Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 5012496, 17 pages
https://doi.org/10.1155/2021/5012496

Review Article

Computational Image Encryption Techniques: A Comprehensive Review

Mandeep Kaur,[1] Surender Singh,[1] and Manjit Kaur[2]

[1]*Computer Science and Engineering Department, Chandigarh University, Mohali, India*
[2]*Computer Science Engineering, School of Engineering and Applied Sciences, Bennett University, Greater Noida, India*

Correspondence should be addressed to Manjit Kaur; manjit.kr@yahoo.com

Received 28 April 2020; Revised 27 June 2020; Accepted 30 June 2020; Published 19 July 2021

Academic Editor: Erivelton Geraldo Nepomuceno

Images contain very sensitive and confidential information. Because images play a significant role in many applications such as military communication, remote-sensing, and medical-imaging, therefore, it is necessary to protect sensitive and confidential information from unauthorized use and modification. To achieve this objective, encryption is one of the best methods among the information hiding methods. In recent years, many image encryption approaches are designed by the researchers. They use different concepts for image encryption to increase security. The main aim of this paper is to present a comprehensive review of the existing image encryption approaches. These approaches are categorized based on different concepts such as chaotic maps, DNA, compressive sensing, and optical image encryption. Comparisons are made among the existing approaches to access the various security parameters. Key performance metrics are also presented. The future scope of image encryption is also presented to encourage the research community.

1. Introduction

Due to advancements in technology, digital images are utilized in many applications such as medical imaging, remote sensing, and private conferencing. These images may contain confidential and sensitive information [1]. The transmission of these images over public networks is prone to several issues such as modification and unauthorized access. The leakage of sensitive information may raise military, national security, and discretionary issues. Moreover, when individuals wish to exchange images through a public network, it is necessary to assure their privacy. Therefore, images require security against different security attacks [2].

From the literature, it has been found that image encryption approaches can be utilized to provide security to these images. Image encryption is a procedure which converts plain image to an encrypted image by employing a secret key. The decryption process decrypts the cipher image into the original image by employing the secret key [3, 4]. Mainly, decryption operation is like encryption operation but applies in reverse order. The secret keys play a critical role in encryption. Because the security of the encryption approach is mainly dependent on it, two types of keys are utilized, namely, private key and public key [5, 6]. In the private key, the encryption and decryption processes use the same key to encrypt and decrypt the images. In the case of a public key, two keys are utilized, one key for encryption and one for decryption. In this, the encryption key is made public, but the decryption key is always kept private [7]. Figure 1 represents the block diagram of image encryption.

1.1. Basic Terms Utilized in Encryption.

(i) Plain image: it is the image that needs security while there is transmission over the public network. It is also known as the original or input image.

(ii) Cipher image or encrypted image: the plain image converted into a nonreadable form after encryption is called a cipher image.

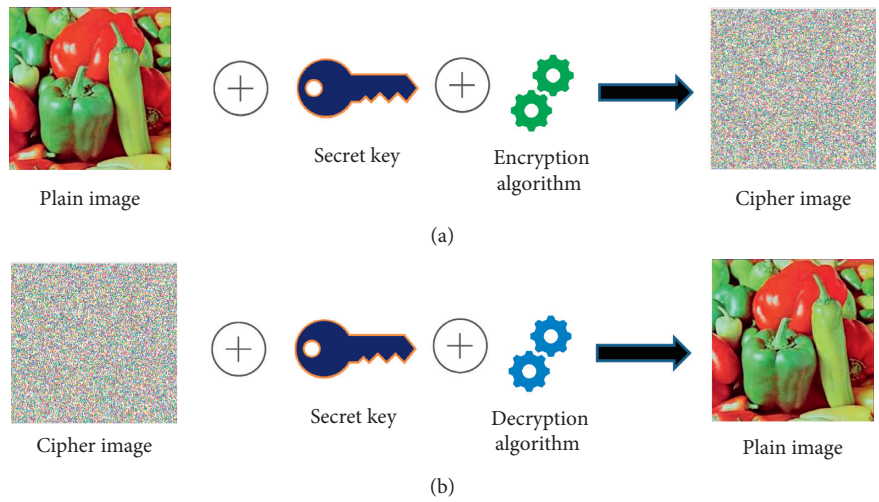

Figure 1: General framework of image encryption. (a) Encryption process at sender side. (b) Decryption process at receiver side.

(iii) Encryption: it is the process of converting a plain image into a cipher image utilizing an encryption approach and a secret key.

(iv) Decryption: at the receiver side, the cipher image is converted into a plain image utilizing a decryption approach and a secret key. This process is known as decryption.

(v) Key: the security of the encryption approach is mainly depending on the key. It can be numeric or alphanumeric. Both encryption and decryption need the key to performing their respective operations. Strong keys are always needed for better security of information.

1.2. Materials and Methods. Various image encryption approaches are designed so far. With time, researchers have also applied different types of concepts to increase the security of images. The traditional approaches such as DES, AES, and IDEA, have been obsolete in the case of images. Because the images have different properties as compared to text, many image encryption approaches are utilized in the last few decades; but in this study, we have considered only the last eight-year approaches (2013–2020), because we have found the application of diverse concepts in the area of information security.

Preferred reporting items for systematic reviews and meta-analyses (PRISMA) method is used in this study for getting the accurate results in order to summarize the existing work in image encryption field. The method consists of four phases: (i) identification, (ii) screening, (iii) eligibility, and (iv) inclusion that provide the accurate report for the analysis. By using the PRISMA method, the concluding outcome will be free of biases of the review studies; however, most of the reviews may be suffered from the selective outcome reports. In addition to this, number of sources can be utilized by giving the relevant Boolean queries for eliminating the articles that are not relevant to the study. The model begins from the step of identifying the sources of article, after that screening is performed by eliminating the replica and also the irrelevant articles by going through the titles and abstracts. Afterward, the articles left will be further screened by going through the full paper and all the articles that are not relevant to the study are excluded from the review studies.

In this study, five well-known databases have been selected for getting the relevant articles for performing the review including Wiley library, IEEE, Springer, Science-Direct, and Google scholar. The Boolean query that has been run on these databases are: Query: TITLE-ABS-KEY ("image ∗ " AND "encrypt ∗ " AND PUBYEAR 2015–2020). Based on the abovementioned query entered in five different databases, a total of 10446 articles were found for related articles. Using PRISMA method, 9523 articles were excluded based on titles and abstracts. Now the remaining 923 were again the screened and 397 articles were again removed from the study as they were either the conference articles or the duplicate ones. Now, the number comes to 526 out of which 348 articles are not relevant to the study as these are not having all the evaluation metrics that were the actual evaluation parameters of the study. Thereafter, 19 articles were again excluded as they were not written in English language. Then, the final number that comes after passing through various parameters was 159. The detailed analysis report of all these 159 articles with their outcomes is summarized. Figure 2 shows the flow chart for the database search of publications for systematic reviews.

1.3. Contribution. To the best of our knowledge, this is the first systematic literature review paper which has discussed the metaheuristics-based image encryption techniques. Beside this, we have also compared optical image encryption techniques which were ignored in the most of the existing review papers. Also, by reviewing the latest papers, we have evaluated various shortcomings of the recently published image encryption techniques. The main contributions of this paper are as follows:

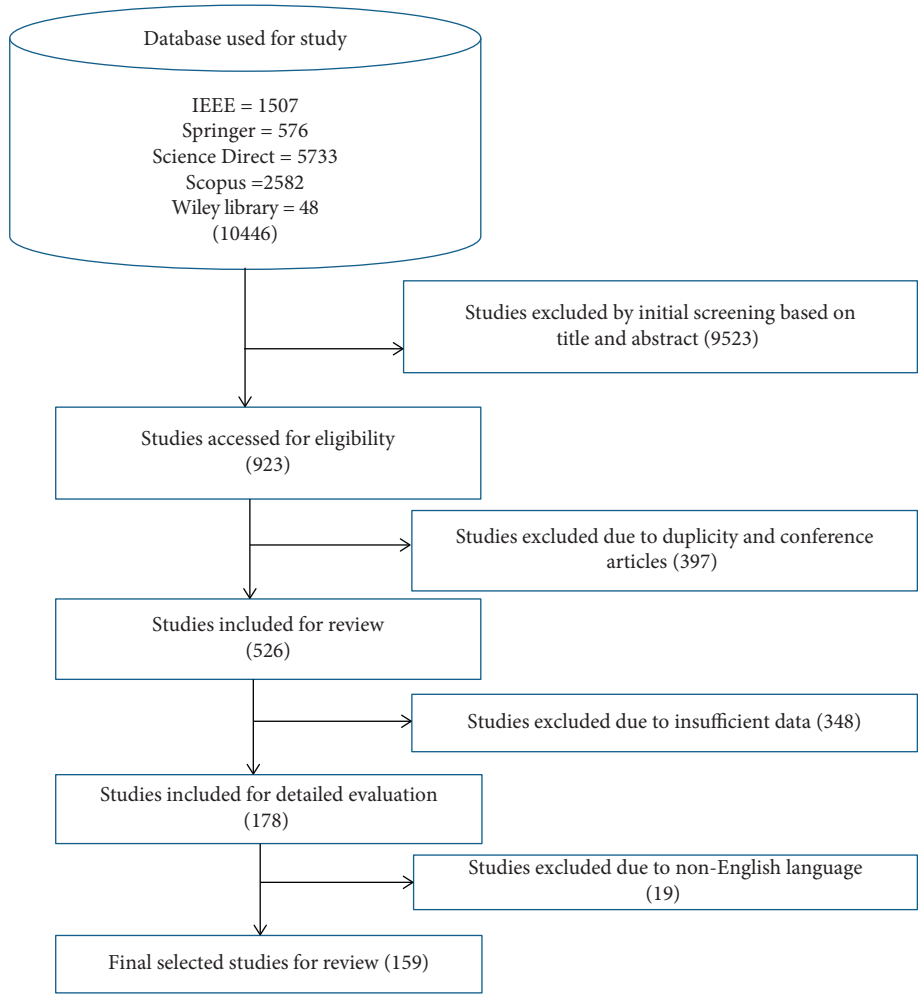

Figure 2: The flow chart for the database search of publications for systematic reviews.

(i) Initially, the existing image encryption approaches are categorized based upon various concepts such as chaos, DNA, compressive sensing, and optical.

(ii) Various metrics utilized to compute the performance of image encryption approaches are also discussed.

(iii) Comparisons are made among the existing approaches to access the various security parameters.

(iv) Finally, the future scope of image encryption is also presented to encourage the research community.

The remaining paper is organized as follows: the performance metrics are discussed in Section 2. In Section 3, various categories of the existing image encryption approaches are discussed. Section 4 presents the comparative analyses among the existing image encryption approaches. Future directions are discussed in Section 5. Section 6 concludes the paper.

2. Evaluation Parameters

Evaluation parameters are utilized to assess the performance of image encryption. There are many security attacks performed by the attackers to break the encryption approach as well as to find the key. Attackers mainly utilize the cryptanalysis to study the encryption approaches [8, 9]. Therefore, it is necessary to hide the statistics of plaintext and the secret key. The strength of image encryption can be evaluated utilizing security and quality analyses. The quality analysis assesses the image quality of decrypted image utilizing peak signal-to-noise ratio, mean square error, etc. The security analyses include statistical analysis, differential analysis, and key analysis.

Statistical properties of the generated cipher image can be tested utilizing entropy, correlation coefficient, and histogram analysis. It is required that the encryption approaches do not provide statistical details of the plain image. Sometimes, we assume that an attacker obtains the details of the encryption approach without knowing the key. In other words, the key is considered to be embedded in the encryption approach. Then, the attacker supplies an image to the encryption approach and gets a corresponding cipher image. Thereafter, he made small changes in the same image and got another cipher image. Then, he tries to find the similarity between two ciphered images to break the encryption approach. It means that the encryption approach is

required to be sensitive to small changes towards the plain image. It is assessed utilizing differential analysis. In this, unified average changing intensity and number of pixel change rate metrics can be utilized for the same.

As we know that the performance of the image encryption approach is mainly dependent on the key, therefore, it should be large enough, so that it cannot be guessed easily. Secondly, it should be sensitive to small changes. The encryption approach should generate a totally different cipher image, even if the only one-bit difference is present in two keys. While there is transmission over a noisy channel, the cipher image may get affected. Therefore, the encryption approach should be robust against noise attacks. The receiver should be able to recover the original image. In real-time applications, the speed of encryption approaches matters a lot. It is always desirable that the encryption approach should be fast. Table 1 defines the various parameters utilized for image encryption performance evaluation. It also presents the desirable expectation of every parameter.

3. Image Encryption Approaches

Different types of image encryption approaches are designed so far. By reviewing the literature, we have divided it into different types such as spatial, transform, optical, and compressive sensing based image encryption approaches. Figure 3 demonstrates the categories of image encryption approaches. In the preceding subsection, these approaches are discussed and analyzed utilizing evaluation metrics. These parameters are KA, NPCR, HA, UACI, IE, CC, and NA. In comparisons, ✓ and ✗ symbols are utilized to represent whether the given approach has considered the respective metric and not, respectively.

3.1. Image Encryption in Spatial Domain. The approaches that are directly manipulating the pixels of the image are considered as spatial domain approaches. The various spatial domain-based image encryption are present in the literature. But we have considered the most famous approaches such as chaotic-based, elliptic curve-based, fuzzy-based, DNA, and Metaheuristics-based approaches.

3.1.1. Chaos-Based Image Encryption Approaches. Chaotic maps have great significance in the field of encryption. These maps generate random numbers that are utilized as secret keys in encryption [17]. The reason is its properties such as dynamic and deterministic nature, sensitive to initial conditions, and ergodicity. Different types of chaotic maps are utilized so far. But these are mainly divided as one-dimensional and higher-dimensional chaotic maps. Chaotic maps help in performing the confusion and diffusion operations in the encryption process [18]. Figure 4 demonstrates the diagrammatic flow of the chaotic maps in the image encryption approach.

Chen et al. [19] developed an image encryption approach utilizing a 2D sine map and Chebyshev map. It designed an antidegradation universal approach for chaotic maps, which improves the performance even on low-accuracy devices. Xuejing and Zihui [20] proposed image encryption based on spatiotemporal chaotic map and DNA encoding. Firstly, a plain image is changed into three DNA matrices dependent on a random encoding rule; afterward, DNA resultant is joined into a modern matrix. Then, it is permutated by the ascent matrix to generate the ciphered image. Wang et al. [21] utilized coupled map lattices (CML) and the DNA approach to encrypt the images. Ismail et al. [22] examined a new lossless image encryption system that was based on fractional-order and double-humped logistic maps.

Wu et al. [23] designed an encryption approach utilizing a 2D discrete wavelet transform and hyperchaotic system for color images. Chai et al. [24] designed an encryption approach for color images utilizing a 4D memristive hyperchaotic map with genetic recombination. Luo et al. [25] developed an image encryption approach based on quantum coding and hyperchaos system. Kumar Patro and Acharya [26] proposed an image encryption approach utilizing a piece-wise linear chaotic map (PWLCM). In this, a rotating permutation is applied row-wise and column-wise. At last, it applies a diffusion operation on the row, column, and block to generate the ciphered image.

Feng et al. [27] utilized a discrete logarithm and a memristive chaotic system to encrypt the images. Wang and Gao [28] developed an image encryption strategy based on matrix semitensor. Hyperchaotic Lorenz map is also utilized to generate random numbers. Hua and Zhou [29] designed an approach for encrypting the images that provide excellent effects against differential and statistical attacks. Image filtering idea is utilized in image encryption to enhance the security of encryption. Gan et al. [30] implemented an image encryption approach based on 3D bit-plane confusion. Lu et al. [31] proposed an image encryption approach based on chaotic map and S-box. The discrete compound chaotic map was designed in this approach. S-box is also constructed utilizing logistic-sine system.

Deng and Zong [32] presented a binary image encryption approach based on chaotic mapping. The authors hypothetically examined the approach and figured out that the approach did not need to have the earlier information on the orbital distribution and one can pick out any chaotic model. Patro et al. [33] developed a color image encryption approach that overcomes the drawbacks of execution block-level dispersion processes in arbitrary sized images. Wang et al. [34] implemented an image encryption approach utilizing logistic-dynamic mixed linear-nonlinear coupled map lattices.

Ye et al. [35] utilized a memristive chaotic map to generate the secret keys to perform image encryption. Liu et al. [36] designed a fast image encryption approach derived from a sine map and the iterative chaotic map with infinite collapse based on a closed-loop modulation coupling model. Cao et al. [37] designed an image encryption approach for medical images by utilizing edge maps. It consists of three parts: bit-plane decomposition, random number generator, and permutation. Chai [38] designed a bit-level Brownian motion and 1D chaotic framework for encrypting the digital images. Table 2 demonstrates the comparison among the exiting chaos-based image encryption approaches. It can be

Table 1: Image encryption evaluation parameters.

Evaluation parameter	Abbr.	Expectation
Key space analysis [3]	KA	Large key size (more than 2^{100})
Histogram analysis [1]	HA	Pixels should uniformly distribute
Information entropy [10]	IE	Equal to 8, for a 256-gray level image
Noise attack [11]	NA	Ought to be safe to noise attacks
Correlation coefficient [12]	CC	Near to 0
Mean squared error [13]	MSE	Minimum
Peak signal-to-noise ratio [2, 14]	PSNR	Low between encrypted and actual images; high between the ciphered and decrypted images
Execution time [2]	ET	Minimum for practical implementation
Number of pixel change rate [15]	NPCR	Maximum value (according to critical analysis, it should be near to 99.609% or more)
Unified average changing intensity [16]	UACI	Minimum value (according to critical analysis, it should be near to 33.464% or more)

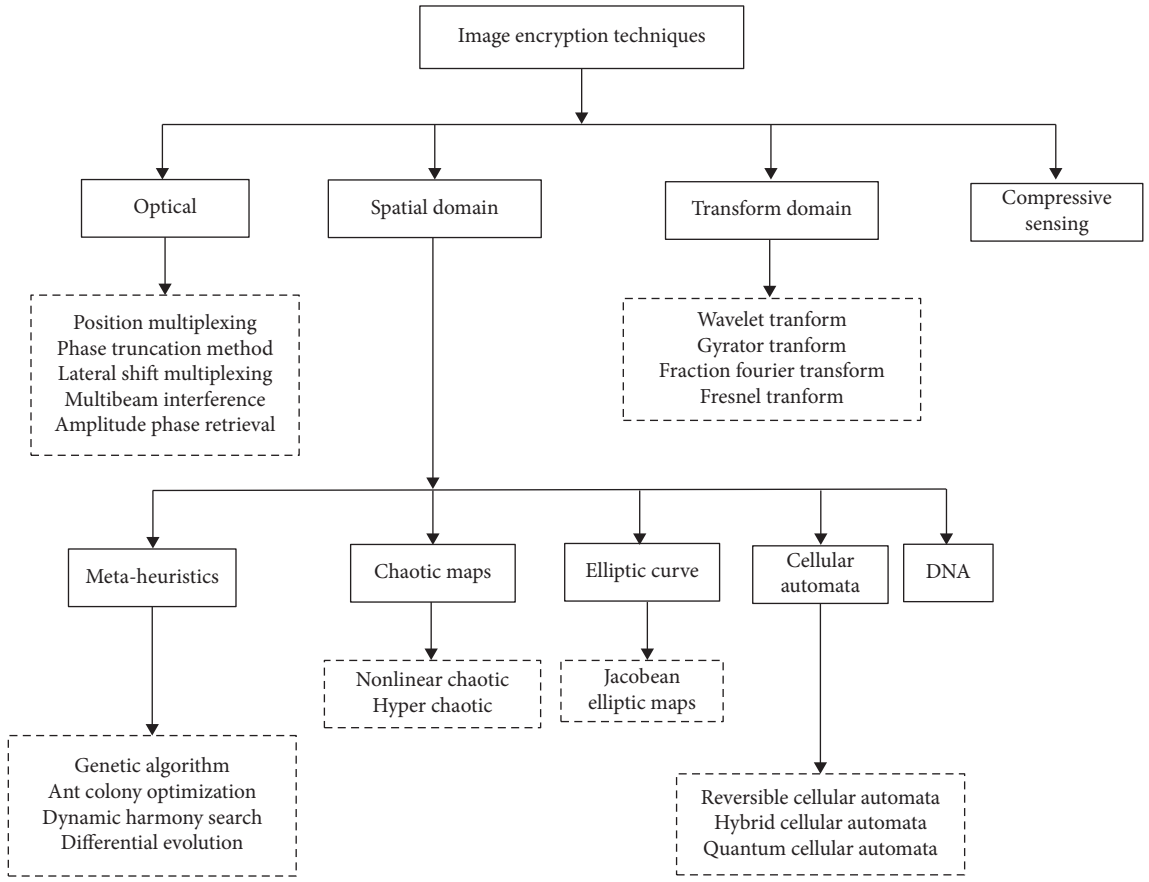

Figure 3: Categorization of image encryption approaches.

seen that most of the approaches do not satisfy all the security parameters. Therefore, it is still an open area for research.

3.1.2. Elliptic Curve-Based Image Encryption. Elliptic curve cryptography (ECC) works on the least amount of memory with the small key size [39]. Figure 5 demonstrates the use of elliptic curve in image encryption. The color image is initially compressed and changed into gray scale. Then, encryption is done by utilizing elliptic curve, 3D Lorenz chaotic map, and 4D Arnold cat map [40].Hayat and Azam [41] developed an approach based on pseudorandom numbers and substitution boxes for encrypting a digital image by utilizing an elliptic curve. Luo et al. [42] presented the asymmetric image encryption approach which depends on chaotic theory and the elliptic curve ElGamal (EC-ElGamal) cryptography. Banik et al. [43] discovered a medical image encryption approach based on Mersenne Twister pseudorandom number generator and elliptic curve analog ElGamal cryptosystem. The proposed approach enlivens the encryption time just as take care of the issue of information

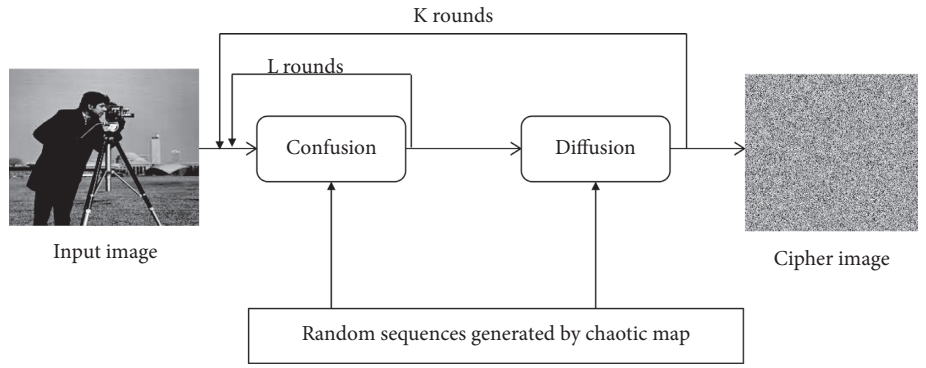

Figure 4: Working of chaotic map-based image encryption.

Table 2: Comparison of various chaotic-based image encryption approaches.

Ref.	Technique	HA	KA	IE	NA	NPCR	UACI	CC
[19]	Logistic map	✓	✓	✓	✓	✓	✓	✗
[20]	DNA and chaotic system	✓	✓	✓	✓	✓	✓	✗
[21]	Chaotic-based DNA	✓	✓	✓	✓	✓	✓	✗
[22]	Edge detection and chaotic map	✗	✗	✓	✓	✓	✓	✗
[23]	6D hyperchaotic	✓	✓	✓	✓	✓	✗	✓
[24]	Hyperchaotic system	✓	✓	✓	✓	✓	✗	✓
[25]	Hyperchaotic with quantum coding	✓	✓	✓	✓	✓	✓	✓
[26]	PWLCM system	✓	✓	✓	✓	✓	✓	✓
[27]	Standard memristive chaotic system	✓	✓	✓	✓	✓	✓	✓
[28]	Semitensor product theory	✗	✗	✓	✓	✓	✗	✓
[30]	3D bit-plane permutation	✓	✓	✓	✓	✓	✗	✓
[32]	Chaotic map	✗	✗	✓	✓	✓	✗	✓
[33]	Block level diffusion operation	✓	✓	✓	✓	✓	✗	✗
[34]	Coupled map lattices	✓	✓	✓	✓	✓	✓	✓
[35]	Mixed memristive chaotic circuit	✓	✓	✗	✓	✓	✓	✓
[36]	Chaotic map	✓	✓	✓	✓	✗	✗	✗
[37]	Edge maps	✓	✓	✗		✗	✗	✗
[38]	Bit level Brownian motion	✗	✗	✓	✓	✓	✗	✗

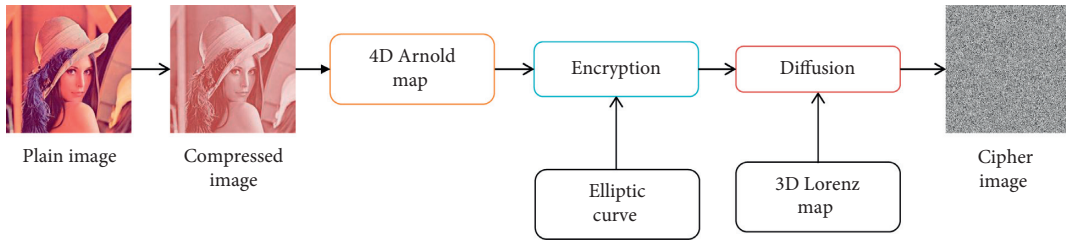

Figure 5: Chaotic map and elliptic curve-based image encryption.

extension related with ElGamal cryptosystem. Reyad and Kotulski [44] studied an image encryption approach which depends on computational tasks (such as add, double, and multiply) that depend on ECC.

Kumar et al. [45] implemented an image encryption approach utilizing ECC and DNA encoding. The approach initially encodes the RGB image utilizing DNA encoding. Thereafter, the elliptic curve Diffie–Hellman encryption (ECDHE) is utilized to perform encryption. Zhang and Wang [46] presented an improved ECC-based image encryption approach. The Diffie–Hellman approach is utilized to generate the secret key. The chaotic map is also applied in the combination with ECC to perform permutation and diffusion. Laiphrakpam and Khumanthem [47] developed an image encryption approach based on a chaotic framework and elliptic curve over a limited field.

Dawahdeh et al. [48] developed an image encryption approach by combining ECC with Hill cipher (ECCHC). Toughi et al. [39] implemented image encryption by utilizing an elliptic curve to obtain a series of random numbers established on curves. Liu et al. [49] designed a Menezes–Vanstone elliptic curve cryptosystem. In this, the 2D

fractional triangle function is utilized with a discrete chaotic map. Wu et al. [40] proposed a color image encryption approach based on chaotic systems and elliptic curve ElGamal approach. Firstly, the original image is compressed and then the compressed image is encrypted by utilizing the improved 4D cat map.

Nagaraj et al. [50] combined the elliptic curve and magic matrix operation to encrypt the images. The input image lies on the points on the elliptic curve utilizing the transform approach. The image is decomposed into information matrices. Every single pixel of an image is permuted by the magic matrix. At last, each pixel is diffutilized to produce a cipher image by utilizing ECC. Table 3 demonstrates the comparison among various ECC-based image encryption approaches. It is observed that there exists no such approach which has considered all parameters.

3.1.3. Cellular Automata-Based Image Encryption Approaches. Cellular automata have been widely used in image encryption as a pseudorandom generator. These models are complex which have a degree of efficiency and robustness. Cellular automata use rules to produce random sequences. Due to the properties of cellular automata such as parallelism and easy and simple hardware structure, it is significant for encryption approaches [51]. Figure 6 demonstrates the general framework of cellular automata-based image encryption. The confusion and diffusion operations are performed by utilizing the key generator and cellular automata, respectively. Cellular automata generate random sequences to diffuse the pixel values of the image [7].

Khan et al. [52] designed a hybrid image encryption approach by merging a logistic sine system with 2D cellular automata. Mondal et al. [51] implemented an image encryption approach that is exceptionally secure based on a chaotic skew tent map and cellular automata. Zhang et al. [53] utilized 1D chaotic map for generating the pseudorandom number. To perform permutation-substitution, bit-level cellular automata are utilized to generate an encrypted image.

Su et al. [54] designed a deterministic image encryption approach based on reversible cellular automata (DERCA). This approach addresses the problem of similarity search on encrypted images. It finds one-to-many mapping between histograms of encrypted and original images. Ramírez et al. [55] presented a partial image encryption strategy depending on the cellular machine rule. The security examination demonstrates that this cryptosystem is impervious to various tests. Wang et al. [56] evaluated the image cryptosystem on the two-dimensional partitioned cellular automaton.

Yaghouti Niyat et al. [57] implemented a nonuniform cellular automata system to illuminate the major drawbacks of cellular automata in cryptography. It incorporates a predetermined number of inversion rules. Chai et al. [58] utilized a memristive hyperchaotic system, cellular automata, and DNA sequence operations to encrypt the images. Wei et al. [59] designed a double-color image-enciphering method depending on off-axis Fourier holography and maximum length cellular automata (MLCA). The color image is separated into red, green, and blue, three channels, and all channels are autonomously scrambled by utilizing MLCA.

Chen et al. [60] developed an encryption and compression approach based on a combination of Kronecker CS (KCS) with elementary cellular automata (ECA). Souyah and Faraoun [61] evaluated the symmetric approach for enciphering digital images by combining chaos and cellular automata (CA) under the situation of one round encryption or decryption. Tralic and Grgic [62] presented an approach for image encryption based on a 2D cellular automaton and pixel division. Application of the balanced 2D cellular automata with amplified Moore neighborhood for each degree of pseudorandom key-image makes it different from existing approaches.

Yang et al. [63] proposed an encryption approach for grayscale images based on 1D quantum cellular automata. Murugan et al. [64] designed an image encryption approach by combining chaos and cellular automata. Logistic map and Conway's game-of-life cellular automata are utilized in the permutation process and the Chebyshev map and Lorenz equation are utilized for diffusion.

Souyah and Faraoun [65] discussed the approach for image encryption that combines the image's quadtree decomposition approach with reversible memory cellular automata mechanism. Enayatifar et al. [66] designed an encryption approach by utilizing a Tinkerbell hybrid model of a chaotic map, deoxyribonucleic acid (DNA), and cellular automata. Table 4 demonstrates the comparison of various cellular automata-based image encryption approaches. It is found that no approach has utilized every performance metric.

3.1.4. DNA-Based Image Encryption Approaches. Deoxyribonucleic acid (DNA) cryptography has become very popular due to its properties such as massive parallelism, huge storage, and ultra-low power consumption. The complementary rules of DNA are utilized to perform encoding and decoding [73]. Figure 7 demonstrates the block diagram of DNA-based image encryption process. Firstly, the color image is decomposed into three channels red (R), blue (B), and green (G). After that, DNA encoding and XOR operations are utilized to encode the channels. A chaotic map is utilized to scramble matrices. Finally, three R, G, and B channels are combined to obtain the cipher image [74].

Wu et al. [75] designed the color image encryption approach by utilizing three one-dimensional chaotic maps with DNA sequences. The original image and keystream are changed into matrices utilizing DNA operation. Complementary and XOR encoding operations are connected to rearrange the matrices. The matrices are decayed into blocks and rearrange them arbitrarily. DNA addition and XOR encoding operations are performed on these scrambled matrices to get the cipher image. Mondal and Mandal [76] utilized two pseudorandom number sequences with DNA for the encryption of sensitive images. Wu et al. [77] implemented an encryption approach for color images

Table 3: Comparison among various elliptic curve-based image encryption approaches.

Ref.	Technique	HA	KA	IE	NA	NPCR	UACI	CA	PSNR	MSE
[41]	Elliptic curve cryptography	✓	✓	✓	✓	✓	✓	✓	✗	✗
[42]	Elliptic with EIGamal encryption	✓	✓	✓	✓	✓	✓	✓	✗	✓
[43]	Elliptic curve with Mersenne Twister	✓	✓	✓	✓	✓	✗	✓	✓	✗
[39]	Elliptic curve and AES	✓	✓	✗	✗	✓	✗	✓	✗	✗
[45]	DNA with elliptic curve	✗	✗	✓	✓	✗	✗	✓	✓	✓
[40]	Elliptic curve EIGamal encryption	✓	✓	✓	✓	✓	✗	✓	✓	✗
[46]	Elliptic curve with ECC	✓	✓	✓	✓	✓	✗	✓	✗	✗
[47]	Elliptic curve over finite field	✗	✗	✓	✓	✓	✓	✗	✓	✗
[48]	Elliptic with Hill cipher	✗	✓	✗	✗	✓	✗	✗	✓	✗
[49]	Menezes–Vanstone elliptic curve	✓	✓	✗	✓	✓	✗	✗	✗	✗

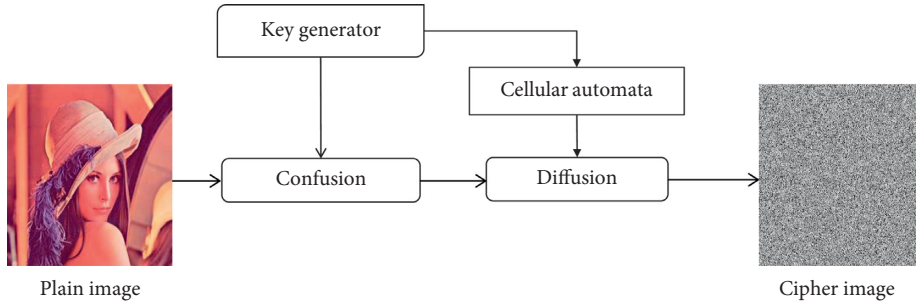

Figure 6: General framework of cellular automata-based image encryption.

Table 4: Comparison of various cellular automata-based image encryption approaches.

Ref.	Technique	KA	NPCR	UACI	IE	CA	HA	PSNR	MSE
[54]	Reversible cellular automata	✓	✓	✓	✗	✓	✓	✗	✗
[55]	Cellular automata	✗	✗	✗	✓	✗	✗	✗	✗
[67]	Logistic mapped convolution	✗	✗	✓	✓	✓	✗	✓	✓
[56]	Partitioned cellular automata	✗	✗	✗	✗	✗	✓	✗	✗
[57]	Hybrid chaotic system	✗	✗	✓	✓	✓	✓	✗	✗
[58]	Memristive hyperchaotic	✓	✓	✓	✓	✗	✗	✓	✓
[59]	Holography	✗	✗	✓	✓	✗	✓	✗	✗
[60]	Kronecker compressed sensing	✓	✓	✓	✓	✓	✓	✓	✗
[61]	Weighted histogram	✗	✗	✓	✓	✓	✓	✗	✗
[62]	Pixel separation	✓	✓	✓	✓	✓	✓	✗	✗
[68]	8-layer cellular automata	✓	✓	✓	✓	✓	✓	✗	✗
[63]	Quantum cellular automata	✓	✓	✓	✗	✗	✓	✓	✓
[64]	Conway's cellular automata	✓	✓	✓	✗	✓	✓	✗	✗
[65]	Quadtree decomposition	✗	✗	✗	✓	✓	✗	✗	✗
[69]	DNA and cellular automata	✓	✓	✓	✗	✗	✗	✗	✗
[66]	Hybrid DNA	✓	✓	✓	✓	✓	✗	✗	✗
[70]	3D cellular automata	✓	✓	✓	✓	✗	✗	✗	✗
[51]	Chaotic skew tent map	✓	✓	✓	✓	✓	✓	✓	✓
[71]	4^{th} order cellular automata	✓	✓	✓	✓	✓	✗	✗	✗
[72]	Linear cellular chaos-based automata	✗	✗	✓	✗	✗	✗	✗	✗
[52]	FSM-based DNA	✗	✗	✓	✓	✗	✓	✗	✗
[53]	Coupled logistic Bernoulli map	✓	✓	✗	✗	✗	✗	✗	✗

utilizing DNA. This approach contains four steps: key generation, DNA sequence for permutation, DNA sequence for diffusion, and diffusion process for pixel level.

Li et al. [78] enhanced the security of image encryption utilizing complex chaotic maps and quaternary coding in DNA. Wang et al. [79] implemented a DNA sequence and CML-based color image encryption approach. Initially, R, G, and B components of the color image are utilized to form the matrix. DNA encoding operation is utilized further to encrypt rows and columns of the matrix to get an encrypted image. Nematzadeh et al. [80] developed a DNA and binary search tree- (DNA-BST-) based image encryption approach. Rehman et al. [15] designed a block cipher image encryption approach for gray images based on DNA complementary

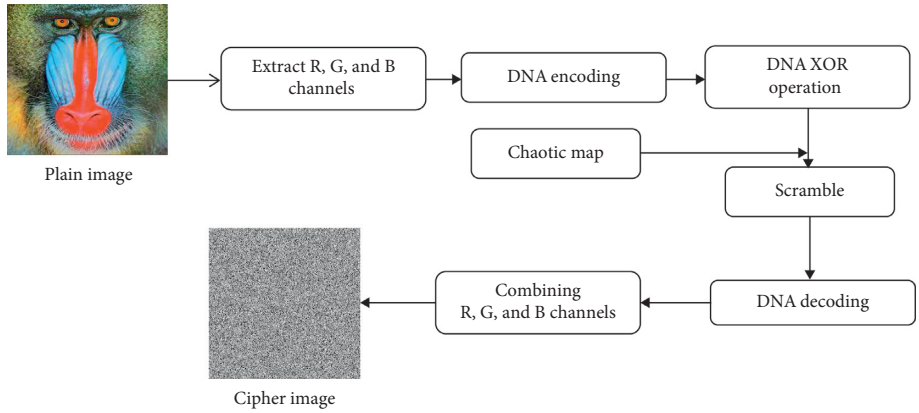

Figure 7: DNA-based image encryption.

rules and piece-wise linear chaotic map. Jain and Rajpal [81] implemented an image encryption approach utilizing DNA and a 2D chaotic map. In this, the input image encoded by utilizing DNA operation as a resultant matrix was generated. Resultant matrix permuted by utilizing a 2D chaotic map followed by DNA decoding operation to get the cipher image.

Wang and Liu [82] designed an image encryption approach based on DNA operation and chaos mapping. In this approach, eight DNA rules are applied to encode the rows of the plain image. The selection of DNA rule is done through a chaotic map. Zhang et al. [83] designed image encryption utilizing permutation and diffusion based on DNA encoding and Feistel network. Chai et al. [84] utilized a chaotic system and DNA to design an image encryption approach. In this approach, permutation and diffusion are done by the DNA matrix which makes it different from the traditional approach. Zhang et al. [85] implemented an image encryption approach utilizing DNA encoding, Lorenz chaotic approach, and Chan's hyperchaotic approach. DNA encoding rules are utilized randomly to improve the security of the encryption process.

Liu et al. [86] designed an image encryption approach by utilizing dynamic S-boxes calm of DNA and chaotic system. Dynamic S-box calm of DNA encoding operation is utilized to confuse the pixel values of the image for the encryption process. Norouzi and Mirzakuchaki [87] presented an image encryption by utilizing DNA sequence operation and cellular neural network. Liu et al. [88] presented the color image encryption approach based on DNA masking and a hybrid model of multidirectional circular permutation. The initial position of pixels of an image is rotated by circular permutation, and by DNA sequence operation, the values of the pixel are substituted to attain an encrypted image. Zhang et al. [89] designed an image encryption approach based on bit permutation and dynamic DNA encoding. This approach is exceptionally successful against noise and known-plaintext attacks. Table 5 demonstrates the comparison of various DNA-based image encryption approaches. It demonstrates that there exist only two approaches that have utilized every performance metric.

Table 5: Comparison of various DNA-based image encryption approaches.

Ref.	KA	NPCR	UACI	IE	CA	HA	PSNR	MSE
[90]	✓	✓	✓	✓	✓	✓	✗	✗
[76]	✓	✓	✓	✗	✓	✗	✗	✗
[15]	✓	✓	✓	✓	✓	✓	✗	✗
[81]	✓	✓	✗	✓	✗	✓	✗	✗
[77]	✓	✓	✗	✓	✓	✓	✗	✗
[73]	✓	✓	✓	✓	✓	✓	✓	✓
[79]	✓	✓	✓	✗	✓	✓	✗	✗
[80]	✓	✓	✗	✓	✓	✓	✗	✗
[82]	✗	✗	✗	✓	✓	✗	✗	✗
[91]	✓	✓	✓	✓	✓	✓	✓	✓
[83]	✓	✓	✗	✓	✓	✓	✗	✗
[84]	✓	✓	✓	✓	✗	✓	✗	✗
[92]	✓	✓	✗	✗	✗	✗	✗	✗
[93]	✓	✓	✗	✓	✓	✓	✗	✗
[85]	✓	✗	✗	✓	✗	✓	✗	✗
[94]	✓	✓	✓	✓	✓	✓	✓	✗
[86]	✓	✓	✗	✓	✓	✗	✓	✓
[95]	✓	✓	✓	✓	✓	✓	✓	✓
[87]	✓	✓	✓	✓	✓	✓	✓	✓
[78]	✗	✗	✓	✓	✓	✓	✗	✗
[88]	✓	✓	✗	✓	✓	✓	✗	✗
[89]	✗	✗	✓	✓	✓	✓	✗	✗

3.1.5. Metaheuristics-Based Image Encryption Approaches. Metaheuristic approaches are mainly utilized in a situation where we need optimized results. Recently, the use of such approaches has been increased in the image encryption. There are two aspects to use metaheuristic approaches in image encryption: (a) generate multiple cipher images and then select optimized one and (b) optimize the initial parameters of chaotic maps to generate efficient keys. Researchers have implemented the image encryption approaches based on metaheuristic approaches, considering different aspects.

Medical images are encrypted by [96] utilizing coupled map lattices and modified genetic algorithm. The genetic algorithm selects the encrypted image which has high entropy. The algorithm approach is utilized by [97] to generate the optimized key. ECC is utilized to perform the encryption

process utilizing an optimized key. Kaur and Kumar [98] utilized differential evolution to optimize the beta-chaotic map to generate efficient secret keys. They further utilized a nondominated sorting genetic algorithm (NSGA) [99] to optimize the initial parameters of the intertwining logistic map.

Genetic approach is applied by [5] to optimize the beta chaotic map. To generate the efficient keys, Nematzadeh et al. [100] utilized NSGA-II for intertwining logistic map. Adaptive differential evolution is utilized by [4] to optimize the initial parameters of the Lorenz chaotic map. In [101], medical gray images are optimized utilizing a genetic algorithm. Talarposhti et al. [102] proposed an image encryption approach based on a dynamic harmony search (DHS) combined with a chaotic map.

Memetic differential evolution is applied by [103] to generate the optimized cipher image. Pareto evolutionary algorithm-II was utilized by [13] to obtain the optimized encrypted image. In [104], NSGA-III is utilized to generate the optimal cipher image by optimizing the hyperchaotic map. In [6], a 5D chaotic map is optimized by combining NSGA and local chaotic maps. Table 6 demonstrates the comparison of various metaheuristic image encryption approaches. Most of the approaches have not applied all the performance metrics.

Table 6: Comparison of various metaheuristic image encryption approaches.

Ref.	NPCR	UACI	KA	HA	IE	CA
[11]	✓	✓	✗	✓	✓	✗
[105]	✓	✓	✓	✗	✓	✓
[102]	✗	✗	✓	✗	✓	✓
[106]	✓	✓	✗	✓	✗	✓
[100]	✓	✓	✓	✓	✓	✓
[96]	✓	✓	✗	✗	✗	✓
[107]	✓	✓	✓	✓	✗	✓
[108]	✗	✗	✓	✓	✗	✓
[109]	✓	✓	✓	✓	✗	✓
[110]	✓	✓	✓	✓	✓	✗
[111]	✓	✓	✗	✓	✓	✓

3.2. Compressive Sensing-Based Image Encryption Approaches. Compressive sensing can perform compression as well as encryption at the same time [112]. It uses a measurement matrix and reconstruction approach to perform the same. The measurement matrix is utilized to perform the compression. At the same time, when the measurement matrix is utilized as a secret key between the sender and receiver, it works as a cryptosystem [113]. Various image encryption approaches based on compressive sensing have been proposed by the researchers. Some of the approaches are discussed in this section.

Ponuma and Amutha [114] utilized chaotic compressive sensing to encrypt the color images. It also performed compression at the same time. The chaotic measurement matrix constructed utilizing one-dimensional chaotic map is utilized. This approach is further enhanced in [115] by making it visually meaningful. Wavelet transform is utilized to hide the encrypted image into a cover image. Shao et al. [116] utilized analog-digital hybrid electro-optic chaotic sources and compressive sensing to encrypt the images. Zhu et al. [117] designed a hybrid approach for image compression and encryption by utilizing block compressive sensing. The nonuniform sampling approach is utilized to improve the efficiency of compression.

Shen et al. [118] utilized nonuniform quantization and compressive sensing to encrypt the images. It reduces the data precision in cipher images while evaluating the true compression ratio (CR). Jiang et al. [119] proposed a color image encryption approach based on compressive sensing and multi-image cross pixel scrambling approach. A discrete wavelet transform is also applied to process the subimages. Yao et al. [120] implemented an image encryption approach depending upon improved two-dimensional closed-loop modulation coupling approach. The approach was combined with compressive sensing to build a fast image encryption process.

Xu et al. [121] implemented an image encryption strategy utilizing compressive sensing, wavelet transform, and chaotic map. Gong et al. [122] utilized compressive sensing and RSA approach for optical image compression and encryption. To sample the initial image, the optical compressive imaging is utilized. Zhu and Zhu [123] encrypted the images based on compressive sensing and cyclic shift. Sparse transform and Gauss matrix is applied to perform compression. Wang et al. [124] proposed an image encryption strategy based on parallel compressive sensing. The logistic-tent system and 3D cat map are utilized to generate the measurement matrices.

Luo et al. [125] designed compression and encryption strategy for images based on compressive sensing and Haar wavelet. Ponuma and Amutha [126] utilized sparse coding and compressive sensing to encrypt the images. Sparse coding is utilized to discover the sparse representation of images as a straight combination of iotas from an overcomplete fixed dictionary. Song et al. [127] implemented an image encryption based on entropy coding and compressive sensing.

Han et al. [128] proposed a self-adaptive double-color image encryption approach. In this, each RGB color element of two input images is initially compressed and encrypted by 2D compressive sensing. The complex image is re-encrypted by self-adaptive random phase encoding and discrete fractional random transform (DFrRT) to get the final scrambled image. Zhang et al. [129] designed hybrid image compression and encryption approaches by exploring compressive sensing and Fibonacci-Lucas transform with the advantages of one-dimensional chaotic system. Pan et al. [130] utilized block compressive sensing to design an image encryption approach. The original image is separated into blocks and then each block is rendered sparse. The crisscross encryption strategy is utilized to encrypt pixel positions in all the blocks, and subsequently, dimension reduction is taken by compressive sensing. Table 7 demonstrates the comparison of various compressive sensing encryption approaches. It demonstrates that there is no such approach that has considered all the performance metrics.

Table 7: Comparison of various compressive sensing encryption approaches.

Ref.	HA	KA	IE	NA	NPCR	UACI	CA	PNSR	MSE
[114]	✗	✗	✓	✓	✓	✗	✓	✓	✓
[115]	✗	✗	✓	✗	✗	✓	✓	✓	✓
[116]	✗	✗	✓	✓	✗	✗	✓	✓	✗
[117]	✓	✓	✓	✓	✗	✗	✗	✓	✓
[118]	✗	✗	✓	✓	✓	✗	✓	✓	✗
[119]	✗	✗	✓	✓	✗	✓	✓	✗	✓
[120]	✗	✗	✗	✓	✗	✗	✓	✓	✓
[121]	✓	✓	✓	✓	✓	✓	✓	✓	✗
[123]	✓	✓	✓	✓	✓	✗	✗	✗	✗
[124]	✗	✗	✓	✓	✓	✓	✓	✓	✗
[125]	✗	✗	✓	✓	✗	✓	✓	✓	✗
[126]	✓	✓	✓	✓	✓	✗	✓	✓	✗
[127]	✗	✗	✗	✓	✓	✗	✗	✓	✗
[12]	✗	✗	✓	✓	✗	✓	✓	✓	✓
[128]	✗	✗	✗	✗	✓	✗	✓	✓	✓
[129]	✓	✓	✓	✗	✓	✓	✗	✗	✗
[130]	✗	✗	✓	✓	✗	✗	✗	✓	✗

3.3. Optical Image Encryption Approaches. Optical approaches are widely utilized in the field of cryptography due to its good computational speed and parallel processing. In this, a double random-phase encoding (DRPE) approach is utilized to convert the plain image into stationary white noise [131]. It uses two random phase masks that place in the input and Fourier plane. These random phase masks act as a key in DRPE. This method has been deeply researched and various optical encryption approaches have also been proposed [131].

Wu et al. [132] proposed a scalable asymmetric compressing and encrypting strategy for images by utilizing the nonlinear operation of phase truncation after cylindrical diffraction and discrete wavelet transform (DWT). Wu et al. [133] designed an asymmetric multiple-image encryption approach by utilizing compressed sensing and phase truncation. In this, a single ciphertext is attained by topsy-turvy operation of phase truncation after cylindrical diffraction. Yu et al. [134] implemented an image encryption approach depending on the hyperchaotic framework and the phase-truncated short-time fractional Fourier transform.

Wang et al. [135] implemented an image encryption based on phase-truncated Fresnel transform and random amplitude mask (RAM). Huang et al. [136] proposed a nonlinear optical multi-image encryption utilizing a chaotic map and 2D straight canonical transform. Wang et al. [137] increased the computational time and encryption capacity by reducing the number of iterations in image encryption with an improved amplitude-phase retrieval approach.

Mehra and Nishchal [138] implemented a gyrator wavelet transform by optical processing to encrypt an image depending on amplitude- and phase-truncation. The proposed approach consists of four basic factors: type and level of the mother wavelet, gyrator transform order, and position of different frequency bands. These factors are utilized as a secret key for image encryption. Sui et al. [139] designed a color image encryption approach by utilizing Yang-Gu mixture amplitude-phase retrieval approach and gyrator transform domain. A logistic map is utilized to generate the keys for encryption and decryption processes.

Wang et al. [137] designed an asymmetric optical image encryption approach by utilizing an improved amplitude-phase retrieval approach. In this, the public encryption key is generated by utilizing two random phases. To encrypt an input image into a ciphertext, an iterative amplitude and phase retrieval process are utilized. Verma and Sinha [140] proposed a nonlinear image encryption approach based on phase-truncated Fourier transform (PTFT) and natural logarithms. Liansheng et al. [141] developed an image encryption approach based on two random phases. It is free from an amplitude-phase recovery attack. Wang et al. [142] presented an encryption approach that abolishes the risk of information loss by utilizing phase-truncation approach. Table 8 demonstrates the comparison of various optical-based image encryption approaches. It demonstrates that there exists no such approach which has utilized all performance metrics.

3.4. Transform-Based Image Encryption Approaches. In transform-based image encryption approaches, the input image changed from spatial to frequency space by utilizing one of the transform domains. In most of the approaches, a color image is decomposed into three channels (i.e., R, G, and B channels). Each color channel is then encrypted through permutation and diffusion processes. The color channels can be independently processed or may be dependent on each other. After encrypting the channels, the final encrypted image is obtained by applying the inverse of transform. Some of the approaches based on the transform domain are discussed as follows.

Ran et al. [143] designed a solution for the information-independency problem in an image encryption by utilizing nonseparable fractional Fourier transform (NFrFT). Li et al. [144] implemented an encryption approach to encrypt multiple images based on cascaded FrFt. The input images are divided into two-phase masks. First phase mask is for secret key generation and second phase mask is for encrypting the images. Li and Lee [145] implemented an image encryption approach based on modified computational integral imaging reconstruction (CIIR) to solve the problem of occlusion in double-image encryption. But, the drawback of this method is transmission overhead in the network which is increasing. Chen et al. [146] designed double-image encryption by utilizing the gyrator transform (GT) and local pixel encrypting approach. It offers the clarification for crosstalk disorder found in phase-based images. In this approach, two images are combined to get complex functions.

Abuturab [147] utilized Hartley transform and GT to encrypt the images. Firstly, the Hartley transform is utilized to scramble the image, and then GT is applied to obtain the final encrypted image. Yao et al. [148] implemented an encrypted approach that encrypts the color images by deduced GT. The process of encryption involves Fourier and gyrator transform. Yaru and Jianhua [149] developed an image encryption approach by utilizing FrDCT via

Table 8: Comparison of various optical-based image encryption approaches.

Ref.	HA	KA	IE	NA	NPCR	UACI	CA	PSNR
[132]	✗	✗	✓	✗	✗	✗	✓	✓
[133]	✗	✗	✗	✗	✗	✗	✓	✓
[134]	✓	✓	✓	✓	✗	✗	✓	✗
[136]	✓	✓	✓	✗	✓	✗	✓	✗
[137]	✗	✗	✓	✗	✗	✓	✓	✗
[135]	✗	✗	✓	✗	✗	✓	✓	✗

polynomial interpolation (PI-FrDCT) and dependent scrambling and diffusion (DSD) process. Kanso and Ghebleh [150] utilized lift wavelet transform to make the encryption process visually secure. Mehra et al. [138] suggested the combination of wavelet transform and GT to guard the phase images. Lima et al. [151] designed medical image encryption by utilizing cosine number transform (CNT). It decomposes an image into blocks firstly. Afterward, CNT is applied sequentially to each block. Once image is processed, completely encrypted image is attained.

Luo et al. [152] implemented an integer wavelet transform- (IWT-) based image encryption approach. Initially, the original image is decomposed through IWT to obtain approximation and detailed coefficients. By spatiotemporal chaos, approximation coefficients are diffutilized. Afterward, by applying inverse IWT, the encrypted image is achieved.

Li et al. [153] designed an image encryption approach based on chaotic maps in the wavelet domain. Initially, plain image was decomposed by discrete wavelet transform and reconstructed the low-frequency modules. Afterward, Arnold cat map is utilized to make permutations. At last, the keystream in each diffusion process is generated by a robust chaotic map. Vaish et al. [154] evaluated an encryption approach for quantum images by utilizing quantum geometric transform, phase-shift transforms, and quantum Haar wavelet packet transform. Table 9 demonstrates the comparison of various transform domain-based image encryption approaches. It demonstrates that the development of transform-based image encryption approaches is still an open area of research.

Table 9: Comparison of various transform domain-based image encryption approaches.

Ref.	KA	NPCR	UACI	IE	CA	HA	PSNR	MSE	
[143]	✗	✗	✓	✓	✗	✓	✓	✗	✗
[144]	✗	✗	✓	✓	✗	✓	✓	✗	✗
[145]	✗	✗	✓	✗	✗	✓	✓	✗	✗
[149]	✗	✗	✓	✓	✗	✓	✓	✗	✗
[150]	✗	✗	✓	✓	✗	✓	✓	✗	✗
[151]	✓	✓	✓	✓	✓	✗	✓	✗	✗
[152]	✓	✓	✓	✓	✓	✗	✗	✗	✗
[153]	✓	✓	✓	✗	✗	✗	✗	✗	✗
[154]	✗	✗	✗	✗	✗	✗	✗	✓	✗

4. Future Scope

From the comprehensive review, it has been found that the existing image encryption approaches suffer from various issues. Also, there is still room for improvement in various fields of image encryption approaches. Therefore, in the near future, one may consider the following issues to continue the research in the field of image encryption.

(i) Application-specific approaches: the current research in the field of image encryption is not done towards the building of application-specific image encryption approaches. So, in the near future, the development of application-aware image encryption approaches is a hot area of research.

(ii) Compressive sensing: development of compressive sensing-based image encryption approaches can be improved further for lightweight devices such as mobiles, spy cameras, and surveillance cameras.

(iii) Hyperparameters tuning: hyperparameters tuning of key generators such as chaotic map can be achieved utilizing the recently developed metaheuristic approaches, machine learning [155], deep learning [156], deep belief networks, or deep-transfer learning [157, 158].

(iv) Parallel processing: due to rapid advancement in the various multimedia applications such as medical and satellite imaging. These applications require high-resolution images; therefore, the development of image encryption approaches for such applications will be computationally extensive. So, the parallel image encryption approaches can be utilized to handle this issue.

(v) Multidimensional multimedia data: development of encryption approaches for multimedia data such as multispectral images is still an undeveloped area. It is required to design high-dimensional hyperchaotic systems for such kind of multidimensional multimedia data.

(vi) Steganography/data hiding: the combination of encryption with reversible data hiding/steganography has become another research direction. Therefore, one may combine both encryption and steganography kind of approaches to obtain more secure results.

5. Conclusion

This paper presented a comprehensive study of the existing image encryption approaches. It was observed that the image encryption approaches require high confusion, zero correlation with the input images, less computational complexity, and high resistance to cryptanalysis process. The comparisons among the image encryption approaches were carried out based on evaluation parameters to show their strength and weaknesses. Future research directions related to image encryption strategies were examined. It was found that the development of image encryption approaches is still an open area for researchers. This paper encourages researchers to understand the challenges involved in image encryption approaches. It will also help them to choose an appropriate

approach to develop new encryption models according to an application which saves their time.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] Y. Xie, J. Yu, S. Guo, Q. Ding, and E. Wang, "Image encryption scheme with compressed sensing based on new three-dimensional chaotic system," *Entropy*, vol. 21, no. 9, p. 819, 2019.

[2] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Archives of Computational Methods in Engineering*, vol. 27, pp. 1–29, 2018.

[3] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[4] M. Kaur and V. Kumar, "Adaptive differential evolution-based lorenz chaotic system for image encryption," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 8127–8144, 2018.

[5] M. Kaur and V. Kumar, "Beta chaotic map based image encryption using genetic algorithm," *International Journal of Bifurcation and Chaos*, vol. 28, no. 11, Article ID 1850132, 2018.

[6] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5d chaotic map," *Future Generation Computer Systems*, vol. 107, pp. 333–350, 2020.

[7] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, 2013.

[8] C. Zhu, G. Wang, and K. Sun, "Improved cryptanalysis and enhancements of an image encryption scheme using combined 1d chaotic maps," *Entropy*, vol. 20, no. 11, p. 843, 2018.

[9] S. Zhu and C. Zhu, "Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map," *IEEE Access*, vol. 7, pp. 147106–147118, 2019.

[10] T. Sivakumar and R. Venkatesan, "A novel image encryption using calligraphy based scan method and random number," *KSII Transactions on Internet & Information Systems*, vol. 9, no. 6, 2015.

[11] H. Liu, B. Zhao, and L. Huang, "A novel quantum image encryption algorithm based on crossover operation and mutation operation," *Multimedia Tools and Applications*, vol. 78, no. 14, pp. 20465–20483, 2019.

[12] Y. Zhang, B. Xu, and N. Zhou, "A novel image compression-encryption hybrid algorithm based on the analysis sparse representation," *Optics Communications*, vol. 392, pp. 223–233, 2017.

[13] M. Kaur, D. Singh, and R. S. Uppal, "Parallel strength pareto evolutionary algorithm-ii based image encryption," *IET Image Processing*, vol. 14, no. 6, pp. 1015–1026, 2019.

[14] D. Singh and V. Kumar, "A comprehensive review of computational dehazing techniques," *Archives of Computational Methods in Engineering*, vol. 26, no. 5, pp. 1395–1413, 2019.

[15] A. Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, "Selective encryption for gray images based on chaos and dna complementary rules," *Multimedia Tools and Applications*, vol. 74, no. 13, pp. 4655–4677, 2015.

[16] E. Chen, L. Min, and G. Chen, "Discrete chaotic systems with one-line equilibria and their application to image encryption," *International Journal of Bifurcation and Chaos*, vol. 27, no. 3, Article ID 1750046, 2017.

[17] M. Kaur and V. Kumar, "Efficient image encryption method based on improved lorenz chaotic system," *Electronics Letters*, vol. 54, no. 9, pp. 562–564, 2018.

[18] J. Liu, S. Tang, J. Lian, Y. Ma, and X. Zhang, "A novel fourth order chaotic system and its algorithm for medical image encryption," *Multidimensional Systems and Signal Processing*, vol. 30, no. 4, pp. 1637–1657, 2019.

[19] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision," *Signal Processing*, vol. 168, Article ID 107340, 2020.

[20] K. Xuejing and G. Zihui, "A new color image encryption scheme based on dna encoding and spatiotemporal chaotic system," *Signal Processing: Image Communication*, vol. 80, Article ID 115670, 2020.

[21] X. Wang, Y. Wang, X. Zhu, and C. Luo, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level," *Optics and Lasers in Engineering*, vol. 125, Article ID 105851, 2020.

[22] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-ElYazeed, "A novel image encryption system merging fractional-order edge detection and generalized chaotic maps," *Signal Processing*, vol. 167, Article ID 107280, 2020.

[23] X. Wu, D. Wang, J. Kurths, and H. Kan, "A novel lossless color image encryption scheme using 2d dwt and 6d hyperchaotic system," *Information Sciences*, vol. 349-350, pp. 137–153, 2016.

[24] X.-L. Chai, Z.-H. Gan, Y. Lu, M.-H. Zhang, and Y.-R. Chen, "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system," *Chinese Physics B*, vol. 25, no. 10, Article ID 100503, 2016.

[25] Y. Luo, S. Tang, J. Liu, L. Cao, and S. Qiu, "Image encryption scheme by combining the hyper-chaotic system with quantum coding," *Optics and Lasers in Engineering*, vol. 124, Article ID 105836, 2020.

[26] K. A. Kumar Patro and B. Acharya, "An efficient colour image encryption scheme based on 1-d chaotic maps," *Journal of Information Security and Applications*, vol. 46, pp. 23–41, 2019.

[27] W. Feng, Y.-G. He, H.-M. Li, and C.-L. Li, "Image encryption algorithm based on discrete logarithm and memristive chaotic system," *The European Physical Journal Special Topics*, vol. 228, no. 10, pp. 1951–1967, 2019.

[28] X. Wang and S. Gao, "Application of matrix semi-tensor product in chaotic image encryption," *Journal of the Franklin Institute*, vol. 356, no. 18, pp. 11638–11667, 2019.

[29] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," *Information Sciences*, vol. 396, pp. 97–113, 2017.

[30] Z.-H. Gan, X.-L. Chai, D.-J. Han, and Y.-R. Chen, "A chaotic image encryption algorithm based on 3-d bit-plane permutation," *Neural Computing and Applications*, vol. 31, no. 11, pp. 7111–7130, 2019.

[31] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single s-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

[32] Z. Deng and S. Zhong, "A digital image encryption algorithm based on chaotic mapping," *Journal of Algorithms & Computational Technology*, vol. 13, 2019.

[33] K. A. K. Patro, B. Acharya, and V. Nath, "Various dimensional colour image encryption based on non-overlapping block-level diffusion operation," *Microsystem Technologies*, vol. 26, pp. 1–12, 2019.

[34] X. Wang, H. Zhao, L. Feng, X. Ye, and H. Zhang, "High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices," *Optics and Lasers in Engineering*, vol. 122, pp. 225–238, 2019.

[35] X. Ye, X. Wang, S. Gao, J. Mou, Z. Wang, and F. Yang, "A new chaotic circuit with multiple memristors and its application in image encryption," *Nonlinear Dynamics*, vol. 99, no. 2, pp. 1489–1506, 2020.

[36] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Optics and Lasers in Engineering*, vol. 84, pp. 26–36, 2016.

[37] W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Processing*, vol. 132, pp. 96–109, 2017.

[38] X. Chai, "An image encryption algorithm based on bit level brownian motion and new chaotic systems," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 1159–1175, 2017.

[39] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, "An image encryption scheme based on elliptic curve pseudo random and advanced encryption system," *Signal Processing*, vol. 141, pp. 217–227, 2017.

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

[41] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, pp. 391–402, 2019.

[42] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An image encryption method based on elliptic curve elgamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019.

[43] A. Banik, Z. Shamsi, and D. S. Laiphrakpam, "An encryption scheme for securing multiple medical images," *Journal of Information Security and Applications*, vol. 49, p. 102398, 2019.

[44] O. Reyad and Z. Kotulski, "Image encryption using Koblitz's encoding and new mapping method based on elliptic curve random number generator," in *Proceedings of the International Conference on Multimedia Communications, Services and Security Communications in Computer and Information Science*, pp. 34–45, Springer, Kraków, Poland, November 2015.

[45] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography," *Signal Processing*, vol. 125, pp. 187–202, 2016.

[46] X. Zhang and X. Wang, "Digital image encryption algorithm based on elliptic curve public cryptosystem," *IEEE Access*, vol. 6, pp. 70025–70034, 2018.

[47] D. S. Laiphrakpam and M. S. Khumanthem, "A robust image encryption scheme based on chaotic system and elliptic curve over finite field," *Multimedia Tools and Applications*, vol. 77, no. 7, pp. 8629–8652, 2018.

[48] Z. E. Dawahdeh, S. N. Yaakob, and R. Razif bin Othman, "A new image encryption technique combining elliptic curve cryptosystem with hill cipher," *Journal of King Saud University - Computer and Information Sciences*, vol. 30, no. 3, pp. 349–355, 2018.

[49] Z. Liu, T. Xia, and J. Wang, "Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes-Vanstone elliptic curve cryptosystem," *Chinese Physics B*, vol. 27, no. 3, Article ID 030502, 2018.

[50] S. Nagaraj, G. S. V. P. Raju, and K. K. Rao, "Image encryption using elliptic curve cryptograhy and matrix," *Procedia Computer Science*, vol. 48, pp. 276–281, 2015.

[51] B. Mondal, S. Singh, and P. Kumar, "A secure image encryption scheme based on cellular automata and chaotic skew tent map," *Journal of Information Security and Applications*, vol. 45, pp. 117–130, 2019.

[52] S. Khan, L. Han, H. Lu, K. K. Butt, G. Bachira, and N.-U. Khan, "A new hybrid image encryption algorithm based on 2D-CA, FSM-DNA rule generator, and FSBI," *IEEE Access*, vol. 7, pp. 81333–81350, 2019.

[53] W. Zhang, Z. Zhu, and H. Yu, "A symmetric image encryption algorithm based on a coupled logistic-Bernoulli map and cellular automata diffusion strategy," *Entropy*, vol. 21, no. 5, p. 504, 2019.

[54] Y. Su, Y. Wo, and G. Han, "Reversible cellular automata image encryption for similarity search," *Signal Processing: Image Communication*, vol. 72, pp. 134–147, 2019.

[55] M. T. Ramírez, M. Mejía Carlos, J. S. Murguía Ibarra, and L. J. Ontañón García Pimentel, "Partial image encryption using cellular automata," *Computación y Sistemas*, vol. 23, no. 4, 2019.

[56] Y. Wang, Y. Zhao, Q. Zhou, and Z. Lin, "Image encryption using partitioned cellular automata," *Neurocomputing*, vol. 275, pp. 1318–1332, 2018.

[57] A. Yaghouti Niyat, M. H. Moattar, and M. Niazi Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Optics and Lasers in Engineering*, vol. 90, pp. 225–237, 2017.

[58] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Processing: Image Communication*, vol. 52, pp. 6–19, 2017.

[59] R. Wei, X. Li, and Q.-H. Wang, "Double color image encryption scheme based on off-axis holography and maximum length cellular automata," *Optik*, vol. 145, pp. 407–417, 2017.

[60] T. Chen, M. Zhang, J. Wu, C. Yuen, and Y. Tong, "Image encryption and compression based on kronecker compressed sensing and elementary cellular automata scrambling," *Optics & Laser Technology*, vol. 84, pp. 118–133, 2016.

[61] A. Souyah and K. M. Faraoun, "An image encryption scheme combining chaos-memory cellular automata and weighted histogram," *Nonlinear Dynamics*, vol. 86, no. 1, pp. 639–653, 2016.

[62] D. Tralic and S. Grgic, "Robust image encryption based on balanced cellular automaton and pixel separation," *Radioengineering*, vol. 25, no. 3, pp. 548–555, 2016.

[63] Y.-G. Yang, J. Tian, H. Lei, Y.-H. Zhou, and W.-M. Shi, "Novel quantum image encryption using one-dimensional quantum cellular automata," *Information Sciences*, vol. 345, pp. 257–270, 2016.

[64] B. Murugan, A. G. Nanjappa Gounder, and S. Manohar, "A hybrid image encryption algorithm using chaos and Conway's game-of-life cellular automata," *Security and Communication Networks*, vol. 9, no. 7, pp. 634–651, 2016.

[65] A. Souyah and K. M. Faraoun, "Fast and efficient randomized encryption scheme for digital images based on quadtree

decomposition and reversible memory cellular automata," *Nonlinear Dynamics*, vol. 84, no. 2, pp. 715–732, 2016.

[66] R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, and I. F. Isnin, "A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata," *Optics and Lasers in Engineering*, vol. 71, pp. 33–41, 2015.

[67] S. Hanis and R. Amutha, "Double image compression and encryption scheme using logistic mapped convolution and cellular automata," *Multimedia Tools and Applications*, vol. 77, no. 6, pp. 6897–6912, 2018.

[68] X. Zhang, H. Zhang, and C. Xu, "Reverse iterative image encryption scheme using 8-layer cellular automata," *KSII Transactions on Internet & Information Systems*, vol. 10, no. 7, 2016.

[69] S. Zhou, B. Wang, X. Zheng, and C. Zhou, "An image encryption scheme based on DNA computing and cellular automata," *Discrete Dynamics in Nature and Society*, vol. 2016, Article ID 5408529, 9 pages, 2016.

[70] A. M. Del Rey and G. R. Sánchez, "An image encryption algorithm based on 3d cellular automata and chaotic maps," *International Journal of Modern Physics C*, vol. 26, no. 1, Article ID 1450069, 2015.

[71] M. N. Aslam, A. Belazi, S. Kharbech, M. Talha, and W. Xiang, "Fourth order mca and chaos-based image encryption scheme," *IEEE Access*, vol. 7, pp. 66395–66409, 2019.

[72] X. Li, Y. Wang, Q.-H. Wang, Y. Liu, and X. Zhou, "Modified integral imaging reconstruction and encryption using an improved sr reconstruction algorithm," *Optics and Lasers in Engineering*, vol. 112, pp. 162–169, 2019.

[73] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 88, pp. 197–213, 2017.

[74] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm sha-2," *Nonlinear Dynamics*, vol. 83, no. 3, pp. 1123–1136, 2016.

[75] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Applied Soft Computing*, vol. 37, pp. 24–39, 2015.

[76] B. Mondal and T. Mandal, "A light weight secure image encryption scheme based on chaos & DNA computing," *Journal of King Saud University - Computer and Information Sciences*, vol. 29, no. 4, pp. 499–504, 2017.

[77] X. Wu, K. Wang, X. Wang, and H. Kan, "Lossless chaotic color image cryptosystem based on DNA encryption and entropy," *Nonlinear Dynamics*, vol. 90, no. 2, pp. 855–875, 2017.

[78] X. Li, L. Wang, Y. Yan, and P. Liu, "An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems," *Optik*, vol. 127, no. 5, pp. 2558–2565, 2016.

[79] X.-Y. Wang, H.-L. Zhang, and X.-M. Bao, "Color image encryption scheme using cml and DNA sequence operations," *Biosystems*, vol. 144, pp. 18–26, 2016.

[80] H. Nematzadeh, R. Enayatifar, M. Yadollahi, M. Lee, and G. Jeong, "Binary search tree image encryption with DNA," *Optik*, vol. 202, p. 163505, 2020.

[81] A. Jain and N. Rajpal, "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps," *Multimedia Tools and Applications*, vol. 75, no. 10, pp. 5455–5472, 2016.

[82] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6229–6245, 2017.

[83] X. Zhang, Z. Zhou, and Y. Niu, "An image encryption method based on the Feistel network and dynamic DNA encoding," *IEEE Photonics Journal*, vol. 10, no. 4, pp. 1–14, 2018.

[84] X. Chai, Z. Gan, Y. Lu, Y. Chen, and D. Han, "A novel image encryption algorithm based on the chaotic system and DNA computing," *International Journal of Modern Physics C*, vol. 28, no. 5, Article ID 1750069, 2017.

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

[86] Y. Liu, J. Wang, J. Fan, and L. Gong, "Image encryption algorithm based on chaotic system and dynamic s-boxes composed of DNA sequences," *Multimedia Tools and Applications*, vol. 75, no. 8, pp. 4363–4382, 2016.

[87] B. Norouzi and S. Mirzakuchaki, "An image encryption algorithm based on DNA sequence operations and cellular neural network," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13681–13701, 2017.

[88] W. Liu, K. Sun, Y. He, and M. Yu, "Color image encryption using three-dimensional sine ICMIC modulation map and DNA sequence operations," *International Journal of Bifurcation and Chaos*, vol. 27, no. 11, Article ID 1750171, 2017.

[89] X. Zhang, F. Han, and Y. Niu, "Chaotic image encryption algorithm based on bit permutation and dynamic DNA encoding," *Computational Intelligence and Neuroscience*, vol. 2017, Article ID 6919675, 11 pages, 2017.

[90] H. R. Shakir, "A color-image encryption scheme using a 2D chaotic system and Dna coding," *Advances in Multimedia*, vol. 2019, 2019.

[91] S. Chirakkarottu and S. Mathew, "A novel encryption method for medical images using 2D Zaslavski map and DNA cryptography," *SN Applied Sciences*, vol. 2, no. 1, p. 1, 2020.

[92] M. Xu, "Cryptanalysis of an image encryption algorithm based on dna sequence operation and hyper-chaotic system," *3D Research*, vol. 8, no. 2, p. 15, 2017.

[93] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining dna coding and entropy," *Multimedia Tools and Applications*, vol. 75, no. 11, pp. 6303–6319, 2016.

[94] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image dna encryption using nca map-based cml and one-time keys," *Signal Processing*, vol. 148, pp. 272–287, 2018.

[95] X. Wu, J. Kurths, and H. Kan, "A robust and lossless dna encryption scheme for color images," *Multimedia Tools and Applications*, vol. 77, no. 10, pp. 12349–12376, 2018.

[96] S. Mozaffari, "Parallel image encryption with bitplane decomposition and genetic algorithm," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25799–25819, 2018.

[97] K. Shankar and P. Eswaran, "An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm," in *Artificial Intelligence and Evolutionary Computations in Engineering Systems, Advances in Intelligent Systems and Computing*, pp. 705–714, Springer, Berlin, Germany, 2016.

[98] M. Kaur and V. Kumar, "Colour image encryption technique using differential evolution in non-subsampled contourlet transform domain," *IET Image Processing*, vol. 12, no. 7, pp. 1273–1283, 2018.

[99] M. Kaur and V. Kumar, "Fourier-Mellin moment-based intertwining map for image encryption," *Modern Physics Letters B*, vol. 32, no. 9, Article ID 1850115, 2018.

[100] H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães, and V. N. Coelho, "Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices," *Optics and Lasers in Engineering*, vol. 110, pp. 24–32, 2018.

[101] N. K. Pareek and V. Patidar, "Medical image protection using genetic algorithm operations," *Soft Computing*, vol. 20, no. 2, pp. 763–772, 2016.

[102] K. Mirzaei Talarposhti and M. Khaki Jamei, "A secure image encryption method based on dynamic harmony search (dhs) combined with chaotic map," *Optics and Lasers in Engineering*, vol. 81, pp. 21–34, 2016.

[103] M. Kaur, V. Kumar, and L. Li, "Color image encryption approach based on memetic differential evolution," *Neural Computing and Applications*, vol. 31, no. 11, pp. 7975–7987, 2019.

[104] A. Gupta, D. Singh, and M. Kaur, "An efficient image encryption using non-dominated sorting genetic algorithm-iii based 4-d chaotic maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1309–1324, 2020.

[105] M. Mahmud, M. Atta-ur-Rahman, M. Lee, and J.-Y. Choi, "Evolutionary-based image encryption using rna codons truth table," *Optics & Laser Technology*, vol. 121, p. 105818, 2020.

[106] M. Kaur and V. Kumar, "Parallel non-dominated sorting genetic algorithm-ii-based image encryption technique," *The Imaging Science Journal*, vol. 66, no. 8, pp. 453–462, 2018.

[107] X.-L. Chai, Z.-H. Gan, Y. Lu, M.-H. Zhang, and Y.-R. Chen, "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system," *Chinese Physics B*, vol. 25, no. 10, p. 100503, 2016.

[108] J. Wang, "Digital image encryption algorithm design based on genetic hyperchaos," *International Journal of Optics*, vol. 2016, 2016.

[109] X. Wang and H.-l. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dynamics*, vol. 83, no. 1-2, pp. 333–346, 2016.

[110] X. Zhang, X. Wang, and Y. Cheng, "Image encryption based on a genetic algorithm and a chaotic system," *IEICE Transactions on Communications*, vol. E98.B, no. 5, pp. 824–833, 2015.

[111] R. Premkumar and S. Anand, "Secured and compound 3-d chaos image encryption using hybrid mutation and crossover operator," *Multimedia Tools and Applications*, vol. 78, no. 8, pp. 9577–9593, 2019.

[112] L. Wang, L. Li, J. Li, J. Li, B. B. Gupta, and X. Liu, "Compressive sensing of medical images with confidentially homomorphic aggregations," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1402–1409, 2018.

[113] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Optics & Laser Technology*, vol. 115, pp. 257–267, 2019.

[114] R. Ponuma and R. Amutha, "Encryption of image data using compressive sensing and chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 9, pp. 11857–11881, 2019.

[115] R. Ponuma, R. Amutha, S. Aparna, and G. Gopal, "Visually meaningful image encryption using data hiding and chaotic compressive sensing," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 25707–25729, 2019.

[116] W. Shao, M. Cheng, C. Luo et al., "An image encryption scheme based on hybrid electro-optic chaotic sources and compressive sensing," *IEEE Access*, vol. 7, pp. 156582–156591, 2019.

[117] L. Zhu, H. Song, X. Zhang, M. Yan, L. Zhang, and T. Yan, "A novel image encryption scheme based on nonuniform sampling in block compressive sensing," *IEEE Access*, vol. 7, pp. 22161–22174, 2019.

[118] Q. Shen, W. Liu, Y. Lin, and Y. Zhu, "Designing an image encryption scheme based on compressive sensing and nonuniform quantization for wireless visual sensor networks," *Sensors*, vol. 19, no. 14, p. 3081, 2019.

[119] H. Jiang, Z. Nie, N. Zhou, and W. Zhang, "Compressive-sensing-based double-image encryption algorithm combining double random phase encoding with josephus traversing operation," *Optica Applicata*, vol. 49, no. 3, 2019.

[120] S. Yao, L. Chen, and Y. Zhong, "An encryption system for color image based on compressive sensing," *Optics & Laser Technology*, vol. 120, p. 105703, 2019.

[121] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," *Optics and Lasers in Engineering*, vol. 121, pp. 203–214, 2019.

[122] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An optical image compression and encryption scheme based on compressive sensing and rsa algorithm," *Optics and Lasers in Engineering*, vol. 121, pp. 169–180, 2019.

[123] S. Zhu and C. Zhu, "A new image compression-encryption scheme based on compressive sensing and cyclic shift," *Multimedia Tools and Applications*, vol. 78, no. 15, pp. 20855–20875, 2019.

[124] H. Wang, D. Xiao, M. Li, Y. Xiang, and X. Li, "A visually secure image encryption scheme based on parallel compressive sensing," *Signal Processing*, vol. 155, pp. 218–232, 2019.

[125] Y. Luo, J. Lin, J. Liu et al., "A robust image encryption algorithm based on Chua's circuit and compressive sensing," *Signal Processing*, vol. 161, pp. 227–247, 2019.

[126] R. Ponuma and R. Amutha, "Image encryption using sparse coding and compressive sensing," *Multidimensional Systems and Signal Processing*, vol. 30, no. 4, pp. 1895–1909, 2019.

[127] Y. Song, Z. Zhu, W. Zhang, L. Guo, X. Yang, and H. Yu, "Joint image compression-encryption scheme using entropy coding and compressive sensing," *Nonlinear Dynamics*, vol. 95, no. 3, pp. 2235–2261, 2019.

[128] F. Han, X. Liao, B. Yang, and Y. Zhang, "A hybrid scheme for self-adaptive double color-image encryption," *Multimedia Tools and Applications*, vol. 77, no. 11, pp. 14285–14304, 2018.

[129] T. Zhang, S. Li, R. Ge, M. Yuan, and Y. Ma, "A novel 1d hybrid chaotic map-based image compression and encryption using compressed sensing and fibonacci-lucas transform," *Mathematical Problems in Engineering*, vol. 2016, 2016.

[130] C. Pan, G. Ye, X. Huang, and J. Zhou, "Novel meaningful image encryption based on block compressive sensing," *Security and Communication Networks*, vol. 2019, 2019.

[131] Y. Qin and Q. Gong, "Multiple-image encryption in an interference-based scheme by lateral shift multiplexing," *Optics Communications*, vol. 315, pp. 220–225, 2014.

[132] C. Wu, K.-Y. Hu, Y. Wang, J. Wang, and Q.-H. Wang, "Scalable asymmetric image encryption based on phase-

truncation in cylindrical diffraction domain," *Optics Communications*, vol. 448, pp. 26–32, 2019.

[133] C. Wu, Y. Wang, Y. Chen, J. Wang, and Q.-H. Wang, "Asymmetric encryption of multiple-image based on compressed sensing and phase-truncation in cylindrical diffraction domain," *Optics Communications*, vol. 431, pp. 203–209, 2019.

[134] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional fourier transform and hyper-chaotic system," *Optics and Lasers in Engineering*, vol. 124, p. 105816, 2020.

[135] W. Chen, "Optical multiple-image encryption using three-dimensional space," *IEEE Photonics Journal*, vol. 8, no. 2, pp. 1–8, 2016.

[136] Z.-J. Huang, S. Cheng, L.-H. Gong, and N.-R. Zhou, "Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform," *Optics and Lasers in Engineering*, vol. 124, p. 105821, 2020.

[137] Y. Wang, C. Quan, and C. J. Tay, "Asymmetric optical image encryption based on an improved amplitude-phase retrieval algorithm," *Optics and Lasers in Engineering*, vol. 78, pp. 8–16, 2016.

[138] I. Mehra and N. K. Nishchal, "Optical asymmetric image encryption using gyrator wavelet transform," *Optics Communications*, vol. 354, pp. 344–352, 2015.

[139] L. Sui, B. Liu, Q. Wang, Y. Li, and J. Liang, "Color image encryption by using yang-gu mixture amplitude-phase retrieval algorithm in gyrator transform domain and two-dimensional sine logistic modulation map," *Optics and Lasers in Engineering*, vol. 75, pp. 17–26, 2015.

[140] G. Verma and A. Sinha, "Optical image encryption system using nonlinear approach based on biometric authentication," *Journal of Modern Optics*, vol. 64, no. 13, pp. 1321–1329, 2017.

[141] S. Liansheng, Z. bei, W. Zhanmin, and S. qindong, "Amplitude-phase retrieval attack free image encryption based on two random masks and interference," *Optics and Lasers in Engineering*, vol. 86, pp. 1–10, 2016.

[142] Y. Wang, C. Quan, and C. J. Tay, "Optical color image encryption without information disclosure using phase-truncated fresnel transform and a random amplitude mask," *Optics Communications*, vol. 344, pp. 147–155, 2015.

[143] Q. Ran, L. Yuan, and T. Zhao, "Image encryption based on nonseparable fractional Fourier transform and chaotic map," *Optics Communications*, vol. 348, pp. 43–49, 2015.

[144] Y. Li, F. Zhang, Y. Li, and R. Tao, "Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform," *Optics and Lasers in Engineering*, vol. 72, pp. 18–25, 2015.

[145] X.-W. Li and I.-K. Lee, "Modified computational integral imaging-based double image encryption using fractional Fourier transform," *Optics and Lasers in Engineering*, vol. 66, pp. 112–121, 2015.

[146] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and H. Yu, "Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains," *Optics and Lasers in Engineering*, vol. 66, pp. 1–9, 2015.

[147] M. R. Abuturab, "An asymmetric single-channel color image encryption based on Hartley transform and gyrator transform," *Optics and Lasers in Engineering*, vol. 69, pp. 49–57, 2015.

[148] L. Yao, C. Yuan, J. Qiang, S. Feng, and S. Nie, "An asymmetric color image encryption method by using deduced gyrator transform," *Optics and Lasers in Engineering*, vol. 89, pp. 72–79, 2017.

[149] L. Yaru and W. Jianhua, "New image encryption combining fractional DCT via polynomial interpolation with dependent scrambling and diffusion," *The Journal of China Universities of Posts and Telecommunications*, vol. 22, no. 5, pp. 1–9, 2015.

[150] A. Kanso and M. Ghebleh, "An algorithm for encryption of secret images into meaningful images," *Optics and Lasers in Engineering*, vol. 90, pp. 196–208, 2017.

[151] J. B. Lima, F. Madeiro, and F. J. R. Sales, "Encryption of medical images based on the cosine number transform," *Signal Processing: Image Communication*, vol. 35, pp. 1–8, 2015.

[152] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 2, pp. 447–460, 2015.

[153] C.-L. Li, H.-M. Li, F.-D. Li, D.-Q. Wei, X.-B. Yang, and J. Zhang, "Multiple-image encryption by using robust chaotic map in wavelet transform domain," *Optik*, vol. 171, pp. 277–286, 2018.

[154] A. Vaish, S. Gautam, and M. Kumar, "A wavelet based approach for simultaneous compression and encryption of fused images," *Journal of King Saud University-Computer and Information Sciences*, vol. 31, no. 2, pp. 208–217, 2019.

[155] G. Qi, H. Wang, M. Haner, C. Weng, S. Chen, and Z. Zhu, "Convolutional neural network based detection and judgement of environmental obstacle in vehicle operation," *CAAI Transactions on Intelligence Technology*, vol. 4, no. 2, pp. 80–91, 2019.

[156] Y. Pathak, P. K. Shukla, A. Tiwari, S. Stalin, S. Singh, and P. K. Shukla, "Deep transfer learning based classification model for COVID-19 disease," *IRBM*, 2020.

[157] H. S. Basavegowda and G. Dagnew, "Deep learning approach for microarray cancer data classification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 22–33, 2020.

[158] Y. Tingting, W. Junqian, W. Lintai, and X. Yong, "Three-stage network for age estimation," *CAAI Transactions on Intelligence Technology*, vol. 4, no. 2, pp. 122–126, 2019.