parameters required by encryption process. Evolutionary algorithms (EAs) have the ability to develop several feasible outcomes in single evolution as it is based upon population behavior [75].

Figure 8 shows the working of EA in encryption process. EA originates by producing the random samples from

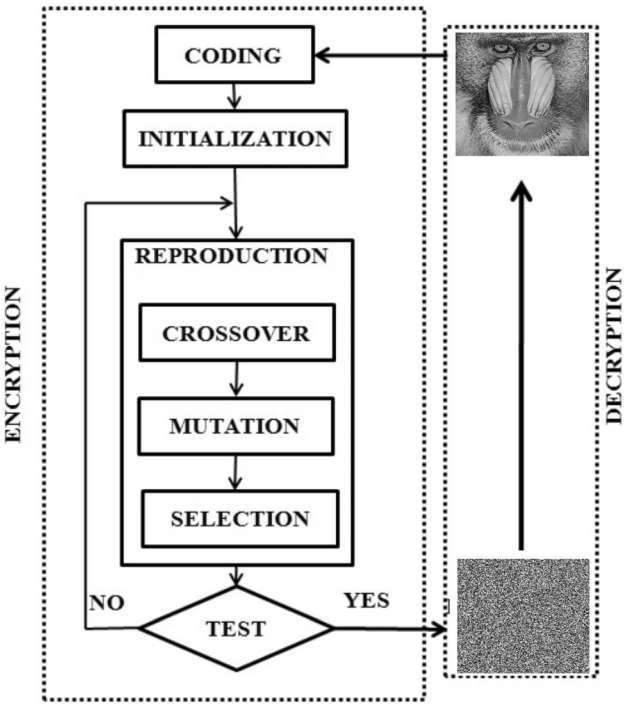

Fig. 8 Working of evolutionary optimization in encryption process [75]

given population, *i.e.,* problem domain. Based upon the appropriate objective function, EA find those samples which are best among the given samples. The main operators of EA are mutation, crossover, and recombination. These operators are used to evaluate best solution from obtained solutions. If the stopping criteria is satisfied, then EA returns best solution. Otherwise, the whole process is repeated to find appropriate solutions [76].

Abdullah et al. [77] used Genetic Algorithm (GA) for image encryption. This technique is used to select best encrypted image from the initial population. The chaotic technique is utilized to develop a given number of encrypted images. Thereafter, GA is used to select the best encrypted image which has high entropy and low correlation coefficient.

Sreelaja et al. [78] developed a technique to create secure keys by utilizing Ant Colony Optimization (ACO) algorithm. It reduces the burden of storage and distribution of keys. It enhances the security through encoding keys using a code table. In this technique, plain image is represented in the form of characters and key-stream is generated from the combinations of plaintext characters.

Enayatifar et al. [79] used weighted discrete Imperialist Competitive Algorithm (ICA) in image encryption. It provides best optimization results with maximum entropy and minimum correlation coefficients. The chaotic map is used to generate initial population for algorithm and then weighted discrete ICA is used to select the encrypted image with highest entropy and low correlation coefficient.

Enayatifar et al. [75] proposed an image cryptosystem based on hybrid GA and DNA sequence. A hybrid algorithm has an ability to improve the quality and choose best optimum mask. DNA sequence and chaotic map are used to generate DNA masks. Then, GA is used to select the optimum DNA mask. GA is used to maximize entropy during the encryption.

Abbas [16] described an image encryption algorithm based on Independent Component Analysis (ICoA) and Arnold Cat Map (ACM). ACM is used to create a random mixing matrix by injecting an arbitrary image. The source images are converted into vectors and combined with mixing matrix for mixing process that results in encryption of images. This technique can encrypt more than one image with the same process. Finally, ICoA is used to decrypted the images.

Talarposhti and Jamei [80] proposed an encryption algorithm for gray scale images based on Dynamic Harmony Search (DHS). This technique uses skew tent map to create encrypted images. DHS selects the best encrypted image based on maximum entropy and minimum correlation coefficient. The main drawback is its computational time.

Table 5 shows the performance comparison of evolutionary based image encryption techniques. The main drawback of these techniques is computational speed. However, these techniques provide better encryption as compared to the existing image encryption techniques.

3.1.5 Elliptic Curve and Fuzzy Based Image Encryption Techniques

Elliptic curves are based on the properties of algebraic curves. Koblitz and Miller developed a public key encryption technique by utilizing elliptic curve. The main features of elliptic curve encryption are small key size and better computational [3].

Figure 9 shows the role of elliptic curve in image in an encryption. A pseudo-random keystream developed using cyclic elliptic curve and chaotic technique. It contains two phases such as allocation for development of initial keystream using chaotic map and merging with pseudo-random bit sequence [12]. An image is initially decomposed into a binary data sequence. This data is masked with random keystream . The generation of keystream is done through hybridization of elliptic curve and chaotic system. The analogous encrypted image is attained.

El-Latif and Niu [12] proposed a technique to develop strong keystream based on hybridization of elliptic curve and chaotic maps. The input image is converted into data stream. Keys are applied to encryption function which are generated from the combination of elliptic curve and chaotic technique to mask the data. The encrypted data stream is converted into pixels of image to get ciphered image.

Behnia et al. [81] introduced an image encryption technique based on Jacobian elliptic maps. These maps are used to remove the drawbacks of chaotic cryptosystems such as small key space and weak security.

Nagaraj et al. [82] proposed a new image encryption technique which is the combination of elliptic curve cryptography and magic matrix operations. The input image is embedded on the points of the elliptic curve using transform algorithm. The image is divided into data matrices and each pixel of an image is represented by magic matrix. Thereafter, each pixel is encoded using elliptic cryptography function to generate an encrypted image.

Liu et al. [83] introduced a new color image encryption scheme based on chaotic maps and Choquet Fuzzy Integral (CFI) . This scheme uses a piecewise linear chaotic map to generate the secret keys and Lorenz map. It is used to initialize the inputs of CFI. CFI creates a random keystreams which are used to confuse and diffuse an image to obtain a decrypted image.

Table 5 Comparison of evolutionary based image encryption techniques

References	NPCR	UACI	KA	HA	CC	IE	NA	KCPA	Speed
[77]	✗	✗	✔	✔	✔	✔	✗	✗	Poor
[78]	✗	✗	✔	✔	✔	✗	✗	✔	Average
[79]	✔	✔	✔	✔	✔	✔	✗	✗	Good
[75]	✔	✔	✔	✔	✔	✔	✗	✔	Average
[16]	✗	✗	✗	✗	✗	✗	✗	✗	Average
[80]	✔	✔	✔	✔	✔	✔	✗	✗	Poor

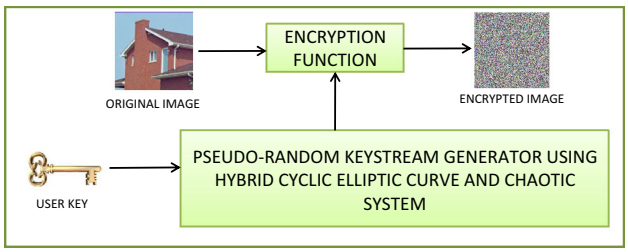

Fig. 9 Encryption process using elliptic curve and chaotic map [12]

Seyedzadeh et al. [84] used CFI to generate a keystream to encrypt the color images. This technique has three phases such as generation of keystream, circular shift, and diffusion process. CFI is used to generate the pseudo-random key-streams and bits of each color pixel are shifted circularly based on key-stream. The permuted bits are encrypted using the combination of key-stream and color pixels.

Table 6 shows the performance comparison of elliptic and fuzzy based image encryption techniques. Both elliptic and fuzzy techniques are mainly used in image encryption to generate efficient secret keys.

3.2 Transform Based Image Encryption Techniques

Transform based image encryption techniques have been extensively used in the field of image encryption. The given image is transformed from spatial to frequency domain by using suitable transform model. Figure 10 shows the working of transform domain based image encryption technique. It uses the double transform to encrypt the image [85]. For color images, the majority of schemes divide the input color image into three color channels (i.e., R, G, and B channels). Each color channel is converted into transform domain for encryption process.

The well-known techniques are fractional Mellin transform, Fractional Fourier Transform (FrFT), Gyrator Transform (GT), Discrete Cosine Transform (DCT), affine transform, etc. These techniques are discussed in the preceding sections.

3.2.1 Gyrator Transform Based Image Encryption Techniques

Singh and Sinha [86] implemented a novel cryptosystem using chaos in gyrator domain. In this technique, scrambled image is developed by utilizing gyrator domain and dual chaotic masks. The tent, Kaplan-Yorke and logistic map are used to encrypt the image. However, the computational speed is low.

Wang et al. [87] used linear exchanging operation and random phase encoding in GT domain for double image encryption. In the linear exchanging operation, two primitive images are linearly recombined *via* a random orthogonal transform matrix. The resultant blended images are employed to constitute a complex-valued image. Then, the image is encoded into a noise-like encrypted image by a Double Phase Random Encoding (DRPE). This scheme is highly sensitive towards the fractional orders of GT.

Wang et al. [88] used a Modified Gerchberg-Saxton Algorithm (MGSA) with Phase-Only Mask (POM) in GT domain for encryption. It reduces cross talk effect on multiplexing images.

Table 6 Performance comparison of elliptic and fuzzy based image encryption techniques

References	NPCR	UACI	KA	HA	CC	IE	NA	KCPA	Speed
[12]	✔	✔	✔	✔	✔	✔	✗	✗	Average
[81]	✔	✔	✔	✔	✔	✔	✗	✗	Average
[83]	✔	✔	✔	✔	✔	✔	✗	✗	Average
[84]	✔	✔	✔	✔	✔	✗	✗	✗	Poor
[82]	✗	✗	✗	✗	✗	✗	✗	✗	Average

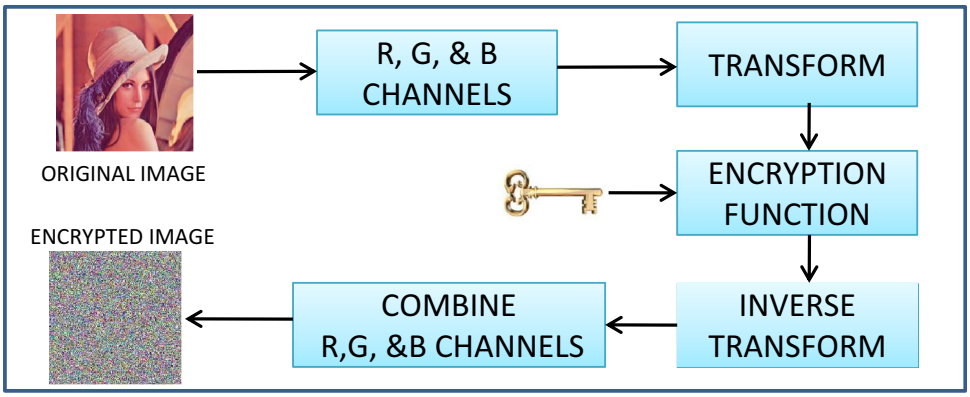

Fig. 10 Image encryption scheme using transformations [85]

Abuturab [89] proposed a new asymmetric image encryption technique for color images. A color image is divided into three channels and each channel is altered using Hartley transform. The altered channels are combined to get the first scrambled image. The first decryption key is generated by truncating the phase and amplitude of altered channels. GT is applied on already scrambled image to get the final encrypted image and second decryption key. The decryption process is reversible process to retrieve the original image.

Chen et al. [90] presented the solution for cross-talk disturbance found in phase-based images. This technique implements double image encryption using GT and local pixel scrambling scheme. Two images are encoded into a complex function and then this function is shuffled using local pixel scrambling. The shuffled image is rotated using GT to enhance the cryptosystem.

Yao et al. [91] encrypted the color images with the help of deduced GT. The primary feature of this algorithm is its decryption process. The encryption process involves gyrator and Fourier transform. But, decryption process involves only inverse of Fourier transform. This technique enhances the security of image encryption technique against the various attacks.

Table 7 shows the performance comparison of gyrator transform based image encryption techniques. From the table, it can be concluded that gyrator based image encryption techniques do not satisfy all the required performance measures. These techniques do not provide information regarding differential analysis.

3.2.2 Fractional Fourier Transform Based Image Encryption Techniques

Wang et al. [92] proposed a optimistic technique of optical image scrambling by utilizing binary Fourier transform. The keys are developed using order of scrambled pixels to encrypt and decrypt the image. This technique provides good security and robust against noise and distortion attacks. The main advantage of this technique easy to implement.

Guo et al. [93] designed an improved color image cryptosystem by utilizing Arnold transform and discrete fractional random transform. R,G, and B channels of an input color image is converted into intensity-hue-saturation (IHS) color space. The intensity channels are encrypted by using discrete fractional random transform and Arnold transform. This technique saves the storage space of cryptosystem keys. Due to transform domain, it losses the potential detail in the actual image which degrades its performance.

Li et al. [94] proposed an encryption technique to encrypt multiple images using cascaded FrFt. The original images are decomposed into two phase masks. One phase mask is used to generate keys and another phase mask is used to encrypt the images. The decryption process uses

Table 7 Comparison of gyrator transform based image encryption techniques

References	NPCR	UACI	KA	HA	CC	IE	NA	KCPA	Speed
[86]	✗	✗	✔	✗	✗	✗	✗	✗	Good
[87]	✗	✗	✔	✔	✗	✗	✔	✗	Good
[88]	✗	✗	✔	✗	✗	✗	✔	✗	Good
[89]	✗	✗	✔	✔	✔	✗	✔	✔	Average
[90]	✗	✗	✔	✗	✗	✗	✔	✗	Good
[14]	✗	✗	✔	✗	✔	✗	✗	✗	Good
[91]	✗	✗	✔	✔	✔	✗	✔	✔	Average

reverse FrFt to obtain the original image and decryption keys.

Li and Lee [95] tried to overcome the drawback of occlusion in double image encryption using modified Computational Integral Imaging Reconstruction (CIIR). FrFT technique is used to encrypt the elemental image array which is stored through pickup process. The reconstruction process uses modified CIIR to obtain actual images which enhances the resolution of recovered images. The disadvantage of this scheme is that it increases the transmission overhead in network.

Ran et al. [96] suggested a solution to solve the problem of information-independency in an image encryption by applying Non-Separable Fractional Fourier Transform (NFrFT). This technique has potential of tangling the information along and across the directions together which is not possible in FrFT and GT.

3.2.3 Fresnel, Wavelet and Cosine Transform Based Image Encryption Techniques

Zhao et al. [97] proposed a multiple-image encryption technique based on the position multiplexing of Fresnel phase. This scheme is less time-consuming because of its non-iterative nature. The encryption key can be further designed to realize a better reconstruction of plaintext.

Wang et al. [98] suggested the solution of silhouette problem which is presented in interface-based encoding schemes using Fresnel transform and random phase modulation. This scheme used single beam implementation. Therefore, there is no need of beam splitting during the decryption process. It is also time-saving scheme because of non-iterative nature.

Wang et al. [99] addressed the issue of cross-talk noise in multiple-image encryption schemes. This technique implemented the retrieval algorithm and phase mask multiplexing in Fresnel domain. In this, each image is encrypted individually into a phase-only function to remove the noise.

Wang et al. [100] tried to eliminate the threat of information disclosure in image cryptosystems based on phase-truncation scheme. For this, a random amplitude mask is used to remove the information disclosure risk. This technique can be extended to other domains such as gyrator, Fourier, and Fractional Fourier.

Luo et al. [101] suggested a encryption architecture using Integer Wavelet Transform (IWT). In this architecture, the decomposition process is done through IWT to divide input image into approximation and detail coefficients. The approximation coefficients are diffused using spatiotemporal chaos. Then, the diffused image is obtained by inverse IWT. The permutation process is performed to reduce the correlation among pixels using logistic map to get an encrypted image.

Mehra and Nishchal [14] used the combination of GT and WT to protect the phase images. The secret key is created by different random phase codes as well as parameters of GT and WT. Therefore, the developed secret key is stronger than the earlier techniques.

Kanso and Ghebleh [102] contributed in the field of visual image encryption by implementing embedded process in lift wavelet transform. It enhances the security of encryption techniques and quality of resultant images.

Lima et al. [103] suggested the use of Cosine Number Transform (CNT) for medical images encryption. The technique is used to avoid round-off errors and maintain high quality of images. It divides the image into blocks. Then, each block is sequentially applied to CNT. The encrypted image is obtained when whole image is processed.

Wu et al. [104] used Reality-Preserving Fractional Discrete Cosine Transform (RPFrDCT) to encrypt the color images. The encrypted image of this technique is a single color image. Therefore, it is convenient for storage and transmission.

Yaru and Jianhua [105] proposed an image encryption algorithm based on FrDCT *via* polynomial interpolation (PI-FrDCT), and Dependent Scrambling and Diffusion (DSD) process. Sinusoidal chaotic map is used to generate the pseudo-random sequence which is utilized by PI-FrDCT to encrypt the images. The coefficients of PI-FrDCT are also limited by sigmoid function. DSD is applied to generate an encrypted image.

Table 8 shows the comparison of Fourier, Fresnel, wavelet and cosine transforms based image encryption techniques. Transform based image encryption techniques have significant encryption speed. However, these techniques do not satisfy differential analysis efficiently.

3.3 Compressive Sensing Based Image Encryption Techniques

According to the Nyquist theorem, the signal is sampled at a least twice rate of its highest frequency to represent the signal without any error [107]. However, we often compress the data soon after sensing. It is wastage of valuable sensing resources. Over the past few years, a new theory of "Compressive Sensing" (CS) has emerged. In this technique, the signal is sampled and compressed simultaneously which reduce the rate at a great extent.

CS theory asserts that one can recover certain signals and images from fewer samples or measurements than the traditional techniques. CS relies on two principles namely, sparsity and incoherence. Sparsity pertains to the signals of

Table 8 Comparison between transform based image encryption techniques

References	NPCR	UACI	KA	HA	CC	IE	NA	KCPA	Speed
[92]	✗	✗	✗	✗	✗	✗	✗	✗	Good
[93]	✗	✗	✔	✗	✗	✗	✔	✔	Average
[97]	✗	✗	✔	✗	✔	✗	✔	✗	Good
[98]	✗	✗	✔	✗	✗	✗	✔	✗	Good
[99]	✗	✗	✔	✗	✔	✗	✔	✔	Good
[104]	✗	✗	✔	✔	✔	✗	✗	✗	Good
[94]	✗	✗	✔	✔	✔	✗	✔	✔	Good
[95]	✗	✗	✔	✗	✗	✗	✔	✗	Good
[96]	✗	✗	✔	✔	✗	✗	✔	✗	Average
[100]	✗	✗	✔	✗	✔	✗	✔	✔	Good
[101]	✔	✔	✔	✔	✔	✔	✗	✔	Good
[105]	✗	✗	✔	✔	✔	✗	✔	✗	Good
[106]	✗	✗	✔	✔	✔	✗	✔	✔	Good
[102]	✗	✗	✔	✔	✗	✗	✔	✔	Good
[103]	✔	✔	✔	✔	✔	✔	✗	✔	Good

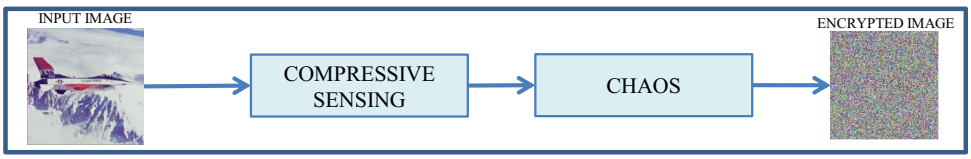

Fig. 11 Image encryption using compressive sensing

interest and incoherence pertains to the sensing modality [107].

In image encryption, CS has a significant contribution because encryption and compression can be applied at the same time to protect the sensitive images with storage reduction. Encryption is performed during sampling process. CS can be implemented with chaos and optical domain to improve the security [108]. Figure 11 shows the image encryption using compressive sensing and chaotic map.

Zhang et al. [109] demonstrated that CS has the ability to improve the speed of image cryptosystems. CS-based cryptosystems reduce the unwanted data in the plain image, then encryption process is used to encrypt the compressed image. Lu et al. [110] utilized an image encryption technique using CS and random phase based cryptography. A plain image is encrypted using CS technique and then random projection and dimensional reduction are used to encrypt the image. Zhou et al. [111] demonstrated a cryptography technique by utilizing encryption and CS concurrently. Partial Hadamard patterns are employed to encrypt the input image which are guarded by Chaos maps. This technique can handle several attacks. Zhou et al. [112] integrated CS with Nonlinear-Fractional Mellin Transform (NFMT). CS reduces the amount of data in the plain image. NFMT is utilized to encrypt the image. The frequency patterns are guided by chaos maps. This technique provides more secured image than the existing CS based encryption techniques.

Zhou et al. [113] utilized Discrete Fractional Random Technique (DFRT) and CS to encrypt a plain image. Two plain images are compressed and encrypted by utilizing CS and converted into the single image. The encrypted image is then re-encrypted by utilizing Arnold transform and DFRT. Zhou et al. [114] found that the several cryptography techniques based upon chaos maps suffer from several attacks. The encryption process is time-consuming in nature. To handle these issues, an improved cryptographic scheme is proposed by CS based hyper chaotic maps. It reduces the size of an image and provides better way for keys distribution.

Leihong et al. [115] shown that the most of image cryptographic systems suffer from low computational speed, especially when the size of input image is large. To overcome this issue, a cryptography technique by utilizing compressive ghost imaging with FFT is designed. This technique has high security, fast communication, and good quality of decrypted image. Rawat et al. [15] demonstrated an improved cryptography system based upon CS, Arnold transform, and structurally random patterns. It has good computational speed and improved the quality of decrypted image.

Cao et al. [17] implemented an image cryptosystem without embedding the secret image into a cover image.

Table 9 Performance comparison of compressive sensing based encryption techniques

References	NPCR	UACI	KA	HA	CC	IE	NA	KCPA	Speed
[109]	✗	✗	✔	✗	✗	✗	✔	✔	Good
[110]	✗	✗	✔	✗	✗	✗	✔	✗	Good
[111]	✗	✗	✔	✔	✔	✗	✔	✔	Average
[112]	✗	✗	✔	✔	✔	✗	✔	✔	Average
[113]	✗	✗	✔	✔	✔	✗	✔	✗	Good
[114]	✗	✗	✔	✔	✔	✗	✔	✔	Good
[115]	✗	✗	✔	✔	✔	✗	✔	✗	Good
[15]	✗	✗	✗	✗	✗	✗	✔	✗	Good
[18]	✗	✗	✔	✔	✔	✗	✔	✔	Good

This technique used the coupled dictionary learning and CS. It can encrypt multiple images within one cover image. Zhang et al. [18] used sparse model with CS to encrypt and compress the images. In this technique, pixel scrambling technique is used to re-encrypt the compressed and encrypted image to enhance the security of algorithm against brute force attack, statistical analysis, and chosen plaintext attack.

The comparison of above studied image encryption techniques based on compressive sensing is shown in Table 9. It is observed that compressive sensing based image encryption techniques have better computational speed. However, these techniques do not provide significant entropy of encrypted/decrypted images. Thus, these are not effective against differential attacks.

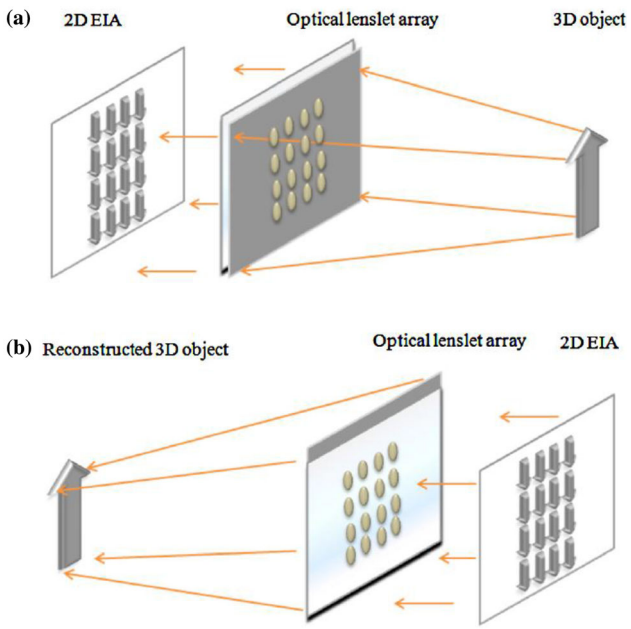

Fig. 12 The integral imaging system: **a** pickup process, **b** display process [118]

3.4 3D Image Encryption Techniques

Integral imaging is a well-known 3D image encryption technique. It receives more attention from researchers as it provides high robustness, security, and has good computational speed [106]. This technique produces an elemental image array (EIA) obtained from optical pinhole (or a lenslet) array [116]. Every elemental image has its own perspective decomposing whole information of a 3D image and can be reconstructed by using partial information even if some pixels of an encrypted image can be lost by possible number of attacks. Therefore, it is more efficient against various security attacks [95].

The conventional II system contain two optical processes i.e., pickup and display processes (see Fig. 12a, b). The lenslet array has been implemented in both processes to reconstruct 3D images [117]. From Fig. 12, it has been demonstrated that the rays information projecting from the 3D image is passing through the lenslet array and develop a set of elemental images (EIs) with different perspective information; and these EIs called as EIA are evaluated by a charge-coupled device (CCD) [118].

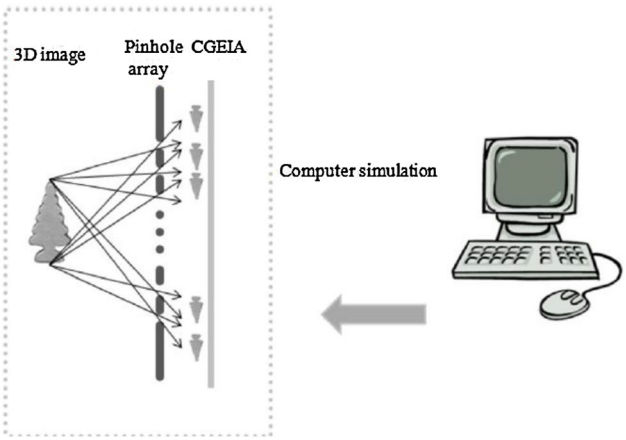

Fig. 13 The pickup process of computer-generated integral imaging system [118]

In the case of display, the evaluated EIA is shown on display panel and merged by the lens array into a 3D image at similar distance. But, according to the conventional optical II, the performance of reconstructed Image is degraded because of the diffraction and constraints of physical devices.

To handle these issues, the computational integral-imaging(CII) is designed. From Fig. 13, it has been demonstrated that the CII reconstructs by a computer using EIs that were selected using an optical lenslet array and CCD. The computational integral-imaging reconstruction (CIIR) is a volumetric technique that utilizes entire set of EIs's information to reconstruct a set of 3D plane images by considering the arbitrary distance. The quality of images obtained by CIIR has better performance as compared to optical II [119]. Because, CIIR is free of diffraction and device constraints. However, in optical pickup process of CII system suffers from the optical diffraction and constraints of physical devices [120].

3.5 Optical Image Encryption Techniques

Optical encryption techniques have been extensively utilized in the field of image cryptography because of their faster computational speed, parallel processing, and information storage in different dimensions [121]. The most important optical encryption technique is Double Random Phase Encoding (DRPE) [120]. It has opened new fields of research in optical image and signal processing. Figure 14 depicts the image encryption process of DRPE technique. It uses two random phase diffusers $D1$ and $D2$ both in space and frequency domains, respectively. An input image passes through $D1$ and then $2D$ optical Fourier transform (OFT). Again, image passes through $D2$ and then finally second $2D$ OFT. The encrypted image generated through DRPE technique looks like stationary white noise due to the statistical properties of diffusers. As $D1$ makes the input image white, while $D2$ makes the image stationary and encrypted.

A number of optical image encryption techniques has been proposed in the literature based on DRPE system.

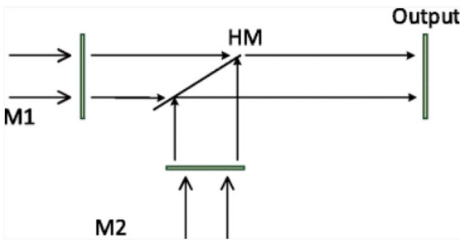

Fig. 14 Image encryption using DRPE technique [120]

Ding and Chen [122] presented the optical color image cryptosystem using position multiplexing technique and phase truncation operation. The color image is encrypted in the single spatial channel instead of three channels. It also maintains non-linear characteristics of encryption process. This cryptosystem resists iterative attack.

Qin and Gong [121] used lateral shift multiplexing to implement the multiple-image encryption. This scheme has addressed the silhouette problem of interference domain in very efficient way. Three POMs are used to encrypt the multiple images. The decryption process captures the plain images at output plane and secret key with the process of lateral shifting. Wang et al. [123] applied reverse engineering on modified amplitude-phase retrieval based algorithm for optical image encryption. This scheme shows the fake image instead of a noisy image after the encryption process that will help to protect the information

Chen et al. [124] used the concept of multi-beams interference with vector composition to encrypt the optical images. The ingenious technique is used to create n phase masks which are used as encryption keys. The ciphered image is obtained by multi-beams interference and vector composition. The original image is retrieved at receiver end by illuminating n-beams at POMs at the output plane after Fourier transform. Chen et al. [125] invented a technique to create color-ciphertext of a gray image by using Common Vector Composition (CVC) technique and three-beam interference technique. CVC technique breaks an original gray image into three parts of amplitude and phase information. These are used to generate colored ciphertext. The three-beam interference is used to retrieve the gray image from colored ciphertext.

Deng and Wen [126] applied fully phase encoding to implement the multiple- image encryption. This technique overcomes the problems of cross-talk noise, encryption capacity, and iterative computation. The simple interference technique is used to recover all deciphered images. Zhao et al. [127] added the feature of information authentication in image encryption using fingerprint as a secret key. The encryption algorithm is implemented using phase retrieval distribution and RSA algorithm. Wang et al. [128] tried to reduce the number of iterations in image encryption using improved amplitude-phase retrieval algorithm. It enhances the encryption capacity and the computation time.

Chen [129] used three-dimensional space for optical multiple-vision cryptography. Each input image is decomposed into a series of particle-like points distributed in 3-D space, and all generated particle-like points are encrypted in POM.

Table 10 shows the performance comparison between optical domain based image encryption techniques. From the table, it has been observed that these techniques do not

Table 10 Comparative analysis based upon optical techniques

References	NPCR	UACI	KA	HA	CC	IE	NA	KCPA	Speed
[122]	✗	✗	✗	✗	✗	✗	✔	✔	Average
[121]	✗	✗	✗	✗	✔	✗	✔	✗	Average
[123]	✗	✗	✗	✗	✗	✗	✗	✗	Average
[124]	✗	✗	✗	✗	✗	✗	✗	✗	Good
[125]	✗	✗	✔	✗	✗	✗	✔	✗	Good
[126]	✗	✗	✔	✗	✗	✗	✔	✗	Good
[127]	✗	✗	✗	✗	✗	✗	✗	✔	Poor
[128]	✗	✗	✔	✗	✔	✗	✔	✔	Good
[129]	✗	✗	✔	✗	✔	✗	✔	✗	Average

provide significant results against differential and statistical attacks.

Table 11 summarizes the pros and cons of well-known image encryption techniques.

4 Performance Comparison of Encryption Techniques Based on Image Quality Measures

The researchers have focused on the security analysis rather than the quality of encrypted and decrypted images. Image encryption techniques may introduce some amount of distortion or artifacts in the decrypted images, which negatively impacts the user's perception. The assurance of decrypted image quality is an important task for content providers and network operators. Therefore, the image quality metrics are performed to describe the quality of decrypted images. These measures evaluate the relationship between input and decrypted images.

The well-known image quality measures are BCR, PSNR, MSE, SDR, SSIM, RE, MAE, and SNR. Table 12 shows the performance comparison of image encryption techniques based on the above-mentioned quality metrics. Here, ✔ indicates that the given technique uses the corresponding metric to evaluate the performance of image encryption. In the same way, ✗ states that the given technique did not consider the respective metric for their performance evaluation.

5 Performance Analysis

This section describes the performance analysis of the image encryption techniques. To compare the existing image encryption techniques well-known "lena image" has been considered. In case of color images, we have taken the mean values of each parameter. Table 13 shows the performance analysis of some well-known image encryption techniques by considering the NPCR, UACI, Diagonal correlation (Diag. Corr.), Vertical correlation (Verti. Corr.), Horizontal correlation (Hori. Corr.), Entropy and Key size.Table 14 shows the execution time of various existing image encryption techniques.

6 Cryptanalysis on Image Encryption Techniques

In cryptanalysis, the cryptanalyst knows everything about cryptosystem except secret key. Cryptanalyst launch different types of attacks on cryptosystem to explore relation between plaintext and ciphertext to recover the secret key. The different types of attacks are ciphertext only, known plaintext, chosen plaintext, and chosen ciphertext. The various secure image encryption techniques have been broken by cryptanalysts. They suggest further improvements in encryption technique to enhance their security.

Wang and He [159] cryptanalysed Zhang and Liu [160] image encryption technique using chosen-plaintext attack. It was observed that the plain image can be retrieved without knowing the secret key. An image encryption technique that uses both skew tent and hyper chaotic maps proposed by Kadir et al. [33]. This technique cryptanalysed by [161]. The complete keystream can be retrieved through chosen-plaintext attack. Murillo et al. [162] implemented an image encryption technique that was dependent on the plain image. However, this technique was cracked by Fan et al. [163] using known/chosen plaintext attacks.

Zeng et al. [164] broke Li et al. [165] image encryption technique by launching chosen-plaintext and known-plaintext attacks. The security of broken technique can be improved through dynamic permutation process.

Su et al. [166] revealed that the image cryptosystem designed by [167] using chaos and DNA is susceptible to chosen-plaintext attack. Authors suggested that the technique can be improved by replacing the entropy present in chaos system with hash function.

Table 11 Pros and cons of existing image encryption techniques

Technique	Pros	Cons
Chaos based cryptography	(i) Deterministic, meaning that their behavior is predetermined	(i) One-dimensional chaotic maps are suffered from small key space and weak security
	(ii) Unpredictable and nonlinear	(ii) High-dimensional chaotic methods have longer processing time
	(iii) Random behavior	(iii) Poor computational speed
DNA based cryptography	(i) High computational speed	Not suitable for digital computing environment
	(ii) Minimum storage requirements	
	(iii) Energy efficient	
Cellular automata	(i) Easy to implement in both hardware and software	In reversible CA, keys must be kept secret, because the same key is used both for encryption and decryption
	(ii) High degree of security	
	(iii) Able to run in parallel manner independently	
Meta-heuristics	(i) Better quality of decrypted image	(i) Premature convergence
	(ii) Provide high degree of security	(ii) Poor convergence speed
Gyrator	(i) Passive, linear, and lossless technique	(i) Not suitable for non-stationary signals
	(ii) Non-reciprocal transform	
	(iii) Do not modify the range of data	
FFT	(i) Suitable for spectral analysis	(i) It provides only the frequency information of an image
	(ii) Able to capture non-repetitive events	(ii) Not preferable for linear and high order polynomial shapes
	(iii) Able to store the waveforms	
Wavelet transform	(i) Provides both frequency and location description of an image	(i) Computationally intensive
	(ii) Best suitable for non-stationary signal analysis	(ii) Less efficient and natural
	(iii) It has irregular shape	(iii) Wavelets take more energy to implement itself correctly
	(iv) Temporal information retained in transform process	
DCT	(i) Orthogonal transform based upon compression	(i) May introduce random noise due to quantization
	(ii) Better computation good speed	(ii) Truncation of higher spectral coefficients results in blurred images specially when the details are hidden
		(iii) Blocking artifacts
Elliptic curve based cryptography	(i) Equal level of security even with small key size	(i) High computation time
	(ii) Very fast key generation	(ii) Can not apply directly for encryption
	(iii) Require secure random generator	
Fuzzy based cryptography	(i) Suitable for uncertain and approximate reasoning	(i) Rules must be known in prior
	(ii) It is used to generate initial conditions for chaotic maps in image encryption	(ii) Require extensive computation
	(iii) It provides a significant sensitivity to initial conditions that resist differential attacks	(iii) Determine the exact fuzzy rules and membership is a difficult job
Compressive sensing	(i) Reduce the storage space and bandwidth of the secure transmission system	(i) Not effective when the size of image (s) is already small
	(ii) Low cost of CS sampling process makes the CS-based cryptosystem very suitable for low-complexity restricted system	(ii) Not effective for jpeg format images
	(iii) Great potential in the secure communication of digital data	
Optical domain	(i) Computationally faster	(i) Suffer from Silhouette problem
	(ii) Information can hide in various dimensions such as wavelength, polarization of light, phase, and spatial frequency	(ii) Do not retain both frequency and spatial information
	(iii) More applicable for real-time applications	

Table 12 Comparison of image encryption techniques based upon quality metrics

References	BCR	PSNR	MSE	SDR	SSIM	RE	MAE	SNR
[52]	✗	✔	✗	✗	✗	✗	✗	✗
[19]	✗	✔	✔	✗	✗	✗	✔	✔
[13]	✔	✔	✔	✗	✗	✗	✗	✗
[16]	✗	✔	✗	✔	✔	✗	✗	✗
[86]	✗	✗	✔	✗	✗	✗	✗	✗
[87]	✗	✗	✔	✗	✗	✗	✗	✗
[88]	✗	✔	✗	✗	✗	✗	✗	✗
[90]	✗	✗	✔	✗	✗	✗	✗	✗
[93]	✗	✗	✔	✗	✗	✗	✗	✗
[95]	✔	✔	✗	✗	✗	✗	✗	✗
[96]	✗	✗	✔	✗	✗	✗	✗	✗
[98]	✗	✗	✗	✗	✗	✔	✗	✗
[14]	✗	✗	✔	✗	✗	✗	✗	✗
[102]	✗	✔	✗	✗	✔	✗	✗	✗
[109]	✗	✔	✗	✗	✗	✗	✗	✗
[110]	✗	✔	✗	✗	✗	✗	✗	✗
[15]	✗	✔	✗	✗	✗	✗	✗	✗
[17]	✗	✔	✗	✗	✔	✗	✗	✗
[18]	✗	✔	✔	✗	✔	✗	✔	✗
[122]	✗	✗	✔	✗	✗	✗	✗	✗
[123]	✗	✗	✔	✗	✗	✗	✗	✗
[124]	✗	✗	✔	✗	✗	✗	✗	✗
[125]	✗	✔	✔	✗	✗	✗	✗	✗
[126]	✗	✗	✔	✗	✗	✗	✗	✗
[66]	✗	✗	✗	✗	✔	✗	✗	✗

Zhang et al. [168] used chosen-plaintext attack to break the encryption algorithm proposed by [169]. To improve the security, they proposed a modification in keystream of [169]. Norouzi and Mirzakuchaki [170] revealed that Zhao et al. [171] image encryption technique suffers from weak secret key. The keystream of [171] does not depend on the plain-image. Therefore, the secret key can be easily recovered using the chosen-plaintext attack. Table 15 shows the cryptanalysis of existing image encryption techniques.

It can be observed from the cryptanalysis that chaotic map based image encryption techniques can be broken easily. There is need to replace the chaotic map with another method which can provide more security. So, it is still an challenging issue to make chaotic map more secure.

7 Applications of Image Encryption

Image encryption techniques are widely used in various computer vision based applications. Table 16 shows various applications of image encryption techniques.

8 Future Research Directions

It has been observed from literature that the development of an efficient image encryption technique is still an open area research. The existing image encryption techniques suffer from various issues such as poor computational speed, security flaws, parameter tuning, etc. Based upon these issues, the following future directions have been discussed below.

8.1 Transmission Process

During the transmission process, if the image is tampered by third party, the integrity and authenticity verification are very necessary to ensure the confidentiality of the image content. Therefore, the design of combined approach for encryption and authentication is more desirable in near future.

8.2 Image Compression

The image encryption technique undermines the correlation between pixels and reduces the compression ratio.

Table 13 Comparative analysis of image encryption techniques

References	NPCR	UACI	Diag. Corr.	Verti. Corr.	Hori. Corr.	Entropy	Key size
[54]	–	–	− 0.0323	− 0.0653	− 0.0158	–	10^{45}
[29]	–	–	− 0.0183	− 0.0074	− 0.0142	–	10^{70}
[55]	99.606	33.456	0.0148	0.0021	0.0007	–	2^{128}
[42]	–	–	0.0010	0.0034	− 0.0893	7.9993	2^{296}
[56]	–	–	− 0.0052	− 0.0061	0.0087	–	–
[6]	99.622	33.704	− 0.0045	− 0.0112	− 0.0048	7.9963	2^{624}
[57]	–	–	0.0163	− 0.0043	0.0042	–	2^{276}
[130]	99.629	38.572	0.0006	0.0019	0.0021	7.9986	2^{348}
[131]	99.730	33.550	0.0012	0.0151	0.0044	7.9984	10^{90}
[132]	99.609	33.463	− 0.0193	− 0.0226	− 0.0245	7.9899	10^{606}
[133]	99.6090	33.429	0.0277	0.0039	0.0172	7.9917	10^{56}
[134]	99.419	33.641	8.3962e−04	− 1.8380e−04	0.0210	7.9973	10^{70}
[135]	99.620	33.450	0.0277	0.0039	0.0172	7.9993	2^{256}
[136]	99.683	33.530	0.0009	0.0025	0.0030	7.9973	2^{572}
[137]	99.589	33.526	0.0003	0.0002	0.0003	7.9971	2^{208}
[138]	99.690	33.510	0.0043	0.0021	0.0042	7.9995	2^{128}
[139]	93.790	16.780	0.0259	0.0232	0.0012	7.9959	10^{60}
[140]	98.798	33.648	0.0007	0.0011	0.0021	7.9972	2^{200}
[141]	99.683	33.530	0.0009	0.0025	0.0030	7.9973	2^{572}
[142]	99.610	33.550	− 0.0125	− 0.0102	− 0.0086	7.9991	2^{128}
[58]	99.609	33.466	0.0054	0.0006	− 0.0065	7.9902	2^{561}
[52]	99.655	33.484	0.0017	− 0.0038	− 0.0026	–	2^{138}
[53]	99.610	33.460	0.0008	− 0.0032	0.0015	7.9972	2^{273}
[61]	99.609	3.481	0.0015	0.0004	0.0084	7.9892	2^{299}
[46]	99.650	33.480	0.9419	0.9526	0.9718	7.9970	10^{54}
[62]	–	–	− 0.0140	− 0.0040	0.0035	–	$2^{144.0674}$
[60]	–	–	0.0017	0.0040	0.0046	7.9974	10^{182}
[63]	99.630	33.600	− 0.0025	− 0.0013	0.0090	7.9974	10^{66}
[65]	99.757	39.120	0.0008	0.0120	0.0011	7.9992	$10^{4}0$
[143]	99.660	33.720	0.0002	0.0005	0.0004	7.9980	2^{256}
[121]	99.611	33.450	0.0058	0.0098	0.0080	7.9871	2^{349}
[144]	99.570	33.420	0.0012	0.0009	0.0011	7.9993	10^{56}
[145]	99.609	33.470	0.0013	0.0140	0.0045	7.9992	2^{160}
[146]	99.600	33.450	0.0079	0.0072	0.0033	7.9975	2^{263}
[7]	99.590	33.410	0.0053	− 1.62e−04	− 0.0045	7.9993	2^{100}
[67]	99.000	33.330	0.0045	0.0192	0.0011	7.9992	2^{286}
[68]	99.122	37.638	0.0089	0.0095	− 0.0063	7.9696	10^{44}
[69]	99.658	33.484	0.0073	0.0025	0.0005	7.9970	2^{256}
[147]	0.9965	0.3355	0.0009	0.0021	0.0024	7.9407	2^{256}
[148]	99.607	33.500	0.0056	0.0054	0.0010	7.9992	2^{520}
[149]	99.650	33.64	− 0.0017	0.0001	0.0022	7.9972	2^{128}
[150]	–	–	− 0.0010	− 0.0089	− 0.0136	–	2^{128}
[151]	–	–	− 0.0007	− 0.0007	− 0.0009	7.9992	$2^{256\times256\times16}$
[152]	99.616	33.472	0.0099	0.0836	0.0314	–	$2^{256\times256\times32}$
[153]	99.612	33.446	− 0.0013	− 0.0023	− 0.0019	7.9972	$2^{4980.}$
[75]	99.710	33.629	0.0001	0.0007	0.0017	7.9997	2^{120}
[77]	–	–	− 0.0009	0.0093	− 0.0054	7.9978	2^{40}

Table 13 continued

References	NPCR	UACI	Diag. Corr.	Verti. Corr.	Hori. Corr.	Entropy	Key size
[79]	99.683	33.573	0.0001	− 0.0009	0.0008	7.9996	2^{240}
[80]	99.591	33.448	0.0001	0.0005	0.0003	7.9997	2^{416}
[122]	99.980	33.532	0.0009	0.0093	0.0054	7.9994	2^{186}
[154]	99.228	30.147	0.0020	0.0021	0.0019	7.9720	2^{40}
[155]	99.61	33.52	0.0088	0.0037	− 0.0081	7.9984	10^{130}
[156]	99.335	33.600	0.0126	0.2389	0.0909	7.8976	10^{37}
[157]	99.78	33.85	0.0056	0.0011	0.0007	7.3419	2^{184}
[129]	99.611	33.465	–	–	–	–	10^{42}
[124]	99.610	31.308	0.0067	0.0138	0.0065	7.9019	10^{39}
[125]	99.810	33.113	0.0026	0.0018	0.0012	7.9998	2^{446}
[158]	99.10	15.38	0.0140	0.0273	0.0007	–	2^{100}

Table 14 Computational speed analysis of image encryption techniques

Ref.	Image size	Color/gray	ET (in seconds)	Platform	GHz	RAM (GB)	Software
[54]	256 × 256	Gray	0.50	Pentium-IV	1.5	0.5	C
[42]	512 × 512	Gray	55.85	Pentium-IV	2.66	4	MATLAB
[56]	256 × 256	Gray	0.187	Intel Core i5	2.27	2	MATLAB
[6]	256 × 256	Gray and color	0.095	Intel Core i3	2.40	4	MATLAB
[142]	256 × 256	Color	0.079	Intel Core i3	2.50	2	MATLAB
[58]	256 × 256	Color	0.438	Intel Core i3	2.40	4	MATLAB
[61]	256 × 256	Color	3.348	Intel Core i5	2.49	8	MATLAB
[69]	256 × 256	Gray	1.184	Intel Pentium Dual Core	2.9	2	MATHEMATICA
[148]	256 × 256	Gray	1.09	Intel Core i7	3	8	C
[153]	256 × 256	Gray	1.02	Intel Core i7	3	1	MATLAB
[75]	256 × 256	Gray	3.284	Intel Core i7	2.3	8	MATLAB
[79]	256 × 256	Gray	9.45	Intel Core i7	2.3	8	MATLAB
[148]	256 × 256	Gray	1.206	Intel Core2 Duo	2.4	2	MATLAB
[130]	256 × 256	Color	1.13	Intel Core 2 Duo	2.26	4	MATLAB
[131]	256 × 256	Gray and color	0.46	Intel Core 2 Duo	3	4	MATLAB
[155]	256 × 256	Gray and color	1.02	Intel Core 2 Duo	2.5	4	MATLAB
[132]	256 × 256	Gray	0.776	Intel Core I7	4	8	C++
[133]	256 × 256	Gray	0.0343	Intel Core i3	2.30	4	MATLAB
[135]	512 × 512	Gray	13.02	Intel Core2 Duo	3	4	MATLAB
[136]	256 × 256	Color	18.6	Intel core i5	2.40	8	MATLAB
[137]	256 × 256	Gray and color	2.67	Intel Core2 Duo	2.0	2	MATLAB
[158]	256 × 256	Gray	0.950	Intel Core2 Duo	2.0	3	MATLAB

Image compression technique not only reduces the amount of data transmitted but also reduces the amount of data. There is a possibility to combine both encryption and compression technique for better efficiency.

8.3 Constant Attributes

In the existing image encryption techniques, constant attributes usually remain unchanged which limits the performance of encryption. There is a possibility to change the constant parameters based on the given input image. Therefore, an

Table 15 Cryptanalysis of image encryption techniques

Cryptanalysis method	Broken technique	Attacks
[159]	[160]	Chosen-plaintext
[161]	[33]	Chosen-plaintext
[163]	[162]	Known-plaintext and chosen-plaintext
[164]	[165]	Known-plaintext and chosen-plaintext
[166]	[167]	Chosen-plaintext
[168]	[169]	Chosen-plaintext
[170]	[171]	Chosen-plaintext

Table 16 Applications of image encryption techniques

Application	References
Medical vision	[103, 172–178]
Multimedia	[8, 134, 149–154, 179–181]
Remote sensing images	[182]
Cloud computing	[183–186]
Mobile networks	[157, 175, 187, 188]
Video conferencing	[189–193]
Multimedia sensor networks	[194–197]
Secure surveillance framework for IoT	[198, 199]
Optical character recognition	[200, 201]

efficient parameter tunning approach is desirable to improve the performance of encryption techniques.

8.4 Key Space

The size of key space in encryption process depends upon the key factor that directly affects the encrypted image. The image compression can be used to improve the weakness of key factor.

8.5 Meta-heuristic Technique

Recently, many researchers have used meta-heuristic techniques to further improve the performance of existing encryption techniques. However, these techniques also suffer from pre-mature convergence, poor convergence speed, stuck in local optima, etc. There is a possibility to select an efficient meta-heuristic technique to improve the performance of the existing image encryption techniques.

8.6 Parallel Processing

Now-a-days, size is becoming huge for medical and remotely sensed applications. Therefore, it becomes essential to use parallel processing in encryption to improve the computational speed.

9 Conclusion

This paper provides an extensive study of the existing image encryption techniques. This paper classifies the existing image encryption techniques in a concise and effective way. It has been observed that security flaws, parameters tuning, and computational speed are still an open area of research in the field of image encryption. To handle these issues, meta-heuristic based image encryption techniques have been designed by various researchers. The majority of existing meta-heuristic based image encryption techniques still suffer from poor convergence speed, pre-mature convergence, and stuck in local optima. The challenges and future research directions associated with image encryption techniques have been discussed. From the comprehensive review of existing image encryption techniques, it has been concluded that an image encryption is still an underdeveloped field. It is largely unexplored in various imaging systems such as underwater, remote sensing, multi-spectral imaging, and 3D imaging systems.

Compliance with Ethical Standards

Conflict of interest The authors declare that there is no conflict of interest.

References

1. Ghebleh M, Kanso A, Noura H (2014) An image encryption scheme based on irregularly decimated chaotic maps. Signal Process Image Commun 29(5):618–627
2. Sivakumar T, Venkatesan R (2015) A novel image encryption using calligraphy based scan method and random number. KSII Trans Internet Inf Syst 9(6):2317–2337
3. Forouzan BA, Mukhopadhyay D (2011) Cryptography and network security (Sie). McGraw-Hill Education, New York
4. Bi N, Sun Q, Huang D, Yang Z, Huang J (2007) Robust image watermarking based on multiband wavelets and empirical mode decomposition. IEEE Trans Image Process 16(8):1956–1966
5. Li XW, Kim ST (2013) Optical 3D watermark based digital image watermarking for telemedicine. Opt Lasers Eng 51(12):1310–1320

6. Belazi A, El-Latif AAA, Belghith S (2016) A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process 128:155–170
7. Chai X, Chen Y, Broyde L (2017) A novel chaos-based image encryption algorithm using DNA sequence operations. Opt Lasers Eng 88:197–213
8. Zhao G, Chen G, Fang J, Xu G (2011) Block cipher design: generalized single-use-algorithm based on chaos. Tsinghua Sci Technol 16(2):194–206
9. El-Samie FEA, Ahmed HEH, Elashry IF, Shahieen MH, Faragallah OS, El-Rabaie E-SM, Alshebeili SA (2013) Image encryption: a communication perspective. CRC Press, Boca Raton
10. Chai X, Gan Z, Yang K, Chen Y, Liu X (2017) An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. Signal Process Image Commun 52:6–19
11. Zhang W, Wong K-W, Yu H, Zhu Z-L (2013) An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. Commun Nonlinear Sci Numer Simul 18(8):2066–2080
12. El-Latif AAA, Niu X (2013) A hybrid chaotic system and cyclic elliptic curve for image encryption. AEU Int J Electron Commun 67(2):136–143
13. Li XW, Cho SJ, Kim ST (2014) A 3D image encryption technique using computer-generated integral imaging and cellular automata transform. Opt Int J Light Electron Opt 125(13):2983–2990
14. Mehra I, Nishchal NK (2015) Optical asymmetric image encryption using gyrator wavelet transform. Opt Commun 354:344–352
15. Rawat N, Kim B, Kumar R (2016) Fast digital image encryption based on compressive sensing using structurally random matrices and arnold transform technique. Optik Int J Light Electron Opt 127(4):2282–2286
16. Abbas NA (2016) Image encryption based on independent component analysis and Arnolds cat map. Egypt Inform J 17(1):139–146
17. Cao X, Wei X, Guo R, Wang C (2017) No embedding: a novel image cryptosystem for meaningful encryption. J Vis Commun Image Represent 44:236–249
18. Zhang Y, Xu B, Zhou N (2017) A novel image compression–encryption hybrid algorithm based on the analysis sparse representation. Opt Commun 392:223–233
19. Khan M, Shah T (2014) A novel statistical analysis of chaotic S-box in image encryption. 3D Res 5(3):1–8
20. Gu G, Ling J (2014) A fast image encryption method by using chaotic 3D cat maps. Optik Int J Light Electron Opt 125(17):4700–4705
21. Huang X, Ye G (2014) An efficient self-adaptive model for chaotic image encryption algorithm. Commun Nonlinear Sci Numer Simul 19(12):4094–4104
22. Ono A, Kohda T (2007) Solvable three-dimensional rational chaotic map defined by Jacobian elliptic functions. Int J Bifurc Chaos 17(10):3645–3650
23. Chen G, Zhang D, Chen Q, Zhou D (2012) The characteristic of different chaotic sequences for compressive sensing. In: 2012 5th international congress on image and signal processing (CISP). IEEE, pp 1475–1479
24. Umamageswari A, Suresh G (2013) Security in medical image communication with Arnold's cat map method and reversible watermarking. In: 2013 international conference on circuits, power and computing technologies (ICCPCT). IEEE, pp 1116–1121
25. Salleh M, Ibrahim S, Isnin IF (2003) Enhanced chaotic imageencryption algorithm based on Baker's map. In: Proceedings of the 2003 international symposium on circuits and systems, 2003. ISCAS'03, vol 2. IEEE, pp II–II
26. Hu H, Liu L, Ding N (2013) Pseudorandom sequence generator based on the chen chaotic system. Comput Phys Commun 184(3):765–768
27. Chattopadhyay D, Mandal M, Nandi D (2011) Symmetric key chaotic image encryption using circle map. Indian J Sci Technol 4(5):593–599
28. Shastry MC, Nagaraj N, Vaidya PG (2006) The b-exponential map: a generalization of the logistic map, and its applications ingenerating pseudo-random numbers. ArXiv preprint arXiv:cs/0607069
29. Gao T, Chen Z (2008) A new image encryption algorithm based on hyper-chaos. Phys Lett A 372(4):394–400
30. Wei-Bin C, Xin Z (2009) Image encryption algorithm based on Henon chaotic system. In: International conference on image analysis and signal processing, 2009. IASP 2009. IEEE, pp 94–97
31. Pareek NK, Patidar V, Sud KK (2006) Image encryption using chaotic logistic map. Image Vis Comput 24(9):926–934
32. Zhen W, Xia H, Yu-Xia L, Xiao-Na S (2013) A new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system. Chin Phys B 22(1):010504
33. Kadir A, Hamdulla A, Guo W-Q (2014) Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. Optik Int J Light Electron Opt 125(5):1671–1675
34. Enayatifar R, Sadaei HJ, Abdullah AH, Lee M, Isnin IF (2015) A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. Opt Lasers Eng 71:33–41
35. Hamza R, Titouna F (2016) A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. Inf Secur J Glob Perspect 25(4–6):162–179
36. Behnia S, Akhshani A, Mahmodi H, Akhavan A (2008) A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Solitons Fractals 35(2):408–419
37. Ye G (2010) Image scrambling encryption algorithm of pixel bit based on chaos map. Pattern Recognit Lett 31(5):347–354
38. Li C, Lin D, Lü J (2017) Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. IEEE MultiMed 24(3):64–71
39. Zhu Z-L, Zhang W, Wong K-W, Yu H (2011) A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci 181(6):1171–1186
40. Zhang Y-Q, Wang X-Y (2014) Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation. Nonlinear Dyn 77(3):687–698
41. Li C (2016) Cracking a hierarchical chaotic image encryption algorithm based on permutation. Signal Process 118:203–210
42. Mirzaei O, Yaghoobi M, Irani H (2012) A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dyn 67(1):557–566
43. Kanso A, Ghebleh M (2012) A novel image encryption algorithm based on a 3D chaotic map. Commun Nonlinear Sci Numer Simul 17(7):2943–2959
44. Wang X-Y, Wang T, Xu D-H, Chen F (2014) A selective image encryption based on couple spatial chaotic systems. Int J Mod Phys B 28(06):1450023
45. Zhang Y-Q, Wang X-Y (2014) A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice. Inf Sci 273:329–351
46. Wang X-Y, Gu S-X, Zhang Y-Q (2015) Novel image encryption algorithm based on cycle shift and chaotic system. Opt Lasers Eng 68:126–134
47. Liu W, Sun K, Zhu C (2016) A fast image encryption algorithm based on chaotic map. Opt Lasers Eng 84:26–36

48. Wang X, Wang Q, Zhang Y (2015) A fast image algorithm based on rows and columns switch. Nonlinear Dyn 79(2):1141–1149
49. Farajallah M, El Assad S, Deforges O (2016) Fast and secure chaos-based cryptosystem for images. Int J Bifurc Chaos 26(02):1650021
50. Chen E, Min L, Chen G (2017) Discrete chaotic systems with one-line equilibria and their application to image encryption. Int J Bifurc Chaos 27(03):1750046
51. Hua Z, Zhou Y (2017) Design of image cipher using block-based scrambling and image filtering. Inf Sci 396:97–113
52. Pak C, Huang L (2017) A new color image encryption using combination of the 1D chaotic map. Signal Process 138:129–137
53. Li Y, Wang C, Chen H (2017) A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Opt Lasers Eng 90:238–246
54. Gao H, Zhang Y, Liang S, Li D (2006) A new chaotic algorithm for image encryption. Chaos Solitons Fractals 29(2):393–399
55. Wang Y, Wong K-W, Liao X, Chen G (2011) A new chaos-based fast image encryption algorithm. Appl Soft Comput 11(1):514–522
56. Chen J-X, Zhu Z-L, Fu C, Yu H (2015) Optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains. Opt Commun 341:263–270
57. Zhou N, Pan S, Cheng S, Zhou Z (2016) Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing. Opt Laser Technol 82:121–133
58. Wu X, Wang D, Kurths J, Kan H (2016) A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. Inf Sci 349:137–153
59. Zhang Q, Liu L, Wei X (2014) Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. AEU Int J Electron Commun 68(3):186–192
60. Li X, Wang L, Yan Y, Liu P (2016) An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems. Optik Int J Light Electron Opt 127(5):2558–2565
61. Wu X, Kan H, Kurths J (2015) A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. Appl Soft Comput 37:24–39
62. Kumar M, Iqbal A, Kumar P (2016) A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. Signal Process 125:187–202
63. Yuan Wang X, Li Zhang H, Mei Bao X (2016) Color image encryption scheme using CML and DNA sequence operations. Biosystems 144:18–26
64. Mondal B, Mandal T (2017) A light weight secure image encryption scheme based on chaos DNA computing. J King Saud Univ Comput Inf Sci 29(4):499–504
65. Wang X, Luan D (2013) A novel image encryption algorithm using chaos and reversible cellular automata. Commun Nonlinear Sci Numer Simul 18(11):3075–3085
66. Li X, Xiao D, Wang Q-H (2018) Error-free holographic frames encryption with CA pixel-permutation encoding algorithm. Opt Lasers Eng 100:200–207
67. Wang X, Luan D (2013) A novel image encryption algorithm using chaos and reversible cellular automata. Commun Nonlinear Sci Numer Simul 18(11):3075–3085
68. Bakhshandeh A, Eslami Z (2013) An authenticated image encryption scheme based on chaotic maps and memory cellular automata. Opt Lasers Eng 51(6):665–673
69. Ping P, Xu F, Wang Z-J (2014) Image encryption based on non-affine and balanced cellular automata. Signal Process 105:419–429
70. Mohamed FK (2014) A parallel block-based encryption schema for digital images using reversible cellular automata. Eng Sci Technol Int J 17(2):85–94
71. Enayatifar R, Sadaei HJ, Abdullah AH, Lee M, Isnin IF (2015) A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. Opt Lasers Eng 71:33–41
72. Yang Y-G, Tian J, Lei H, Zhou Y-H, Shi W-M (2016) Novel quantum image encryption using one-dimensional quantum cellular automata. Inf Sci 345:257–270
73. Li X, Li C, Lee I-K (2016) Chaotic image encryption using pseudo-random masks and pixel mapping. Signal Process 125:48–63
74. Niyat AY, Moattar MH, Torshiz MN (2017) Color image encryption based on hybrid hyper-chaotic system and cellular automata. Opt Lasers Eng 90:225–237
75. Enayatifar R, Abdullah AH, Isnin IF (2014) Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt Lasers Eng 56:83–93
76. Souici I, Seridi H, Akdag H (2011) Images encryption by the use of evolutionary algorithms. Analog Integr Circuits Signal Process 69(1):49–58
77. Abdullah AH, Enayatifar R, Lee M (2012) A hybrid genetic algorithm and chaotic function model for image encryption. AEU Int J Electron Commun 66(10):806–816
78. Sreelaja N, Pai GV (2012) Stream cipher for binary image encryption using ant colony optimization based key generation. Appl Soft Comput 12(9):2879–2895
79. Enayatifar R, Abdullah AH, Lee M (2013) A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption. Opt Lasers Eng 51(9):1066–1077
80. Talarposhti KM, Jamei MK (2016) A secure image encryption method based on dynamic harmony search (DHS) combined with chaotic map. Opt Lasers Eng 81:21–34
81. Behnia S, Akhavan A, Akhshani A, Samsudin A (2013) Image encryption based on the Jacobian elliptic maps. J Syst Softw 86(9):2429–2438
82. Nagaraj S, Raju G, Rao KK (2015) Image encryption using elliptic curve cryptograhy and matrix. Procedia Comput Sci 48:276–281
83. Liu H, Wang X, Kadir A (2013) Color image encryption using Choquet fuzzy integral and hyper chaotic system. Opt Int J Light Electron Opt 124(18):3527–3533
84. Seyedzadeh SM, Norouzi B, Mirzakuchaki S (2014) RGB color image encryption based on Choquet fuzzy integral. J Syst Softw 97:128–139
85. Chen H, Du X, Liu Z, Yang C (2013) Color image encryption based on the affine transform and gyrator transform. Opt Lasers Eng 51(6):768–775
86. Singh N, Sinha A (2009) Gyrator transform-based optical image encryption, using chaos. Opt Lasers Eng 47(5):539–546
87. Wang Q, Guo Q, Lei L, Zhou J (2013) Linear exchanging operation and random phase encoding in gyrator transform domain for double image encryption. Opt Int J Light Electron Opt 124(24):6707–6712
88. Wang Q, Guo Q, Lei L (2014) Multiple-image encryption system using cascaded phase mask encoding and a modified Gerchberg–Saxton algorithm in gyrator domain. Opt Commun 320:12–21
89. Abuturab MR (2015) An asymmetric single-channel color image encryption based on hartley transform and gyrator transform. Opt Lasers Eng 69:49–57
90. Chen J-X, Zhu Z-L, Fu C, Zhang L-B, Yu H (2015) Analysis and improvement of a double-image encryption scheme using

pixel scrambling technique in gyrator domains. Opt Lasers Eng 66:1–9
91. Yao L, Yuan C, Qiang J, Feng S, Nie S (2017) An asymmetric color image encryption method by using deduced gyrator transform. Opt Lasers Eng 89:72–79
92. Wang Y-Y, Wang Y-R, Wang Y, Li H-J, Sun W-J (2007) Optical image encryption based on binary Fourier transform computer-generated hologram and pixel scrambling technology. Opt Lasers Eng 45(7):761–765
93. Guo Q, Liu Z, Liu S (2010) Color image encryption by using arnold and discrete fractional random transforms in ihs space. Opt Lasers Eng 48(12):1174–1181
94. Li Y, Zhang F, Li Y, Tao R (2015) Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform. Opt Lasers Eng 72:18–25
95. Li X-W, Lee I-K (2015) Modified computational integral imaging-based double image encryption using fractional Fourier transform. Opt Lasers Eng 66:112–121
96. Ran Q, Yuan L, Zhao T (2015) Image encryption based on nonseparable fractional Fourier transform and chaotic map. Opt Commun 348:43–49
97. Zhao H, Liu J, Jia J, Zhu N, Xie J, Wang Y (2013) Multiple-image encryption based on position multiplexing of Fresnel phase. Opt Commun 286:85–90
98. Wang Q, Guo Q, Lei L, Zhou J (2014) Single-beam image encryption using spatially separated ciphertexts based on interference principle in the Fresnel domain. Opt Commun 333:151–158
99. Wang Y, Quan C, Tay C (2014) Nonlinear multiple-image encryption based on mixture retrieval algorithm in Fresnel domain. Opt Commun 330:91–98
100. Wang Y, Quan C, Tay C (2015) Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask. Opt Commun 344:147–155
101. Luo Y, Du M, Liu J (2015) A symmetrical image encryption scheme in wavelet and time domain. Commun Nonlinear Sci Numer Simul 20(2):447–460
102. Kanso A, Ghebleh M (2017) An algorithm for encryption of secret images into meaningful images. Opt Lasers Eng 90:196–208
103. Lima JB, Madeiro F, Sales F (2015) Encryption of medical images based on the cosine number transform. Signal Process Image Commun 35:1–8
104. Wu J, Guo F, Liang Y, Zhou N (2014) Triple color images encryption algorithm based on scrambling and the reality-preserving fractional discrete cosine transform. Opt Int J Light Electron Opt 125(16):4474–4479
105. Yaru L, Jianhua W (2015) New image encryption combining fractional DCT via polynomial interpolation with dependent scrambling and diffusion. J China Univ Posts Telecommun 22(5):1–9
106. Li X-W, Wang Q-H, Kim S-T, Lee I-K (2016) Encrypting 2D/3D image using improved lensless integral imaging in Fresnel domain. Opt Commun 381:260–270
107. Candes EJ, Wakin MB (2008) An introduction to compressive sampling. IEEE Signal Process Mag 25(2):21–30
108. Zhang Y, Zhang LY, Zhou J, Liu L, Chen F, He X (2016) A review of compressive sensing in information security field. IEEE Access 4:2507–2519
109. Zhang Y, Zhou J, Chen F, Zhang LY, Wong K-W, He X, Xiao D (2016) Embedding cryptographic features in compressive sensing. Neurocomputing 205:472–480
110. Lu P, Xu Z, Lu X, Liu X (2013) Digital image information encryption based on compressive sensing and double random-phase encoding technique. Opt Int J Light Electron Opt 124(16):2514–2518
111. Zhou N, Zhang A, Wu J, Pei D, Yang Y (2014) Novel hybrid image compression–encryption algorithm based on compressive sensing. Opt Int J Light Electron Opt 125(18):5075–5080
112. Zhou N, Li H, Wang D, Pan S, Zhou Z (2015) Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform. Opt Commun 343:10–21
113. Zhou N, Yang J, Tan C, Pan S, Zhou Z (2015) Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform. Opt Commun 354:112–121
114. Zhou N, Pan S, Cheng S, Zhou Z (2016) Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing. Opt Laser Technol 82:121–133
115. Leihong Z, Zilan P, Luying W, Xiuhua M (2016) High-performance compression and double cryptography based on compressive ghost imaging with the fast Fourier transform. Opt Lasers Eng 86:329–337
116. Li XW, Cho SJ, Kim ST (2014) High security and robust optical image encryption approach based on computer-generated integral imaging pickup and iterative back-projection techniques. Opt Lasers Eng 55:162–182
117. Li S-L, Wang Q-H, Xiong Z-L, Deng H, Ji C-C (2014) Multiple orthographic frustum combing for real-time computer-generated integral imaging system. J Display Technol 10(8):704–709
118. Li XW, Cho SJ, Kim ST (2014) A 3D image encryption technique using computer-generated integral imaging and cellular automata transform. Opt Int J Light Electron Opt 125(13):2983–2990
119. Xing Y, Wang Q-H, Xiong Z-L, Deng H (2016) Encrypting three-dimensional information system based on integral imaging and multiple chaotic maps. Opt Eng 55(2):023107
120. Wang Q, Wei M, Chen X, Miao Z (2018) Joint encryption and compression of 3D images based on tensor compressive sensing with non-autonomous 3D chaotic system. Multimed Tools Appl 77(2):1715–1734
121. Qin Y, Gong Q (2014) Multiple-image encryption in an interference-based scheme by lateral shift multiplexing. Opt Commun 315:220–225
122. Ding X, Chen G (2014) Optical color image encryption using position multiplexing technique based on phase truncation operation. Opt Laser Technol 57:110–118
123. Wang X, Dai C, Chen J (2014) Optical image encryption via reverse engineering of a modified amplitude-phase retrieval-based attack. Opt Commun 328:67–72
124. Chen L, Liu J, Wen J, Gao X, Mao H, Shi X, Qu Q (2015) A new optical image encryption method based on multi-beams interference and vector composition. Opt Laser Technol 69:80–86
125. Chen L, Liu J, Wen J, Mao H, Ge F, Zhao D (2015) Pseudo color image encryption based on three-beams interference principle and common vector composition. Opt Commun 338:110–116
126. Deng X, Wen W (2015) Optical multiple-image encryption based on fully phase encoding and interference. Opt Int J Light Electron Opt 126(21):3210–3214
127. Zhao T, Ran Q, Yuan L, Chi Y, Ma J (2015) Image encryption using fingerprint as key based on phase retrieval algorithm and public key cryptography. Opt Lasers Eng 72:12–17
128. Wang Y, Quan C, Tay C (2016) Asymmetric optical image encryption based on an improved amplitude-phase retrieval algorithm. Opt Lasers Eng 78:8–16
129. Chen W (2016) Optical multiple-image encryption using three-dimensional space. IEEE Photonics J 8(2):1–8

130. Li C, Luo G, Li C (2018) A parallel image encryption algorithm based on chaotic Duffing oscillators. Multimed Tools Appl 77(15):19193–19208
131. Chai X, Gan Z, Zhang M (2017) A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion. Multimed Tools Appl 76(14):15561–15585
132. Zhang Y, Tang Y (2017) A plaintext-related image encryption algorithm based on chaos. Multimed Tools Appl 77:1–23
133. Huang X, Ye G (2018) An image encryption algorithm based on irregular wave representation. Multimed Tools Appl 77(2):2611–2628
134. Chai X, Yang K, Gan Z (2017) A new chaos-based image encryption algorithm with dynamic key selection mechanisms. Multimed Tools Appl 76(7):9907–9927
135. Chai X (2017) An image encryption algorithm based on bit level brownian motion and new chaotic systems. Multimed Tools Appl 76(1):1159–1175
136. Mollaeefar M, Sharif A, Nazari M (2017) A novel encryption scheme for colored image based on high level chaotic maps. Multimed Tools Appl 76(1):607–629
137. Tang Z, Wang F, Zhang X (2017) Image encryption based on random projection partition and chaotic system. Multimed Tools Appl 76(6):8257–8283
138. Liu L, Miao S (2017) An image encryption algorithm based on baker map with varying parameter. Multimed Tools Appl 76(15):16511–16527
139. Zhu J, Yang X, Meng X, Wang Y, Yin Y, Sun X, Dong G (2018) Optical image encryption scheme with multiple light paths based on compressive ghost imaging. J Mod Opt 65(3):306–313
140. Wu J, Zhang M, Zhou N (2017) Image encryption scheme based on random fractional discrete cosine transform and dependent scrambling and diffusion. J Mod Opt 64(4):334–346
141. Li H, Wang Y (2008) Double-image encryption by iterative phase retrieval algorithm in fractional Fourier domain. J Mod Opt 55(21):3601–3609
142. Wang X, Teng L, Qin X (2012) A novel colour image encryption algorithm based on chaos. Signal Process 92(4):1101–1108
143. Norouzi B, Mirzakuchaki S (2017) An image encryption algorithm based on DNA sequence operations and cellular neural network. Multimed Tools Appl 76(11):13681–13701
144. Liang Y, Liu G, Zhou N, Wu J (2015) Image encryption combining multiple generating sequences controlled fractional DCT with dependent scrambling and diffusion. J Mod Opt 62(4):251–264
145. Zhang Y (2018) The image encryption algorithm based on chaos and DNA computing. Multimed Tools Appl 77:1–27
146. Liu X, Mei W, Du H (2014) Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain. J Mod Opt 61(19):1570–1577
147. Chen T, Zhang M, Wu J, Yuen C, Tong Y (2016) Image encryption and compression based on kronecker compressed sensing and elementary cellular automata scrambling. Opt Laser Technol 84:118–133
148. Souyah A, Faraoun KM (2016) An image encryption scheme combining chaos-memory cellular automata and weighted histogram. Nonlinear Dyn 86(1):639–653
149. Niyat AY, Moattar MH, Torshiz MN (2017) Color image encryption based on hybrid hyper-chaotic system and cellular automata. Opt Lasers Eng 90:225–237
150. Wang Y, Zhao Y, Zhou Q, Lin Z (2018) Image encryption using partitioned cellular automata. Neurocomputing 275:1318–1332
151. Hanis S, Amutha R (2017) Double image compression and encryption scheme using logistic mapped convolution and cellular automata. Multimed Tools Appl 77:1–16
152. Jeyaram B, Raghavan R et al (2016) New cellular automata-based image cryptosystem and a novel non-parametric pixel randomness test. Secur Commun Netw 9(16):3365–3377
153. Murugan B, Gounder N, Gounden A, Manohar S (2016) A hybrid image encryption algorithm using chaos and Conway's game-of-life cellular automata. Secur Commun Netw 9(7):634–651
154. Ahmad M, Alam MZ, Umayya Z, Khan S, Ahmad F (2018) An image encryption approach using particle swarm optimization and chaotic map. Int J Inf Technol 10:1–9
155. Gan Z, Chai X, Yuan K, Lu Y (2017) A novel image encryption algorithm based on LFT based s-boxes and chaos. Multimed Tools Appl 77:1–25
156. Deng J, Zhao S, Wang Y, Wang L, Wang H, Sha H (2017) Image compression-encryption scheme combining 2D compressive sensing with discrete fractional random transform. Multimed Tools Appl 76(7):10097–10117
157. Krishnamoorthi R, Murali P (2017) A selective image encryption based on square-wave shuffling with orthogonal polynomials transformation suitable for mobile devices. Multimed Tools Appl 76(1):1217–1246
158. Ahmad J, Khan MA, Hwang S, Khan JS (2017) A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices. Neural Comput Appl 28(1):953–967
159. Wang X, He G (2011) Cryptanalysis on a novel image encryption method based on total shuffling scheme. Opt Commun 284(24):5804–5807
160. Zhang G, Liu Q (2011) A novel image encryption method based on total shuffling scheme. Opt Commun 284(12):2775–2780
161. Wen W (2016) Security analysis of a color image encryption scheme based on skew tent map and hyper chaotic system of 6th-order CNN against chosen-plaintext attack. Multimed Tools Appl 75(6):3553–3560
162. Murillo-Escobar M, Cruz-Hernandez C, Abundiz-Perez F, Lopez-Gutierrez R, Del Campo OA (2015) A RGB image encryption algorithm based on total plain image characteristics and chaos. Signal Process 109:119–131
163. Fan H, Li M, Liu D, An K (2017) Cryptanalysis of a plaintext-related chaotic RGB image encryption scheme using total plain image characteristics. Multimed Tools Appl 77:1–25
164. Zeng L, Liu R, Zhang LY, Liu Y, Wong K-W (2016) Cryptanalyzing an image encryption algorithm based on scrambling and veginere cipher. Multimed Tools Appl 75(10):5439–5453
165. Li S, Zhao Y, Qu B et al (2013) Image scrambling based on chaotic sequences and veginère cipher. Multimed Tools Appl 66(3):573–588
166. Su X, Li W, Hu H (2017) Cryptanalysis of a chaos-based image encryption scheme combining DNA coding and entropy. Multimed Tools Appl 76(12):14021–14033
167. Zhen P, Zhao G, Min L, Jin X (2016) Chaos-based image encryption scheme combining DNA coding and entropy. Multimed Tools Appl 75(11):6303–6319
168. Zhang X, Nie W, Ma Y, Tian Q (2017) Cryptanalysis and improvement of an image encryption algorithm based on hyper-chaotic system and dynamic s-box. Multimed Tools Appl 76(14):15641–15659
169. Liu Y, Tong X, Ma J (2016) Image encryption algorithm based on hyper-chaotic system and dynamic s-box. Multimed Tools Appl 75(13):7739–7759
170. Norouzi B, Mirzakuchaki S (2017) Breaking a novel image encryption scheme based on an improper fractional order chaotic system. Multimed Tools Appl 76(2):1817–1826
171. Zhao J, Wang S, Chang Y, Li X (2015) A novel image encryption scheme based on an improper fractional-order chaotic system. Nonlinear Dyn 80(4):1721–1729

172. Peng H, Tian Y, Kurths J, Li L, Yang Y, Wang D (2017) Secure and energy-efficient data transmission system based on chaotic compressive sensing in body-to-body networks. IEEE Trans Biomed Circuits Syst 11:558–573
173. Cao W, Zhou Y, Chen CP, Xia L (2017) Medical image encryption using edge maps. Signal Process 132:96–109
174. Hua Z, Yi S, Zhou Y (2018) Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process 144:134–144
175. Sajjad M, Muhammad K, Baik SW, Rho S, Jan Z, Yeo S-S, Mehmood I (2017) Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. Multimed Tools Appl 76(3):3519–3536
176. Xu L, Gou X, Li Z, Li J (2017) A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. Opt Lasers Eng 91:41–52
177. Praveenkumar P, Devi NK, Ravichandran D, Avila J, Thenmozhi K, Rayappan JBB, Amirtharajan R (2017) Transreceiving of encrypted medical image—a cognitive approach. Multimed Tools Appl 77:1–26
178. Ismail SM, Said LA, Radwan AG, Madian AH, Abu-Elyazeed MF (2018) Generalized double-humped logistic map-based medical image encryption. J Adv Res 10:85–98
179. Li S, Li C, Chen G, Bourbakis NG, Lo KT (2008) A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Process Image Commun 23(3):212–223
180. Li C, Lo KT (2011) Optimal quantitative cryptanalysis of permutation-only multimediaciphers against plaintext attacks. Signal Process 91(4):949–954
181. Li Y, Song B, Cao R, Zhang Y, Qin H (2016) Image encryption based on compressive sensing and scrambled index for secure multimedia transmission. ACM Trans Multimed Comput Commun Appl (TOMM) 12(4s):62
182. Huang X, Ye G, Chai H, Xie O (2015) Compression and encryption for remote sensing image using chaotic system. Secur Commun Netw 8(18):3659–3666
183. Xiang T, Hu J, Sun J (2015) Outsourcing chaotic selective image encryption to the cloud with steganography. Digit Signal Process 43:28–37
184. Xia Z, Wang X, Zhang L, Qin Z, Sun X, Ren K (2016) A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. IEEE Trans Inf Forensics Secur 11(11):2594–2608
185. Jin X, Guo K, Song C, Li X, Zhao G, Luo J, Li Y, Chen Y, Liu Y, Wang H (2016) Private video foreground extraction through chaotic mapping based encryption in the cloud. In: International conference on multimedia modeling. Springer, pp 562–573
186. Xia Z, Xiong NN, Vasilakos AV, Sun X (2017) EPCBIR: an efficient and privacy-preserving content-based image retrieval scheme in cloud computing. Inf Sci 387:195–204
187. Cui H, Yuan X, Wang C (2017) Harnessing encrypted data in cloud for secure and efficient mobile image sharing. IEEE Trans Mobile Comput 16(5):1315–1329
188. Zou Q, Wang J, Ye J, Shen J, Chen X (2017) Efficient and secure encrypted image search in mobile cloud computing. Soft Comput 21(11):2959–2969
189. El-Bakary EM, El-Rabaie E-SM, Zahran O, El-Samie FEA (2017) Drpe encryption with chaotic interleaving for video communication. Wirel Pers Commun 97(1):1373–1384
190. Long M, Peng F, Li H (2017) Separable reversible data hiding and encryption for HEVC video. J Real-Time Image Processing:1–12
191. Su Y, Tang C, Chen X, Li B, Xu W, Lei Z (2017) Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map. Opt Lasers Eng 88:20–27
192. Sallam AI, El-Rabaie E-SM, Faragallah OS (2017) Efficient HEVC selective stream encryption using chaotic logistic map. Multimed Syst 24:1–19
193. Khlif N, Masmoudi A, Kammoun F, Masmoudi N (2018) Secure chaotic dual encryption scheme for H.264/AVC video conferencing protection. IET Image Process 12(1):42–52
194. Wang W, Peng D, Wang H, Sharif H, Chen H-H (2007) Energy-constrained quality optimization for secure image transmission in wireless sensor networks. Adv Multimed. https://doi.org/10.1155/2007/25187
195. Wang W, Peng D, Wang H, Sharif H (2009) An adaptive approach for image encryption and secure transmission over multirate wireless sensor networks. Wirel Commun Mobile Comput 9(3):383–393
196. Wang W, Hempel M, Peng D, Wang H, Sharif H, Chen H-H (2010) On energy efficient encryption for video streaming in wireless sensor networks. IEEE Trans Multimed 12(5):417–426
197. Khan MA, Ahmad J, Javaid Q, Saqib NA (2017) An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box. J Mod Opt 64(5):531–540
198. Chen R-J, Sun Y-L, He D (2012) Video encryption based on generalized cat mapping and H. 264. Internet Things Technol 1:017
199. Muhammad K, Hamza R, Ahmad J, Lloret J, Wang HHG, Baik SW (2018) Secure surveillance framework for IoT systems using probabilistic image encryption. IEEE Trans Ind Inform 14(8):3679–3689
200. Nagy G, Seth S, Einspahr K (1987) Decoding substitution ciphers by means of word matching with application to OCR. IEEE Trans Pattern Anal Mach Intell PAMI–9(5):710–715
201. Handley JC, Buckley RR (2005) Selective encryption of mixed raster content layers, Oct. 11 2005. US Patent 6,954,532