Multimedia Tools and Applications (2023) 82:11155–11187
https://doi.org/10.1007/s11042-022-12791-6

1226: DEEP-PATTERNS EMOTION RECOGNITION IN THE WILD

A comprehensive survey on encryption techniques for digital images

Monu Singh [1] · Amit Kumar Singh [1]

Received: 19 November 2021 / Revised: 5 January 2022 / Accepted: 24 February 2022 /
Published online: 18 March 2022

Abstract
With the widespread adoption of smart devices and high-speed networks, investigators are focusing on securing digital image applications, such as those on social media, in healthcare, education, business and defence, from unauthorised use. The aim of this paper is to outline various encryption techniques, especially for digital images, and their merits and limitations. Along with the study, a brief overview, notable applications and evaluation metrics of encryption techniques are provided. Then, the contribution of surveyed techniques is also summarised and compared from different technical perspectives. Finally, the significant challenges are highlighted and a few directions of possible research are proposed that could fill gaps in these domains for researchers and developers.

Keywords Digital images · Encryption · Security · Attacks · Hashing

1 Introduction

The widespread adoption of smart devices and high-speed networks has made it convenient to share or upload digital images on websites and social media networks [55]. Furthermore, every hour, more than 81,60,000 photos are uploaded to Facebook [54], while another 38,66,400 photos are uploaded to Instagram [72]. Additionally, the number of images uploaded on Flickr during a very high-traffic day can reach 25 million [66]. However, these images may be downloaded and illegally shared without preserving the copyright and privacy of the content owner or producer. Encryption is one of the key techniques that has been established to secure digital images by transforming an original/plain image into a cipher image using a public or private key [26]. Recent applications of image encryption are depicted in Fig. 1 [20, 31, 53].

✉ Amit Kumar Singh
amit.singh@nitp.ac.in; amit_245singh@yahoo.com

Monu Singh
monus.phd20.cs@nitp.ac.in

[1] Department of Computer Science & Engineering, National Institute of Technology Patna, Patna, Bihar, India

Encryption can be performed in three different ways. One is symmetric encryption, for example, the Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES) and Blowfish, in which the same secret key is used by two parties for the complete process of encryption and decryption. The main limitation of such a type of encryption is key exchange [82]. Another method is asymmetric encryption, for example, the Digital Signature Algorithm, elliptic curve, Diffie–Hellman and Rivest–Shamir–Adleman (RSA) cryptosystem, where two different but mathematically related keys (public and private keys) are utilised [82]. The main limitation of such a type of encryption is the requirement of more processing power for computation [82]. Figure 2 demonstrates the general workflow of image encryption process.

Assume a plain image, 'P_i', and its ciphered image, denoted by 'C_i', the encryption and decryption process of an image are shown in Eqs. 1 and 2, respectively.

$$C_i = EA_{Key1}(P_i) \tag{1}$$

$$P_i = DA_{Key2}(C_i) \tag{2}$$

Where 'EA ()' and 'DA ()' are the encryption and decryption function, respectively. For the symmetric encryption key1 = key2. However, in case of asymmetric encryption, key1 ≠ key2.

Hashing is another encryption technique that is used to maintain the integrity of an image [43]. A one-way hash function is applied on input data (variable length), which produces a message digest of a unique size independent of the size of the input data. A successful hash function is one that cannot be reversed, does not reveal any information about the input and produces the same message digest for the same input. Using the hashing technique, one can verify the integrity of the received message. The main limitation of such a type of encryption is a collision of hash values. The cryptographic hash function is given in Eq. (3):

$$M_D = H_f(I_M) \tag{3}$$

Where M_D= Hash value or message digest (fixed length), H_f = Cryptographic hash function, and I_M = Input message (variable length).

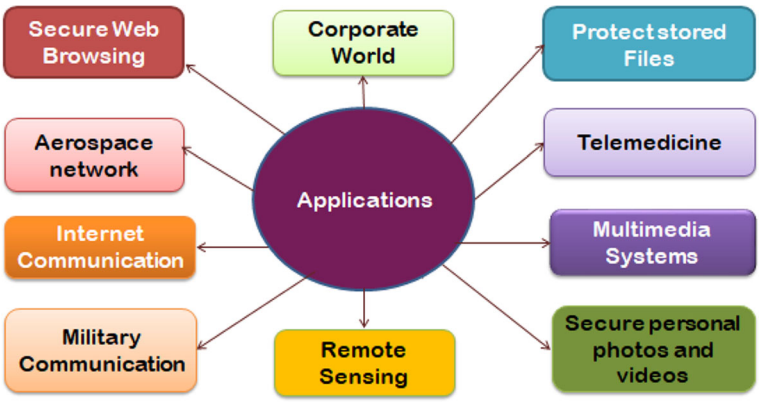

Fig. 1 Recent applications of image encryption

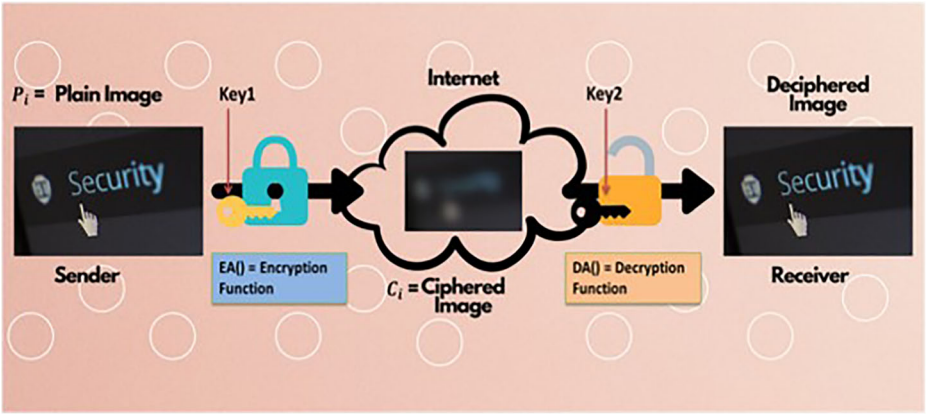

Fig. 2 General workflow of image encryption process

Researchers developed various encryption techniques that use symmetric [4–7, 11, 13, 17–19, 22–24, 26, 32, 38, 39, 44, 45, 47, 49, 50, 52, 55, 58, 59, 69, 74, 79–81, 83, 87, 89], asymmetric [2, 8, 15, 16, 25, 34, 36, 37, 41, 42, 70, 78, 88], hashing [9, 14, 33, 48, 51, 61, 63, 64, 67, 71, 76, 86, 91] and other techniques [1, 3, 10, 12, 20, 21, 29–31, 35, 40, 46, 56, 57, 60, 62, 65, 68, 73, 75, 77, 84, 90] to resolve the security and other equally important issues related to the digital images.

Therefore, this article aims to provide a comprehensive review of current studies related to images and analysis of encryption methods, their merits and limitations. Along with the study, a brief overview, notable applications and evaluation metrics of encryption techniques are provided. Then, the contribution of surveyed techniques is also summarised and compared in different technical perspectives. Finally, we highlight the significant challenges along with a few directions for possible research that could fill the gaps in these domains for researchers and developers.

The rest of the paper is arranged as follows. Various common attacks on images in the domain of encryption and related performance metrics are discussed in Section 2. Section 3 describes the methodologies that comprise the literature corpus. Significant challenges and a few directions of possible research are discussed in Section 4. Finally, Section 5 provides some final remarks and future perspectives related to our survey.

2 Common attacks and related performance evaluation metric

This section outlines the possible attacks on images in the domain of encryption and related metrics [27, 28, 85] to evaluate the performance of any encryption scheme, as shown in Fig. 3. Furthermore, quick summaries of all these measures are given in Table 1.

- **Differential attack:** This is used to analyse the sensitivity of an encryption method to small changes in the original image. The attacker makes a small modification to the plain image and then the same encryption method is used to encode the image before and after modification to find the relationship between the new plain image and the cipher image.
- **Statistical attack:** This attack is carried out to check the statistical resemblance between the encoded and plain images. A histogram and correlation coefficient are used for this analysis.
- **Brute-force attack**: All possible combinations of keys are attempted to crack the secret key used for encryption until it is attained.

- **Ciphertext-only attack:** In this attack, only some sets of ciphertexts are known to cryptanalysts, who then try to decrypt ciphertext to have access to the secret key or plaintext.
- **Noise attack:** Here, the attacker tries to insert noise into an encrypted image to destroy the usable information of the plain image. This makes it impossible for the intended user to recover the original image after the decryption procedure.

3 Encryption approaches for digital images

Several image encryption approaches have been introduced using symmetric, asymmetric and hashing schemes. In the following subsection, we elaborate on different image encryption approaches, including a comparison of the discussed technique in tabular form.

3.1 Symmetric encryption-based approaches

In [4], the author developed an image encryption scheme that aimed to achieve higher security via pixel permutation using a chaotic map. The method uses pixel permutation to obtain the normalised image. Next, a key is obtained from the normalised image and the new matrix of the same size as the original image is created and initialised by the key. Finally, the combination of the normalized and newly created images is utilised to obtain the encrypted image. Simulation results suggested that the proposed method is secure for a chosen-plaintext attack. Although the method outperforms the Arnold technique, security analysis of the scheme needs to be investigated for other attacks. Additionally, complexity analysis of any encryption method is also very significant for practical applications and needs to be investigated for the suggested method.

Kamal et al. [26] proposed an encryption scheme for health images, which has four main steps: first, the digital image is split into image blocks. Second, these image blocks are scrambled. Then, in the third step, random permutation is carried out to achieve confusion. A key is also generated in the third stage based on a logistic map, which is utilised in the final

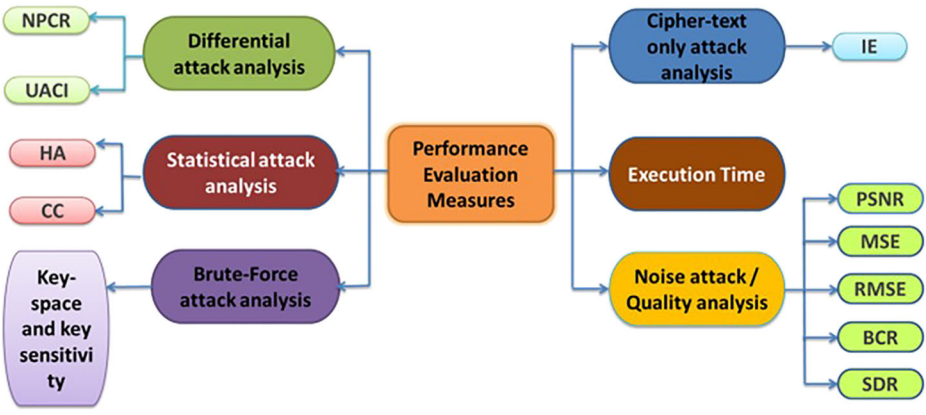

Fig. 3 Common attacks and related performance evaluation metric

Table 1 Summary of common attacks and related performance metric

S. no.	Common Attacks/ Vulnerabilities	Evaluation metric	Formula	Description
1	Differential attack	i) Number of Pixel Change Rate (NPCR)	$NPCR = \frac{\sum_{i,j} D(i,j)}{W^{\times} \times H} \times 100\%$ Where W & H are width and height of image respectively, $D(i,j) = \begin{cases} 1, C1(i,j) \neq C2(i,j) \\ 0, otherwise \end{cases}$ Where C1 and C2 are ciphered image before and after alteration of pixel.	• It measures the change rate of pixel numbers of encrypted image if only a single pixel is changed in plain image. • NPCR value should be close to 100.
		ii) Unified Average Changing Intensity (UACI)	$UACI = \frac{\sum_{i,j} E(i,j) - E'(i,j)}{255^{\times} \times W^{\times} \times H} \times 100$ Where E(i, j) and E'(i, j) are the ciphered images of plain image and modified image respectively.	• It asses the average intensity difference between the ciphered images of plain image and modified image (by one bit) • UACI value should be close to 33.
2	Statistical attack	i) Histogram Analysis (HA)		• It discloses the approximate representation of distribution of image pixel values. • Plain image and cipher image both should have completely different histograms. • It exhibits non-uniform nature in case of plain-image and but it should be uniform for encrypted image
		ii) Correlation Coefficient Analysis(CC)	$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}^{\times} \times \sqrt{D(y)}}$ *Where* $\frac{C(x,y) = \sum_{i=1}^{K} (x_i - E(x))(y_i - E(y))}{K}$ $D(x) = \frac{1}{k} \sum_{i=1}^{K} (x_i - E(x))^2$ $D(y) = \frac{1}{k} \sum_{i=1}^{K} (y_i - E(y))^2$ where x, y=Adjacent pixels of an image C(x, y)=covariance between samples x and y K=number of pixel pairs (x_i, y_i) D(x) and D(y)=standard deviation of x and y E(x)=mean of x_i pixel values.	• It is used to correlate the corresponding pixels of ciphered image and the plain image • Adjacent pixels in plain image are highly correlated in vertical, horizontal and diagonal directions. • Encrypted image should have minimum correlated pixels • Its value should be near to 0.
3	Noise attack	i) Peak Signal to Noise Ratio (PSNR)	$PSNR = 10^{\times} \times log_{10} \frac{(2^n - 1)^2}{MSE}$ Where n=no. of bits per pixel	• It is used to measure the quality of encrypted image. • It will be measured in Decibel (dB) • Its range is {0, ∞} • A good encryption scheme should have max. PSNR value
		ii) Mean Squared Error (MSE)	$MSE = \frac{1}{WH} \sum_{x=1}^{x=W} \sum_{y=1}^{y=H} (P(x,y) - E(x,y)^2$	• It measures the error between plain image and ciphered image

Table 1 (continued)

S. no.	Common Attacks/ Vulnerabilities	Evaluation metric	Formula	Description
			Where (x, y)=pixel coordinates of image W × H=width and height of image P and E=plain and encrypted images	• Its range is {0, ∞} • It is reciprocal of PSNR • Its value should be maximum b/w encrypted and original image.
		iii) Root Mean Squared Error (RMSE)	$RMSE = \sqrt{\frac{\sum_{x=1}^{x=W}\sum_{y=1}^{y=H}(P(x,y)-E(x,y)^2}{W^{\times}\times H}}$ Where (x, y)=pixel coordinates of image W × H=width and height of image P and E=plain and encrypted images	• It provides more accurate and precise data by calculating the root of mean squared error (MSE) • Its range is {0, ∞}
		iv) Bit Correct Ratio (BCR)	$BCR = \left(1-\frac{\sum_{x=0,y=0}^{MxN} O(x,y)\oplus D\ (x,y)}{M^{\times}\times N}\right)^{\times}\times 100\%$ Where x, y=Pixel coordinates M × N=Height and width of image O=original image D=Decrypted image	• The difference between a plain image and decrypted image is calculated using BCR. • It validates the decrypted image's validity.
		v) Signal to Distortion Ratio (SDR)	$SDR = 10log_{10}\frac{\sum_{x,y} O(x,y)^2}{\sum_{x,y}(O(x,y)-D(x,y))^2}$ Where x, y=Pixel coordinates M × N=Height and width of image O=original image D=Decrypted image	• SDR is calculated between the original image and decrypted image pixel values to assess the quality. • It is measured in decibel (dB). • Large value of SDR is desirable.
4	Brute force attack	Key space (KS) and Key sensitivity		• It should be large enough to prevent brute force attack and it should be very sensitive to change.
5	Cipher-text only attack	Information Entropy (IE)	$H(S) = -\sum_{s}(P(S_i)^{\times}\times \log_2 P(S_i))$ Where, H (S)=entropy of message source (S) $P(S_i)$=probability of occurrence of S_i	• It measures the unpredictability of details available in image. • Its range is {0, 8}. For grey scale image, entropy values should be close to 8.
6	NA	Execution Time (ET)		• ET means the total time taken by an encryption scheme to encrypt an image. • The value of ET should be low. • It is measured in milliseconds (ms), Seconds (s) or minutes (m).

stage to change the value of image pixels. Hence, a scrambled image is diffused in the last stage. The receiver applies the decryption process to obtain the original image. Simulation results suggested that this method is robust against common attacks. However, its performance needs to be investigated further in terms of encryption speed.

Ibrahim et al. [23] developed a method for encrypting medical images using key-dependent S-boxes and chaotic maps. The proposed method works in two phases. The first phase is the preparation phase, which generates two nonces. A dynamic S-box (S) is prepared based on a generated nonce. A chaos initialisation vector is used to produce the byte stream. The S-box and produced byte stream are utilised to encrypt the source image in the second phase, i.e. the development phase. To additionally facilitate the decryption process, two nonces are kept in the cipher image header. Simulation results showed that higher values of throughput and sensitivity result in a more efficient encryption method. However, its performance needs to be analysed against other equally important attacks. Furthermore, the encryption time is highly dependent on the image size.

A cryptosystem for securing images based on a colour byte scrambling technique and logistic and Ikeda maps is proposed by Parvees et al. [55]. The logistic map generates a permutation sequence that causes confusion. The Ikeda map is used to create diffusion by creating masking sequences from a 24-bit colour image. The scheme is secured against many attacks, but its performance needs to be analysed further in terms of encryption speed.

Somaraj and Hussain [69] proposed an encryption scheme for colour images using red, green and blue (RGB) pixel displacement and scrambling. In this scheme, an original image is first split into three RGB components. Another image of the same size is used as a key, and the key image is split down into RGB components. Afterwards, an XOR operation is performed on selected bit planes of the original image and RGB components of the key image. Then, the resultant image is scrambled to obtain the encrypted image. Simulation results suggested that the proposed scheme is safe against statistical attacks. Security analysis of the proposed scheme needs to be further conducted for other attacks.

Liu and Miao [39] suggested a 1D chaotic map to ensure the security of encrypted images. 1D chaotic maps are easy to implement and have acceptable chaotic characteristics, but they are prone to attacks because of their limited control parameters, non-uniformly distributed sequences and small key space. To generate the chaotic sequences, this encryption technique uses the aforementioned map. Then, it carries out the shuffling and substitution on the plain image using these iterative sequences to obtain the ciphered image. The algorithm shows good security performance, but its encryption speed needs to be investigated. According to the simulation findings, this method has a wide key space and is resistant to brute-force attacks. Furthermore, it is extremely sensitive to both key and plain images. As a result, this method is not vulnerable to differential attacks. However, its computational complexity should be explored further since, aside from security, it is an important characteristic for an effective encryption technique.

Prasetyo [59] designed an encryption algorithm using a simple chaotic number approach. Image encryption is achieved by first applying the confusion technique and then the pixel values are changed by chaotic keys. According to the simulation results, the proposed scheme is able to resist statistical and differential attacks. However, its performance needs to be investigated further for other attacks.

Diab [17] introduced a cryptosystem based on simultaneous permutation and diffusion. Here, a key stream is generated first using a Chebyshev chaotic map to mix the image pixels in horizontal and vertical directions. After that, a modified logistic map is exploited to generate

the diffusion key and dynamic pixel order, which are used to simultaneously permute and change the pixels of image. The simulation results show that this approach performs well against common attacks. Further investigation is required on computational complexity and other possible attacks.

In [87], image-ciphering employing bit-level pixel permutation and diffusion architecture was presented. Here, the original image is decomposed into multiple distinct components by pixel columns. As a result, several groups are formed depending on the number of bits in a pixel. Then, permutation is applied on each group by employing Arnold's cat map. Later, a permuted image is diffused using a non-adjacent coupled map lattice. Finally, to achieve higher security, permutation and diffusion phases are encrypted in several rounds. The suggested cryptosystem has a decent key space and key sensitivity for brute-force attack resistance. However, this method has a high computational cost due to its multiple rounds and also requires additional hardware and specialised circuits.

In [19], a simple, fast and robust cryptosystem based on chaos was presented. It uses a bit-permutation layer to change the locations of image pixels along with the diffusion layer. A modified 2D cat map is employed for permutation, instead of the original 2D cat map, to achieve a better performance. Here, the author claims that in the single iteration of bit-permutation, it provides superior sensitivity to a single bit change in the original image and the secret key. This claim is examined by Noura et al. [52], who found that this cipher can be compromised by a chosen-plaintext/ciphertext attack. Furthermore, it also requires additional memory space, which limits its application to devices with limited resources.

Noura et al. [52], evaluated the NCIES cipher's [19] performance and found that it can be compromised by a chosen-plaintext/ciphertext attack. A lightweight encryption method is suggested to overcome the problems identified in the NCIES cipher. It is based on round function, a p-box and S-boxes. There are two primary levels in this scheme. First, the round function is repeated twice, which is enough to ensure that the avalanche effect is maintained at the block level. This round function itself consists of three basic operations: the addition of a round key, substitution and diffusion. Finally, to find the encryption copy, the block permutation procedure is used to randomise the serial order of blocks. The proposed scheme overcomes the limitations of the NCIES cipher. In addition, the randomness and error propagation test results show that this method is resistant to noise and statistical attacks. Its performance needs to be analysed further in terms of encryption speed.

Zhang et al. [89] proposed a spatiotemporal chaotic system-based scheme. To set the initial states and parameters of chaotic maps, the original image and an external key are utilised. A pseudo-random number generator is used to produce random numbers. This algorithm is made up of two processes: substitution and diffusion. A circular S-box is used in the substitution process, and a key stream buffer is used in the diffusion process to encipher the pixels of the image. The proposed scheme is computationally fast and secure for statistical, differential and brute-force attacks. However, security analysis of this approach needs to be investigated further for other attacks, such as noise and data loss. Furthermore, the results need to be investigated further since chaotic maps are vulnerable to known/chosen-plaintext attacks [32].

In [13], Author designed an encryption scheme for grey scale medical images using a discrete wavelet transform (DWT). To minimise the correlation and redundancy in image pixels, a DWT property is first exploited. Afterwards, the image is decomposed into subparts, and random permutation is applied on subimages, which are used to generate the subkeys for each part using entropy and the arithmetic mean. Then, the full image is composed, and again, the random permutation, along with the encryption key (64-bit), is employed to achieve

confusion and diffusion. This scheme is simple and provides good encryption speed, but its performance needs to be analysed further, as the author has not discussed its security strength, key space and key sensitivity in depth. Moreover, some research has proven that the permutation-based techniques are vulnerable to ciphertext and known-plaintext attacks [11].

Ashtiyani and Birgani [5] designed an encryption scheme based on Arnold's cat map and simplified-AES (S-AES). Arnold's cat map is utilised for scrambling the locations of image pixels, and S-AES is used for substitution. In S-AES, a chaotic S-box is used for better security of the proposed design. Based on the simulation findings, this scheme appears to have good encryption speed. However, because the histogram of the enciphered image is non-uniform, this method might be vulnerable to statistical attacks. Furthermore, its performance needs to be analysed for other attacks.

A cryptosystem [58] based on chaotic compressing sensing was proposed by Ponuma and Amutha to achieve simultaneous compression and encryption by generating a sparse representation of an input image using DWT. Then, by using measurement and a masking matrix, the sparse coefficients are compressively scrambled and encrypted simultaneously. These two matrices are generated by employing a logistic map and a new proposed 1D chaotic map. This parallel compressive sensing architecture improves the performance of the proposed scheme. Further investigation is needed in terms of security analysis, as some research [22] has proved that sequences created by a logistic map are insecure and vulnerable to attacks.

In [7], the suggested cryptosystem uses chaotic coupled maps in addition to a single chaotic map. The plain image is first converted into a matrix. Then, this matrix is encrypted using the results of the chaotic coupled map iteration and the chaotic map. The coupled map is iterated using the starting condition and control parameters of the coupled map. Later, the chaotic map is created using a function of the new initial condition. The chaotic map is then iterated once again to generate the ciphered image. The suggested scheme is secure against common attacks. However, its complexity needs to be analysed further. Moreover, security analysis needs to be conducted on it for other attacks.

Tedmori and Al-Najdawi [74] designed a lossless image encryption based on a discrete cosine transform (DCT). In this method, the original image is transformed from spatial domain to a frequency domain using block-based DCT. Low and high frequencies are handled in such a way that they are secure and unbreakable. The encryption process then includes dispersing the recognisable discrete cosine value across the other frequencies using a reversible weighting factor. The proposed scheme is designed to scramble and invert the sign of each frequency in the transformed block. Simulation results suggested that this approach can withstand a noise attack. The given analysis is inadequate to employ it for secure applications. Further investigation is required for analysis of its security and encryption speed. In addition, DCT is a lossy technique, whereas authors claimed that it a lossless technique. A simple encryption algorithm using a logistic map and DNA is proposed by Mondal and Mandal [45]. Here, two random numbers are randomly generated for different purposes. The permuted image is first converted to a DNA sequence, then, it is encrypted using DNA computation, and finally, each pixel is XORed with a previous pixel. As the computational overhead is less in the case of a logistic map, and DNA computation is also undertaken on a bit level, the proposed scheme is lightweight. To address the limitations of the logistic map, a cross-coupled logistic map is used for generating a pseudo number. This scheme is fast and robust against common attacks. However, robustness analysis against some equally important attacks still needs to be investigated.

To overcome the weakness of traditional permutation and diffusion architecture (PDA) [79], Ye [83] designed a pixel-level encryption technique using a two-dimensional Sine Logistic modulation map (2D-SLMM). The separation attack found in the traditional PDA is removed using permutation–rewriting–diffusion architecture. It provides double diffusion to improve the security. Keys generated for the confusion and diffusion process are able to resist different attacks. The proposed scheme is safe against brute-force, statistical and differential attacks, but its performance need to be analysed further against noise and data loss attacks.

Jarin et al. [24] used self-adaptive permutation and DNA encoding to propose an image encryption technique. In this scheme, DNA encoding is applied to transform a plain image into a DNA sequence. Both a linear feedback shift register and chaotic map are employed to generate the key stream. Then, the addition operation and key stream are utilised to mask the encoded image. Afterwards, the DNA complement rule is employed. To obtain the final encrypted image, self-adaptive permutation is exploited on the previously encoded image. The suggested technique resists statistical attacks but seems vulnerable to brute-force attacks due to the small key space.

Munir [47] proposed an encryption scheme based on chaotic permutation. First, the plain image is scrambled by an Arnold map. Then, it is divided into different blocks. After splitting, DCT is employed on each block. Arnold's cat map is employed again to permute the AC coefficients. Finally, an inverse operation of DCT is employed on each block to create an encrypted image. Simulation results show that the quality of the ciphered image is not of the required standard. It is also not applicable when each pixel of an image is important, such as in healthcare systems, because DCT transformation is lossy.

Yang [80] proposed a cryptosystem using the Fractional Fourier transform (FFT) to remove the limitations of using DCT transformation. Here, a scrambling matrix is obtained by a logistic map to adapt the plain image with a sine chaotic map. Then, FFT provides a function for the phase mask. This function also utilises a logistic map. This scheme resists brute-force, statistical and differential attacks, but its performance needs to be analysed further for ciphered image quality.

To protect information [44], Mokhtar et al. proposed a method using a different chaotic algorithm. In this work, a plain image is divided into blocks and then distinct chaotic maps are applied in five different phases. First, the cubic map is used to permute the pixels that make up the blocks. Second, the permuted pixels are diffused using the Henon map. Third, the blocks are permuted using a quadratic map. Fourth, to permute all of the pixels, a logistic map is utilised. Finally, the permuted picture is diffused using the XOR Henon map to produce an encrypted image. Simulation results showed that the proposed scheme outperforms noise, statistical and differential attacks. However, the complexity of the suggested method needs to be investigated since there are so many rounds in each phase.

The method suggested by Duseja and Deshmukh [18] not only enhances the randomness of an encrypted image but also compresses it, making it easier to store and send. This scheme is based on a hash map and the Chinese remainder theorem. Participants are given secret co-prime keys that are generated and distributed via a hash map. This achieves compression and encryption by solving various distinct congruent equations, which are then utilised to simultaneously encrypt and compress numerous image pixels. This scheme requires prime modulus values, otherwise we may not be able to find a unique solution, and every co-prime integer's value must be larger than 255. There is a requirement for an efficient method to store huge quantities.

Yang and Liao [81] proposed a secure and efficient symmetric encryption scheme for colour images using a generalised logistic map. Most of the encryption schemes utilise chaotic systems, which work on a real domain. As a result, there is a significant disadvantage in terms of practical applicability. The authors expand the chaotic logistic map to the finite field in this work to successfully solve this problem. Across the finite field, there exists an automorphic mapping between two logistic maps with distinct control parameters. Furthermore, the automorphic mapping sequences are employed for encrypting colour images. A random sequence produced by a logistic map over a finite field is used to encrypt the plain image. Then, the resultant ciphered image is again encrypted by using the random sequence produced by automorphic logistic mapping to obtain the ciphered image. Simulation results showed that the proposed scheme is highly sensitive to change and offers a good encryption speed. However, its performance needs to be analysed against other equally important attacks.

A fast and secure cryptosystem [49] proposed by Nkandeu and Tiedeu is based on a 1D chaotic map and substitution technique. Here, a chaotic map is produced by mixing Gaussian, logistic, May and Gompertz maps to overcome the major limitations of a simple 1D chaotic map, such as inadequate sensitivity and poor randomness [6, 38]. This encryption scheme employs three stages: first, the plain image substitution method is performed on a plain image for enhancing sensitivity. Second, S-boxes are generated using a pseudo-random number sequence (PRNS) produced by a chaotic system. Third, a scrambling-masking approach is adopted, which employs S-boxes to diffuse and permute image pixels in a single operation. Simulation results showed that the proposed scheme is fast and safe against statistical, differential and chosen plain/cipher image attacks. However, its performance needs to be analysed further against noise and data loss attacks.

Nkandeu et al. [50] mixed the outputs of logistic, Sin and Gampertz maps to establish better chaotic properties and PRNS. An encryption method with diffusion-permutation architecture has been developed. The generated PRNS and plain image are both used to derive the encryption keys for the diffusion and permutation process. The diffusion procedure occurred in multiple distinct block arrays of pixels of the plain image and in CBC mode with pixel shuffling, in a synchronised manner. Simulation results suggested that this scheme is faster than that proposed in [49]. Furthermore, it has the ability to stand against statistical, differential and chosen-plain/cipher image attacks. However, its performance needs be investigated further for other common attacks, such as noise and occlusion.

The contribution made by symmetric encryption based approaches is summarised and compared in Table 2.

3.2 Asymmetric encryption-based approaches

An efficient asymmetric encryption scheme is proposed by Jiao and Ye [25] based on RSA and generalised Arnold's map. The initial parameters for Arnold's map are constructed using RSA and iteratively generate a key stream. Three different layers are applied to hide the image data. The first layer of hiding is completed by XOR diffusion on a plain image. In the second layer, to hide the data again, the rows and columns of the image are confused cyclically. To apply a third layer of hiding, additive mode diffusion is used. After this the final cipher image is generated. However, the suggested scheme is secure for statistical, differential and ciphertext-only attacks. Its performance needs to be investigated further for other common attacks and encryption speed.

Table 2 Summary of symmetric encryption based approaches

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attacks considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	Robustness	Histogram		
[4]	To develop a secure encryption scheme for digital images	Pixel permutation and Chaotic map	Y	Y	Infinite	N	N	N	N	Sample Images	Brute-force and chosen-plaintext attack
[26]	To develop a robust encryption algorithm for Medicare systems	Confusion, diffusion and logistic map	Y	Y	10^{35}	O(M×N) where M x N= Size of plain image	Y	Y	Y	Breast Cancer Histopathological, Dermatolsogy, RITE and the Stanford Volume Data Archive	Brute-force attack, statistical,- differential attacks and noise attacks
[23]	To design a new efficient encryption framework for medical data	Dynamic S-boxes and Chaotic Maps	Y	Y	2^{106}	$O(T_N + n)$, where T_N is the chaotic transient length and n is the image size	Y	N	Y	Sample medical images	Brute-force, chosen-ciphertext and chosen plain-text attack
[55]	To design a secure encryption technique for color images	Color byte scrambling, Logistic Map and Ikeda Map	Y	Y	10^{224}	N	Y	Y	Y	Benchmark Waterloo image set	Most of the cryptographic attacks
[69]	To present a method for protecting color images during transmission	RGB pixel displacement and scrambling	N	N	N	N	N	N	Y	USC-SIPI image database	Statistical attacks
[39]	To suggest a 1D Chaotic map for ensuring security of encrypted images	1D chaotic map, shuffling and substitution	Y	N	2^{277}	N	Y	N	Y	Sample images	Brute-force attack and statistical and differential attacks
[59]	To present an efficient image encryption scheme for digital images	Diffusion, confusion and chaotic number	Y	N	N	N	Y	N	Y	USC-SIPI image database	Statistical and differential attack
[17]	To design an cipher which can resist common attacks	Chebyshev-Chebyshev map, modified Logistic map, simultaneous	Y	Y	2^{243}	N	Y	Y	Y	Standard grey scale images	Most of the cryptographic attacks

Table 2 (continued)

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attacks considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	Robustness	Histogram		
		permutation and diffusion									
[87]	To propose an efficient image cryptosystem	Bit-level pixel permutation, non-adjacent coupled map lattices, diffusion	Y	N	2^{400}	(100 x M x N)	N	N	Y	Standard grey image of Lena	Brute-force, statistical and differential attack
[19]	To develop a fast and robust image encryption system	Diffusion, block cipher, permutation and modified 2D-cat map	Y	N	2^{163}	41.87 ms for encrypting an image of size 1024×1024	N	Y	Y	Standard sample images	Brute-force, plaintext sensitivity, key sensitivity, statistical and differential attacks
[52]	To develop an efficient, lightweight and dynamic image encryption scheme for real time applications	S-Box, P-Box and round function	N	Y	512 bits	O(h) where h=block size	Y	N	Y	Sample image	Brute-force, statistical and noise attacks
[89]	To propose a fast and secure image encryption algorithm	S-Box, diffusion, Key stream buffer, logistic map and PWLCM	Y	N	2^{280}	19.5686 ms for encrypting an image of size 1024×1024	N	N	Y	Standard test images	Brute-force, plaintext sensitivity, key sensitivity, statistical and differential attacks
[13]	To design a cryptosystem for grey scale medical images	DWT, and Permutation, symmetric encryption	N	N	64-bit key is used	N	N	N	Y	Sample image	Statistical attacks
[5]	To develop an encryption scheme for securing medical images	Scrambling, diffusion, S-AES and CAT map	Y	Y	2^{128}	N	Y	N	Y	Sample image	Brute-force, statistical, differential and noise attacks
[58]	To present a cryptosystem which jointly	DWT, Scrambling, logistic map and 1D Chaotic map	Y	Y	$>2^{236}$	0.66 s for encrypting an image of size 256×256	Y	Y	Y	Standard sample images	Brute-force, noise, cropping, known-plaintext,

Table 2 (continued)

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attacks considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	Robustness	Histogram		
	perform compression and encryption on image data										chosen plaintext and statistical attacks
[7]	To propose a novel fast image encryption scheme	Chaotic system and cycle shift at bit-level	Y	N	Initial parameters of chaotic map	2.12 s for encrypting image of size 1024×1024	Y	N	Y	Sample image	Brute-force, statistical and differential attacks
[74]	To develop a lossless image encryption algorithm	Discrete cosine transform (DCT)	N	Y	N	N	N	N	N	USC-SIPI image database	Noise attack
[45]	To propose a light weight image encryption scheme	DNA, cross-coupled logistic map	Y	N	2^{133}	*O(n)*	Y	N	Y	Sample grey images	Brute-force, statistical and differential attacks
[83]	To develop an efficient pixel-level image encryption scheme	TD-SLMM, substitution and permutation	Y	N	10^{56}	0.836165 s for encrypting image of size 1024×1024	Y	N	Y	Standard images	Most of the cryptographic attacks
[24]	To present a secure encryption technique for digital images	DNA encoding, ID chaotic map, Linear feedback shift register and self-adaptive permutation	N	N	N	N	Y	N	Y	Sample images	Statistical attacks and ciphertext only attack
[47]	To propose an encryption scheme which provides good quality cipher	Chaotic permutation, DCT, Arnold cat map	N	Y	N	N	N	Y	N	Sample images	Noise attacks
[80]	To develop a chaotic map and utilize it for providing more secure encryption algorithm	Logistic map, Fractional Fourier transform and sine chaotic map	N	Y	10^{87}	N	N	N	Y	Sample images	Exhaustive attack, plaintext and statistical attack
[44]			Y	Y	N	N	Y	Y	N	Sample image	

Table 2 (continued)

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attacks considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	Robustness	Histogram		
	To design a secure cryptosystem for digital images	Cubic map, Hannon map, Quadratic map, Logistic Map, permutation and diffusion									Statistical, differential and noise attacks
[18]	To propose an algorithm which jointly perform encryption and compression of grey scale images	Chinese Remainder Theorem (CRT) and hash map	N	Y	2^{244} if block size is 8 and co-prime key is of 32 bit	$O(\frac{n^2}{r} + \sum_{i=1}^{r} \log(cpi))$	N	Y	Y	Sample Images	Brute-force, statistical and noise attacks
[81]	To produce a secure and efficient encryption scheme for color images	Logistic map over finite field Z_N	Y	Y	2^{256}	0.8193 s for encrypting acolor image of size 512×512	Y	Y	Y	Sample images	Brute-force, statistical, differential and noise attacks
[49]	To design a fast and secure cryptosystem for grey and color images	S-Box and 1D seed Map (obtained by mixing Logistic, Sin, Gaussian and Gompertz map)	Y	N	2^{475}	2.100 s for encrypting a color image of size 512×512	Y	N	Y	Sample images	Brute-force. Statistical, differential, chosen plain image and chosen cipher image attacks
[50]	To develop an encryption scheme which is fast and reinforce security in real-time operations	Parallel diffusion, CBC mode, 1D seed Map (obtained by mixing Logistic, Sin and Gampertz map)	Y	N	2^{400}	983 ms for encrypting a color image of size 512×512	Y	N	Y	Sample images	Brute-force. Statistical, differential, chosen plain image and chosen cipher image attacks

To satisfy the security needs during the transmission of medical data, Ali and Ali [2] proposed a signcryption scheme based on public-key cryptography equipped with an elliptic curve. In this method, an elliptic curve and chaotic maps are used for signcryption and encryption of the image, respectively. This provides a method of digital signature, key exchange and chaotic map image encryption. This scheme has integrity, authentication, confidentiality and non-repudiation, whereas chaos-based encryption is verified against performance matrices. However, the decrypted image is suitable, but its computational cost is very high, and it is not suitable for Internet of Things devices, which are resource constrained.

Lin and Li [36] proposed an effective encryption algorithm based on an RSA algorithm and hyperchaotic system. An RSA algorithm is used to generate the initial values for a hyperchaotic system, which is responsible for producing a key stream iteratively. Several rounds are performed to hide the image data. Additive mode diffusion is employed twice to change the positions and values of pixels of the image. To again hide the image data, a diffusion image matrix is transformed to a 1D image matrix. In the third round of hiding the image data, a finite field diffusion process is employed. Finally, the encrypted image is obtained. Simulation results revealed that this method is secure against statistical, differential and chosen-plaintext/ciphertext attacks. This method, however, is susceptible to noise and data loss attacks.

In [41], to overcome the limitations of symmetric image encryption, i.e. key management and distribution, an asymmetric image encryption approach based on elliptic curve ElGamal and chaotic theory is suggested by Luo et al. In this work, the secure hash algorithm (SHA)-512 is utilised to produce the chaotic system's starting values, and the plain image is scrambled using a crossover permutation. Furthermore, the scrambled image is incorporated inside the elliptic curve. Finally, the diffusion coupled chaos game using a DNA sequence is performed to obtain the cipher image. However, the suggested algorithm is robust against different possible attacks. It takes longer to compute, making it inappropriate for real-time applications.

In [37], Liu and Kadir proposed an asymmetric colour image encryption technique based on a 2D discrete-time map. Here, the encryption process starts with calculating the hash value of a plain image using SHA-256. The initial values of the Hanon map are then created using this hash value. Then, the pixels of the image are circularly shifted by row and column using the random sequences generated by the Hanon map. Finally, using the XOR operation, three colour components (RGB) of the scrambled image are diffused. Overall, the proposed scheme is safe against common attacks. Its encryption complexity needs to be investigated. Furthermore, it resists noise and data loss to a limited level.

Benssalah et al. [8] introduced an improved image encryption scheme to fix the flaws found in [15]. This scheme is based on improved elliptic-curves cryptography with a Hill cipher. In this, communicating parties first generate their private keys and self-invertible matrices (Km). The image obtained after applying Arnold's cat map on the plain image is then multiplied with self-invertible matrices. The resultant matrix obtained after multiplication is then XORed with a hyperchaotic Lorenz to produce a ciphered image. Simulation results suggested that the proposed scheme is robust against common attacks. However, its time complexity is increased due to modifications by elliptic-curve cryptography (ECC). Moreover, compared to the methods proposed in [16, 34], its encryption speed is slower.

Wu et al. [78] developed an eight-dimensional generalised chaos synchronisation (8D-GCS) system using a 4D chaotic system, which meets all the requirements specified for a new chaotic system [70]. Based on this proposed generalised chaos synchronisation (GCS) system, an encryption approach for colour images is developed. In this work, a diffeomorphism

function is used to generate the parameters for transfer function. This transfer function and the 4D chaotic system are utilised to develop an 8D-GCS system. Then, a chaotic sequence is produced by this GCS system. This chaotic sequence and plain image are fused together to obtain the cipher image (48-bit RGB colour image) along with a data validation tag, which is used to validate the data at the receiver end. If verifications fail, the receiver will stop the decryption process. Simulation results revealed that this work is highly sensitive to both the plain image and the key. However, its time complexity needs to be investigated.

An efficient asymmetric encryption scheme [88] is proposed based on ECC, which offers a similar level of authentication to that provided by RSA with a smaller key [42]. Initially, to reduce the encryption time, pixels of a plain image are grouped together to generated large integers. A piece-wise linear chaotic map (PWLCM) is utilised to produce the chaotic sequence. Furthermore, the XOR operation is carried out on plain image pixels using the public key and chaotic big integers, which produce an encrypted big integer. Afterwards, the ciphered image is obtained by recovering the pixels' values from the encrypted big integer. The simulation result suggested that the proposed scheme has good anti-attack capabilities. Furthermore, its encryption speed is also good. However, its performance needs to be investigated further in terms of quality of recovered image.

The contribution made by asymmetric encryption based approaches is summarised and compared in Table 3.

3.3 Hashing-based approaches

In this work [71], Sreelakshmi and Ravi designed an encryption algorithm for colour images based on bidirectional diffusion. The encryption process begins by separating the RGB components of the input image and then splitting them into small blocks. Encryption keys are generated using SHA-256. The following operations are employed on each block, one after another, to obtain the cipher image: scrambling, rotation, inversion, negative-to-positive transformation, integration and forward and reverse diffusion. In each operation completed on a block, a different key is used. Simulation results suggested that this method is safe against brute-force, statistical and differential attacks. However, the security analysis of the scheme needs to be investigated for other attacks, such as noise and data loss attacks.

To overcome the limitation of the 'one-time pad' (OTP) encryption scheme and resist a chosen-plaintext attack, Zhu et al. [91] proposed an encryption scheme using chaos theory and SHA-256. It consists of three main parts: adding pseudo-random sequences (PRS) around the image, image scrambling and image diffusion. The hash value obtained from the plain image is converted into an integer in the [0,255] range and then this number is added around the image instead of using it as a part of the key in the encryption process. Only the initial values of chaotic systems are used as a key in the encryption process, which overcomes the problem of key management of an OTP. The random number sequence in scrambling and diffusion processes is dependent on intermediate ciphertext. Simulation results revealed that the suggested work is highly secure against a chosen-plaintext attack. However, its encryption speed needs to be investigated further.

Chai et al. [9] suggested an encryption approach for grey images based on chaos and a DNA sequence. In this algorithm, the key via SHA-256 is generated first and then DNA encoding, along with the key (hash value), is utilised to create a DNA matrix. On this DNA matrix, DNA-level wave-based permutation is conducted using the random number sequence generated by a logistic map. The characteristics of the wave transmission are exploited to

Table 3 Summary of asymmetric encryption based approaches

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attacks considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	Robustness	Histogram		
[25]	To design an asymmetric encryption scheme with good anti-attack capabilities	RSA, Generalized Arnold Map, confusion and diffusion technology	Y	N	Key is developed by RSA	2.227410 s in one round for encrypting image of size 1024× 1024	Y	N	Y	USC-SIPI and Kodak databases	Brute- force, statistical, differential and ciphertext only attacks
[2]	To develop a novel encryption scheme for secure transmission of medical data	Public Key cryptography, elliptic curve and chaotic maps	Y	Y	2^{299}	**scrambling:** 4MN+ 3MNlog2(MN) **Diffusion:** 10MN where M x N= size of image	Y	Y	Y	open-access medical image repositories/-Ayland.orgimage database	Brute force, statistical, differential, noise and data loss attacks
[36]	To develop an encryption technique for grey scale images	RSA and Lorenz Hyper chaotic System	Y	N	2.56 X 10^{59}	0.269177 s for encrypting image of size 512×512	Y	N	Y	USC-SIPI database	Most of the cryptographic attacks
[41]	To develop a robust and secure digital image encryption scheme	EC-ELGamal, SHA-512, LTM and TSM	Y	Y	2^{564}	4.73389 for encrypting image of size 512×512	Y	Y	Y	Standard images	Most of the cryptographic attacks
[37]	To develop an encryption scheme for secure transmission of color images	2D discrete-time map, Hanon map, SHA-256 and circular shift function	Y	N	10^{58}	N	Y	Y	Y	Sample color images	Brute-force, Statistical, differential, noise and cropping attacks
[8]	To develop a secure medical image encryption scheme for TMIS	IECCHC, Arnold cat map, and hyper chaotic Lorenz	Y	Y	2^{256}	2 s (K_m=4×4) and 2.3 s (K_m=8×8)	Y	Y	Y	Set of grey-scale and DICOM images	Brute-force, Statistical, differential, occlusion and noise attacks
[78]	To design an image encryption algorithm for secure communication of color images	4D chaotic system, 8D GCS system and diffeomorphism function	Y	N	2^{1249}	N	Y	N	Y	Sample images	Most of the cryptographic attacks
[88]	To develop an efficient asymmetric image encryption scheme to protect the content of digital images	PWLCM, SHA-256, ECC-256 and ECC-512	Y	Y	2^{256} or 2^{512}	0.91 m using ECC-256 and 0.61 m using ECC-512	Y	N	Y	Sample images	Brute-force, statistical, differential, noise and known plaintext attacks

create this wave-based permutation at the DNA level. The chaotic map is utilised to produce a key matrix, which is then used to alter the components of the confused DNA matrix. After that, by making use of decoding rules, the diffused DNA matrix is decoded to produce the cipher image. However, the proposed algorithm is fruitful against most security attacks and highly sensitive to secret keys and plain images. Its performance needs to be analysed further in terms of encryption speed.

Dagdu et al. [14] suggested a cryptosystem based on di-chaotic diffusion for medical images. This method utilised two chaotic maps, a PWLCM and Bernoulli shift map, to generate two encryption keys matrices. Two rounds of diffusion are carried out using these matrices to produce an encrypted image via a bitwise XOR operation. A message-digest algorithm (MD5) is utilised to generate the initial values of the PWLCM from the semi-ciphered image obtained after the first round of diffusion. The proposed technique is efficient to resist differential and statistical attacks. However, this scheme has low sensitivity to the input image, as the initial value and parameters of the Bernoulli shift map are independent of the original image. Therefore, it may be vulnerable to chosen-plaintext/ciphertext attacks. Furthermore, security analysis of this scheme needs to be investigated for other attacks.

Rao and Suma [63] proposed a security scheme for securing images and keys. It is also able to detect the modifications in an image being transmitted. Initially, the input image is converted into a string by passing it through a Base64 encoder. SHA-256 is applied on the key to generate a secret key. Then, the secret key and string generated from the input image are given to the AES algorithm to produce an encrypted image. To protect the secret key from an attacker, it is transformed into an image by using the American Standard Code for Information Exchange's encoding scheme. Then visual cryptography is utilised to split the encoded image into two shares. The hash value is calculated by applying MD5 to the ciphertext. The image splits, ciphertext and generated hash value are required to share for the decryption process. Using this scheme, modifications in the image being transmitted can be detected. For an efficient encryption algorithm, security analysis and complexity parameters are also equally important. Therefore, the performance of this algorithm needs to be analysed further.

Ying and Zhang [48] applied modified Josephus traversing the image scramble (row and column-wise), and they considered the pixel permutation and diffusion to encrypt the image. Specifically, SHA-3 is applied to the original image to obtain the binary sequence. Subsequently, a chaotic system in terms of a piecewise linear chaotic map and the hyperchaotic Chen system, along with the diffusion process, are used to encrypt the image. The simulation results showed that the scheme is secure against plaintext and differential attacks. However, the major drawback of this scheme is high computational complexity.

To overcome the shortcomings of classic Baptista algorithms [33, 64], Wang et al. [76] offer an encryption scheme based on SHA-1 and MD5. The initial parameters for the logistic map and PWLCM are obtained using hash functions. To employ scrambling, the authors utilised two logistic maps to produce chaotic coordinates and coupled them with nonlinear equations. Then, diffusion was achieved by applying an upgraded Baptista system and a cyclic-shift function to the scrambled image. The proposed scheme is robust against common attacks. However, for a good encryption algorithm and security, speed is also an important factor. Therefore, its encryption speed needs to be optimised to make it suitable for real-time application.

Zefreh [86] introduced an efficient encryption scheme based on the hash function, chaotic system and DNA operations. To ensure sensitivity to the plain image and key, a combined SHA-256 and MD5 method is applied on the plain image with an external key. SHA-256 is

more secure than MD5 when it comes to collision attacks [61]. Both the permutation and diffusion are carried out at the DNA level. Permutation at the DNA level is achieved by employing a function based on the logistic map. Several DNA operators are employed to achieve diffusion of the permutated image with the key DNA image. However, the scheme is robust against different common attacks and fast enough for grayscale images. It can be further investigated for colour images, too.

In [67], based on SHA-2(512) and an S-box of AES, an encryption algorithm for grayscale and colour images has been designed by Seyedzade et al. The fundamental idea behind this work is to utilise one half of the image to encrypt the other half in a reciprocal manner. This algorithm is divided into two sections: the first performs a pre-processing procedure to shuffle half of the image using an S-box. The hash function SHA-2(512) is used to produce a random no. mask. Then, the image is divided into subimages. The information from the bottom half of the subimage and the random no. mask are then used to encrypt the upper portion of the subimage. In the same way, the information from the upper portion will be used to encrypt the bottom half. The proposed scheme is secure for statistical and brute-force attacks. However, security analysis needs to be conducted for other attacks. Furthermore, its complexity also needs to be analysed.

Norouzi et al. [51] proposed an encryption algorithm aimed at achieving a high security and sensitivity to the key by introducing a hash function (Salsa20) and high complexity by utilising only two iterations of the diffusion process. This hash function generates a secret key based on an external key chosen by the user. Then, the plain image is horizontally segmented into an array in the first round of the diffusion process. After that, it is XORed with the binary sequence produced by the hash function. The identical procedure is performed vertically on the transpose of the array produced in the subsequent round. The simulation results suggested that this method has good anti-attack capabilities. However, its performance needs to be analysed further in terms of time complexity for larger images and for colour images, too.

The contribution made by hashing based approaches is summarised and compared in Table 4.

3.4 Other prospective approaches

The work proposed by Lakshami et al. [31] fully utilised the discrete Hopfield attractor's learning capabilities for encrypting grey images without introducing chaos. This encryption scheme consists of four stages. In the first stage, an adaptive key is created based on a plain image. The second stage is responsible for producing a random sequence. Permutation and substitution are performed in the third and fourth stages, respectively, by incorporating random sequences generated using a Hopfield attractor. The simulation results suggested that the scheme is robust against common attacks and has good encryption speed. Furthermore, a higher throughput, entropy and sensitivity value indicate that the encryption technique is more efficient. However, its encryption speed needs to be analysed against images of a larger size.

Faragallah et al. [20] implemented an efficient colour image encryption technique for cybersecurity applications using RC6 and various operation modes. The encryption process begins by reading and extracting the RGB components of a colour image with some details. Each RGB component is divided into 128-bit blocks, which are then encrypted by RC6 using the different operating modes. The encoded RGB components are then built by assembling the respective ciphertext blocks of RGB components. Then, the resulting RGB components are finally put together to obtain the ciphered image. The simulation results revealed that the

Table 4 Summary of hashing based approaches

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attacks considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	Robustness	Histogram		
[71]	To provide a secure encryption technique for color images	Bidirectional diffusion, scrambling, rotation, inversion, transformation, integration and SHA-256	Y	Y	256-bit keys	N	N	N	Y	Some standard images	Statistical and Differential attacks
[91]	To develop an efficient image encryption scheme for grey scale images	SHA-256, diffusion, scrambling, hyper-chaotic system and Chebyshev maps	Y	N	2^{339}	3.11 s for encrypting image of size 1024 X1024	Y	Y	Y	Some standard images	Most of the cryptographic attacks
[9]	To introduce an highly sensitive and secure encryption algorithm for grey scale images	DNA sequence operation, 2D logistic map and SHA-256, Hamming distance	Y	Y	5.46 10^{80}	(M N)	Y	Y	Y	Some standard images	Most of the cryptographic attacks
[14]	To present a fruitful cryptosystem for medical images	Piecewise linear chaotic map, Bernoulli shift map and MD5	Y	N	Initial parame-ters of chaotic system	0.6239 s and 2.3002 s for encrypting image of size 256×256 and 512×512 respectively	Y	N	Y	Sample grey images	Statistical and differential attacks
[63]	To present a novel image encryption scheme to maintain integrity of digital images	AES, Visual cryptography and MD-5	N	N	N	N	N	N	Y	Standard images	Tempering / mod-ification
[48]	To develop a novel image encryption scheme for digital images	PWLCM, SHA-3(383), and Josephus traversing	Y	Y	383- bit key	1.268 s for encrypting image of size 256×256	Y	Y	Y	Standard images	Most of the cryptographic attacks
[76]	To provide a secure encryption scheme by improving the deficiencies of Baptista algorithm	SHA1, MD5, cyclic-shift function & PWLCM	Y	N	2^{186}	1.172 s for encrypting image of size 256×256	Y	Y	Y	Standard images	Brute-force, statistical, differential, noise and occlusion attack
[86]			Y	Y	2^{512}		Y	Y	Y		

Table 4 (continued)

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attacks considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	Robustness	Histogram		
	To present a secure and fast grey scale image encryption scheme	SHA-256, MD5, logistic map and DNA operations				3.3594 s for image of size 1024×1024				Sample images	Brute-force, Statistical, Differential and noise attack
[67]	To develop a secure, high speed cryptosystem for grey and color images	SHA-2(512), S-box of AES, permutation and diffusion	N	N	2^{128}	N	N	N	Y	USC-SIPI image database	Statistical attack and brute-force attacks
[51]	To introduce a highly sensitive, complex and secure image encryption algorithm for grey scale images	Salsa20 hash function and diffusion	Y	Y	2^{512}	0.41 s for encryption grey image of size 256×256	Y	Y	Y	Standard images	Most of the cryptographic attacks

proposed cryptosystem with the CBC, CFB and OFB operating modes effectively hides all information inside the examined colour images. However, the findings also indicated that using the ECB mode is not recommended. Moreover, its time complexity needs to be investigated.

Based on cellular automata and an S-box, Contreras et al. [12] designed a cipher scheme. In this, the authors extended the pre-processing function suggested by Ramirez-Torres et al. [62] to break the strong correlation between the plain image and its ciphered image. This work begins by selecting a block (24-bits) of the original image. Then, the proposed extended processing function is employed on this block. This pre-processed block is further divided into eight-bit blocks, and the value of each block is replaced using a substitution box. Subsequently, each coordinate's complement can be computed to invert the rows and columns of the pre-processed image in such a way that the pixel, (n, n), occupies the position formerly occupied by the pixel, (0, 0). Finally, the extended pre-processing function is applied once more to the transformed image. The suggested scheme can protect against statistical and differential attacks, but it should be further analysed for other security parameters, too.

In [90], Zhang et al. proposed a multi-image encryption scheme to enhance the transmission speed while taking care of security based on the image hash, dynamic DNA coding and bit-plane decomposition. First, the hash value of multiple grey images is obtained. Then, the multiple images are divided onto a bit plane. To increase the key space and produce a highly unsure chaotic sequence, an enhanced 4D-hyper chaotic system and 3D-chaotic mapping are utilised by the authors. The initial values of these chaotic maps are based on the generated hash value. This chaotic sequence is utilised to replace pixels in the images decomposed on the bit-plane, resulting in a merged image. After that, DNA coding is run on merged images, along with the chaotic sequence. Then DNA calculations are conducted on the generated coding matrix using the operation rules of the chaotic sequence. DNA decoding is performed on the matrix produced after DNA computation. The final encrypted image is obtained when the DNA-decoded binary image is transformed to a decimal. The proposed approach is secure and may be used to detect image tampering. However, this method has high computational complexity.

To provide a secure transmission of digital images, Wang et al. [75] proposed a scheme based on Arnold's cat map and laser chaos synchronisation. In this method, a parameter is produced to impact the secret key based on the original image's pixel values. Then, the plain image is transformed using the reshape function. Later, the transformed image is diffused using an XOR operation. Finally, the general Arnold transformation scrambles the pixels' positions in the diffused image. Simulation results revealed that this method is secured against statistical and noise attacks. Security analysis of this approach needs to be investigated further for other common attacks. Moreover, its computational complexity depends on the image's size.

Li et al. [35] proposed an encryption scheme for medical images based on zigzag confusion and dynamic diffusion. In this approach, PRS are generated using a 2D-SLMM and a two-dimensional Henon-Sine map. The 2D-SLMM was created by Hua et al. [21] to overcome the limitations of a 1D chaotic map. The PRS are utilised to produce the cat mapping coefficient matrix. The plain image is first scrambled by employing a zigzag scan. Furthermore, an improved 2D cat map, along with the PRS, is employed on the scrambled image to carry out the diffusion process. The password feedback mechanism and chaotic iteration are added in the diffusion process to improve the relationship between the key and the password. The simulation results showed that the proposed scheme is lossless and also able to resist common

attacks. However, to make it suitable for real-time applications, its encryption speed needs to be improved.

A fast and robust image encryption scheme is introduced by Yepdia et al. [84] based on the mixing technique. This approach fundamentally consists of three stages. Two are permutation stages, while one is a mixing stage. First, the plain image is divided into multiple equal-sized subimages. The May Gompertz map is used to undertake a block permutation on the subimages. After that, the PWLCM is utilised to perform the pixel-based transposition. The output of the two prior permutations is split into four subimages. Furthermore, these subimages are combined using pseudo-random matrices created from the above two maps to get the ciphered image. This method can be used to encrypt a single image or multiple images, too. The simulation results show that this approach is appropriate for images that are sensitive to noise propagation, such as those used by the military and in medical fields. Further investigation is required on security analysis of this scheme, as low-dimensional chaotic maps are weak in providing security [3].

In [40], a secure image encryption mechanism is provided by Loukhaoukha et al. based on the Rubik's cube principle. Initially, the plain image pixels are scrambled using the Rubik's cube concept. Then, this scrambled image is XORed using two different random secret keys. The proposed scheme is simple and robust against common attacks. Alongside security, the execution speed is also an essential factor in the design of image encryption methods, especially for real-time applications. Therefore, its computational complexity needs to be improved.

In this work [57], the authors aimed to present a fast and secure chaotic map-based multiple grayscale image encryption method. Both equal and unequal-sized images can be encrypted using this scheme, unlike other existing methods, which necessitate the use of identical-sized images [30, 56, 68]. Here, a set of given images is split into non-intersecting blocks. The produced blocks and any leftover pixels (if any) are then separated into different arrays. After that, permutation and diffusion are carried out using a distinct PWLCM system, which makes this algorithm effective for both hardware and software platforms and secure, too. A PWLCM system utilises SHA-256 to produce initial iteration values to resist known/chosen-plaintext attacks. The simulation results suggested that the proposed cryptosystem is secure against most common attacks. However, the performance of this method needs to be analysed further to establish its effectiveness against other attacks and its speed of encryption.

In [46], the authors presented an encryption method based on genetic operators and a hybrid pseudo-random number generator (HPRNG). This proposed HPRNG is based on a linear-feedback shift register (LFSR) and uses a chaotic asymmetric-tent map and logistic map to produce the LFSR's initial vector. Initially, with the aid of a PRS produced by an HPRNG, the first block of the original image is encrypted. Later, the preceding encrypted block and XOR operations are used to create subsequent blocks. This method may also be used to encrypt text and colour images. The simulation results suggested that the proposed technique is lightweight and suitable to resist common attacks. Its computational complexity is too high, which needs to be improved to make it suitable for real-time applications.

To reduce energy consumption, time and space complexity, an encryption scheme based on 2D-Von-Neumann cellular automata was suggested by Roy et al. [65]. It uses 2D-cellular automata rule vectors (2D-CARVS) with a GCA property to achieve encryption by pixel substitution. First, the RGB components of an input image are extracted and transformed into binary matrices. Then, a rule scheduler is applied to choose three cellular automata rule vectors (CARVs) randomly from the 2D-CARV list. Then, these chosen CARVs are used to encrypt

Table 5 Summary of some more encryption based approaches

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attacks considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	Robustness	Histogram		
[31]	To develop an attack resistant image encryption algorithm for grey images	discrete Hopfield attractor, substitution and permutation	Y	N	10^{112}	0.251 s for encrypting a grey image of size 256×256	Y	Y	Y	Sample images	Most of the cryptographic attacks
[20]	To develop an efficient color image encryption scheme for cybersecurity application	RC6, CBC, ECB, CFB and OFB	Y	Y	2^{128}	N	Y	Y	Y	Sample images	Most of the cryptographic attacks
[12]	To develop a new cryptosystem for securing digital images transmission	Cellular automata and S-Box	Y	N	148-bits	N	N	N	Y	Sample image	Statistical, brute-force and Chosen plain image attacks
[90]	To present a secure and fast image encryption techniques for grey scale images	DNA coding, 3D and 4D-heyperchaotic map	Y	Y	10^{141}	Average time to encrypt four test images 19.1744 s	Y	Y	Y	Standard grey images	Exhaustive, statistical, differential, cropping and noise attacks
[75]	To develop a secure encryption mechanism for transmission of digital images	laser chaos synchronization and Arnold cat map	N	Y	Initial parame-ters of chaotic map	O(M x N) where M x N=size of image	Y	N	Y	Sample images	Anti-interference and statistical attacks
[35]	To design a new secure and lossless encryption scheme for medical images	2D-SLMM, 2D-HSM, 2D zigzag confusion and Dynamic diffusion	Y	Y	10^{120}	5 s for encrypting an image of size 1024×1024	Y	Y	Y	National Library of Medicine's Open Access Biomedical Images Search Engine and AI studio	Brute-force, statistical, differential, classical, noise and data loss attacks

Table 5 (continued)

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attacks considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	Robustness	Histogram		
[84]	To introduce a robust and fast encryption scheme for digital images	May-Gompertz map, PWLCM and block permutation	Y	Y	10^{165}	0.3505 s for encrypting an image of size (900×600)	Y	Y	Y	Sample images	Brute-force, statistical, differential, noise, chosen plain image and chosen cipher attacks
[40]	To provide a secure encryption mechanism for digital images	Rubik's Cube Principle and XOR operation	Y	N	10^{1233}	5.40s for encrypting an image of size 1024×1024	Y	Y	Y	Sample images	Brute-force, statistical, noise and cropping attacks
[57]	To present a new method for encrypting multiple grey-scale images of various sizes simultaneously	PWLCM, SHA-256, block based diffusion and confusion operations	Y	Y	1.9635×2^{246}	3.2618 s to 3.2677 s, 0.8419 s to 0.8497 s and 0.4343 s to 0.4391 s for encrypting group 1,2 and 3 images respectively	Y	Y	Y	USC-SIPI and MATLAB R2012a image database	Most of the cryptographic attacks
[46]	To design a secure encryption scheme for digital images as well as text	HPRNG, LFSR, XOR operation, chaotic asymmetric tent map and genetic operations	Y	Y	2^{261}	35.810 s for encrypting an image of size (512×517)	Y	Y	Y	Sample images	Brute-force, statistical, differential, and noise attacks
[65]	To develop an efficient encryption scheme for IOT applications	2D-Von-Neumann cellular Automata	Y	Y	$2^{81 \times P}$	Faster as compared to ASE, DES and 3-DES	Y	Y	Y	Sample images	Brute-force, statistical, differential, cryptanalysis attacks and noise attacks
[29]	To design a lightweight cryptosystem to encrypt the edge-maps of medical images	Edge detection, one-time pad and chaotic map	Y	Y	160,000 for block size =3×3	0.0669 s for encrypting a grey image of size 256×256	N	Y	Y	Sample images	Most of the cryptographic attacks

Table 5 (continued)

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attacks considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	Robustness	Histogram		
[60]	To propose an attack-resistant image encryption against attackable chaotic maps	Hopfield attractor, substitution and permutation	Y	N	10^{112}	0.251 s for encrypting a grey image of size 256×256	Y	Y	Y	Standard grey images	Most of the cryptographic attacks
[77]	To develop a secure encryption technique based on proposed hybrid chaotic system	Hybrid Chaotic system (TLTS & TSTS), Permutation and Diffusion	Y	N	2^{312}	0.6212 s for encrypting an image of size 256 × 256	Y	N	Y	Sample images	Brute-force, statistical, differential and Known/Chosen plaintext attacks
[10]	To develop an efficient image encryption algorithm for multiple grey scale images	Henon and Logistic map, Bit-plane decomposition	N	N	7.3724×10^{134}	9.565 s for encrypting 4 images of size 512×512 simultaneously	Y	Y	Y	Sample images	Brute-force, Statistical, chipertext only, known/chosen plaintext and Chosen ciphertext attack

RGB channels. The encryption module is also responsible for deciding the number of rounds to execute for encryption at random. Finally, the cipher image for the given image is created by combining the encrypted matrices for RGB channels. Although the proposed scheme outperforms in the National Institute of Standards and Technology and diehard randomness tests and is fast enough, its key space is vulnerable to exhaustive attacks.

A lightweight cryptosystem is proposed in [29] by Khashan and AlShaikh for digital medical images. There are three primary phases in the suggested scheme. The given image is first divided into uncorrelated blocks of pixels of a predetermined size. Then, using a specific threshold value, a Prewitt edge detection method [60] is employed to distinguish the significant image blocks. In the second phase, a chaotic map is utilised to create encryption keys that correspond to the significant image blocks. In the last stage, an OTP technique is used to encrypt the selected significant blocks in succession, and the non-significant blocks are left unencrypted. Simulation results suggested that the proposed method is secure against common attacks and also has less computing complexity. However, its performance needs to be analysed further in terms of security analysis, as some of the pixels of the plain image are left unencrypted. Therefore, this scheme might be vulnerable to chosen-plaintext/ciphertext attacks.

Alawida et al. [77] presented a technique for image encryption that included hybrid digital chaotic maps (TLTS and TSTS). In this technique, permutation and diffusion are performed twice. Permutation is used on the plain image in the first round, employing both TLTS and TSTS maps, as well as the secret key. The diffusion method is then applied to the permuted picture using the aforementioned chaotic maps. After being divided into two halves, the resultant image is used as input for the second round. TLTS, TSTS and the secret key are used to conduct permutation on both halves. In the permutation step, both halves are combined. Finally, the ciphered image is obtained by diffusing the permuted image. The simulation results revealed that this scheme is extremely sensitive to the change in the original or ciphered image. Therefore, it is vulnerable to noise and cropping attacks. However, this scheme is highly resistant to statistical, differential and known/chosen-plaintext attacks.

An encryption method capable of encrypting various grayscale images simultaneously is suggested by Tang et al. [10]. There are four phases in this scheme. In the first phase, four grayscale images are divided into bit planes, which are then randomly split into bit blocks governed by the Henon map in the second phase. As a result, bit blocks from various bit planes are exchanged at random. In the last phase, four chaotic images are generated by performing an XOR operation between four scrambled images and a secret matrix governed by a logistic map. The resultant four processed images are represented by the RGB and alpha components of a portable network graphics image, respectively. Simulation results showed that the proposed scheme can withstand brute-force, statistical and known/chosen-plaintext attacks. However, the security analysis of this scheme needs to be investigated for other attacks. Furthermore, it is a lossy algorithm, as well, as it has a limited capability to bare noise containment and data loss.

The contribution made by other encryption based approaches is summarised and compared in Table 5.

4 Potential gaps

This review indicates that improvements can still be made to image encryption schemes to achieve better efficiency. The major issues with the important encryption methods are summarised in Fig. 4.

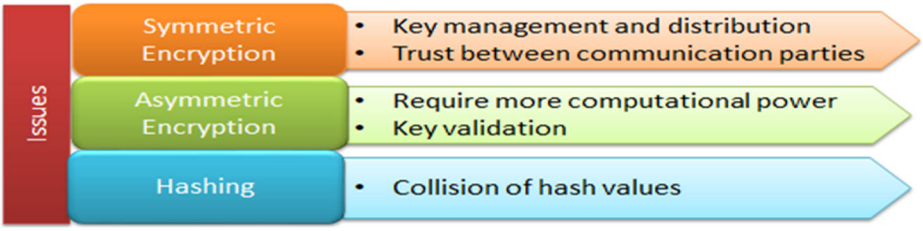

Fig. 4 Issues with encryption methods

Based on the techniques discussed here, we identify the following issues:

- Most of the encryption techniques have focused on one or two performance measures and have not addressed the issue of how to achieve a balance trade-off between competing parameters, such as security and complexity.
- Ordinary encryption may seriously damage the availability of data, as the original data is only available to the user encrypting it.
- When developing new encryption schemes or improving an existing technique, different types of possible attacks (i.e. differential, statistical, brute-force, chosen/known-plaintext, noise and occlusion attacks) should be considered.
- Although symmetric encryption is fast, it puts a burden of key management and exchange on communication parties, whereas asymmetric encryption removes the limitations of symmetric encryption, but computational complexity is high in this case.
- Chaos theory is appropriate for application in cryptography due to its dynamic character. However, compared to DES and AES, it has a higher computational cost.
- Hashing-based techniques suffer from a collision of hash values.
- In DCT-based encryption schemes, quantisation may introduce random noise, which can damage the quality of the recovered image.
- Cryptosystems based on reversible cellular automata require keys to be hidden, as the same is used for encryption and decryption.
- The image encryption techniques based on evolutionary algorithms are vulnerable to known plaintext attacks [56].
- The chosen-plaintext attack made a DNA-based image cipher unsafe [30].

5 Conclusion

In the present era, demand for the security of multimedia content being transmitted over the internet is increasing every day. Encryption is one of the key techniques that has been established to secure digital images. In this work, we have studied various image encryption techniques, their merits and limitations. Along with the study, a brief overview, notable applications and evaluation metrics of encryption techniques are provided. Then, the contributions of surveyed techniques are also summarised and compared in different technical perspectives. Finally, we highlighted the significant challenges and a few directions of possible research that could fill the gaps in these domains for researchers and developers. It has been observed that security flaws, parameter tuning and computational speed are still open areas of research in the field of image encryption. From a comprehensive review of existing image

encryption techniques, it can be concluded that image encryption is still an underdeveloped field. We need to investigate approaches that will manage the multiple performance parameters, i.e. high security and low cost.

References

1. Alawida M, Samsudin A, Teh JS et al (2019) A new hybrid digital chaotic system with applications in image encryption. Signal Process 160:45–58
2. Ali TS, Ali R (2020) A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map. IEEE Access 8:71974–71992
3. Alvarez G, Montoya F, Romera M, Pastor G (2003) Cryptanalysis of a chaotic secure communication system. Phys Lett A-306:200–205
4. Anwar S, Meghana S (2019) A pixel permutation based image encryption technique using chaotic map. Multimed Tools Appl 78(19):27569–27590
5. Ashtiyani M, Birgani PM, Hosseini HM (2008) Chaos-based medical image encryption using symmetric cryptography. In: 2008 3rd international conference on information and communication technologies: from theory to applications, Damascus, Syria
6. Bechikh R, Hermassi H, El-Latif AAA et al (2015) Breaking an image encryption scheme based on a spatiotemporal chaotic system. Signal Process Image Commun 39:151–158
7. 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
8. Benssalah M, Rhaskali Y, Drouiche K (2021) An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. Multimed Tools Appl 80:2081–2107
9. Chai X, Chen Y, Broyde L (2017) A novel chaos-based image encryption algorithm using DNA sequence operations. Opt Lasers Eng 88:197–213
10. Chen J, Chen L, Zhou Y (2020) Cryptanalysis of a DNA-based image encryption scheme. Inf Sci 520:130–141
11. Chengqing L (2016) Cracking a hierarchical chaotic image encryption algorithm based on permutation. Signal Process 118:203–210
12. Contreras J, Ramírez M, Aboytes J (2019) Image Encryption System Based on Cellular Automata and S-Box. Res Comput Sci 148
13. Dagadu JC, Li J, Shah F, Mustafa N, Kumar K (2016) DWT based encryption technique for medical images. In: 2016 13th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, pp 252–255
14. Dagadu JC, Li J, Shah F (2017) An efficient di-chaotic diffusion based medical image cryptosystem. In: 2017 14th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, pp 206–210
15. Dawahdeh Z, Yaakob SN, Othman RR (2017) A New Image Encryption Technique Combining Elliptic Curve Cryptosystem with Hill Cipher. Journal of King Saud University - Computer and Information Sciences 30:349–363
16. Dawahdeh ZE, Yaakob SN et al (2018) A new image encryption technique combining elliptic curve cryptosystem with Hill Cipher. Journal of King Saud University-Computer and Information Sciences 30: 349–355
17. Diab H (2018) An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations. IEEE Access 6:42227–42244
18. Duseja T, Deshmukh M (2019) Image compression and encryption using chinese remainder theorem. Multimed Tools Appl 78:16727–16753
19. El Assad S, Farajallah M (2015) A new chaos-based image encryption system. Signal Process Image Commun 41:144–157
20. Faragallah OS, Afifi A et al (2020) Efficiently Encrypting Color Images with Few Details Based on RC6 and Different Operation Modes for Cybersecurity Applications. IEEE Access 8:103200–103218
21. Hua ZY, Zhou YC, Pun C-M et al (2015) 2D Sine Logistic modulation map for image encryption. Signal Process 297:80–94
22. Huang X, Liu L, Li X, Yu M, Wu Z (2019) A new two-dimensional mutual coupled logistic map and its application for pseudorandom number generator. Math Probl Eng

23. Ibrahim S, Alhumyani H, Masud M et al (2020) Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps. IEEE Access 8:160433–160449
24. Jarin I, Fattah SA, Shahnaz C (2018) Natural and Medical Image Encryption Using Self-Adaptive Permutation and DNA Encoding. In: 2018 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE), Chonburi, Thailand, pp 99–102
25. Jiao K, Ye G, Dong Y, Huang X, Jianquing H (2017) Image encryption scheme based on generalized Arnold map and RSA algorithm. Hindawi Security and Communication Networks 2017
26. Kamal ST, Hosny KM, Elgindy TM, Darwish MM, Fouda MM (2021a) A new image encryption algorithm for Grey and color medical images. IEEE Access 9:37855–37865
27. Kaur M, Kumar V (2020) A Comprehensive Review on Image Encryption Techniques. Arch Computl Methods Eng 27:15–43
28. Khan S, Han L, Lu H, Butt KK, Bachira G, Khan N (2019) A new hybrid image encryption algorithm based on 2D-CA, FSM-DNA rule generator, and FSBI. IEEE Access 7:81333–81350
29. Khashan OA, AlShaikh M (2020) Edge-based lightweight selective encryption scheme for digital medical images. Multimed Tools Appl 79:26369–26388
30. Kong D, Shen X, Xu Q et al (2013) Multiple-image encryption scheme based on cascaded fractional Fourier transform. Appl Opt 52:2619–2625
31. Lakshmi C, Thenmozhi K, Rayappan JBB et al (2020) Hopfield attractor-trusted neural network: an attack-resistant image encryption. Neural Comput & Applic 32:11477–11489
32. Li S, Zheng X (2002) Cryptanalysis of a chaotic image encryption method. In: 2002 IEEE international symposium on circuits and systems, Phoenix-Scottsdale, AZ, USA, p II
33. Li S, Chen G, Wong KW, Mou X, Cai Y (2004) Baptista-type chaotic cryptosystems: problems and countermeasures. Phys Lett A 332:368–375
34. Li L, El-Latif AAA, Niu X (2012) Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images. Signal Process 92:1069–1078
35. Li S, Zhao L, Yang N (2021) Medical Image Encryption Based on 2D Zigzag Confusion and Dynamic Diffusion. In: Security and Communication Networks, vol 2021
36. Lin R, Li S (2021) An image encryption scheme based on Lorenz Hyperchaotic system and RSA algorithm. Secur Commun Netw 2021
37. Liu H, Kadir A (2015) Asymmetric color image encryption scheme using 2D discrete-time map. Signal Process 113:104–112
38. Liu H, Liu Y (2014) Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve. Opt Laser Technol 56:15–19
39. Liu L, Miao S (2016) A new simple one-dimensional chaotic map and its application for image encryption. Multimed Tools Appl 77:21445–21462
40. Loukhaoukha K, Chouinard J-Y, Berdai A (2012) A secure image encryption algorithm based on Rubik's cube principle. J Electr Comput Eng 2012
41. Luo Y, Ouyang X, Liu J, Cao L (2019) An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems. IEEE Access 7:38507–38522
42. Mallouli F, Hellal A, Sharief Saeed N, Abdulraheem Alzahrani F (2019) A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms. In: 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud), Paris, France, pp 173–176
43. Mishra M, Pandit S (2014) Image encryption technique based on chaotic system and hash function. In: Proceedings of IEEE International Conference on Computer Communication and Systems ICCCS14, Chennai, India, pp 063–067
44. Mokhtar MA, Sadek NM, Mohamed AG (2017) Design of Image Encryption Algorithm Based on different chaotic mapping. In: 34th National Radio Science Conference, Alexandria, Egypt
45. Mondal B, Mandal T (2017) A light weight secure image encryption scheme based on chaos & DNA computing. Journal of King Saud University - Computer and Information Sciences 29(4):499–504
46. Mondal B, Mandal T (2020) A secure image encryption scheme based on genetic operations and a new hybrid pseudo random number generator. Multimed Tools Appl 79:17497–17520
47. Munir R (2014) A block-based image encryption algorithm in frequency domain using chaotic permutation. In: 2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA), Kuta, Bali, Indonesia, pp 1–5
48. Niu Y, Zhang X (2020) A novel plaintext-related image encryption scheme based on chaotic system and pixel permutation. IEEE Access 8:22082–22093
49. Nkandeu YPK, Tiedeu A (2019) An image encryption algorithm based on substitution technique and chaos mixing. Multimed Tools Appl 78:10013–10034

50. Nkandeu YPK, Mboupda Pone JR, Tiedeu A (2020) Image encryption algorithm based on synchronized parallel diffusion and new combinations of 1D discrete maps. Sensing Imaging 21
51. Norouzi B, Seyedzadeh SM, Mirzakuchaki S, Mosavi MR (2014) A novel image encryption based on hash function with only two-round diffusion process. Multimedia Systems 20:45–64
52. Noura H, Chehab A, Noura M, Couturier R, Mansour MM (2019) Lightweight, dynamic and efficient image encryption scheme. Multimed Tools Appl 78:16527–16561
53. Oad A, Yadav H, Jain A (2014) Image Encryption Techniques and its Terminologies. Int J Eng Adv Technol 3(4):373–376
54. Osman M (2021) Wild and interesting Facebook statistics and facts, Kinsta, Available: https://kinsta.com/blog/facebook-statistics/
55. Parvees MYM, Samath JA, Raj IK, Bose BP (2016a) A colour byte scrambling technique for efficient image encryption based on combined chaotic map: Image encryption using combined chaotic map. In: 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, pp 1067–1072
56. Patro KAK, Acharya B (2018) Secure multi–level permutation operation based multiple colour image encryption. J Inform Sec Appl 40:111–133
57. Patro KAK, Acharya B (2020) A novel multi-dimensional multiple image encryption technique. Multimed Tools Appl 79:12959–12994
58. Ponuma R, Amutha R (2019) Encryption of image data using compressive sensing and chaotic system. Multimed Tools Appl 78:11857–11881
59. Prasetyo H (2018) A New Image Encryption Technique Using Simple Chaotic Maps. In: 2018 International Symposium on Electronics and Smart Devices (ISESD), Bandung, Indonesia, pp 1–4
60. Prewitt JM (1970) Object enhancement and extraction. Picture Processing and Psychopictorics 10:15–19
61. Rachmawati D, Tarigan J, Ginting A (2017) A comparative study of message digest 5 (MD5) and SHA256 algorithm. In: Journal of physics: conference series, 2017 2nd international conference on computing and applied Informatics-978, Medan, Indonesia
62. Ramírez-Torres MT, Murguía JS, Carlos MM (2014) Image encryption with an improved cryptosystem based on a matrix approach. Int J Modern Phys 25
63. Rao A, Suma D (2018) A Novel Image Encryption Algorithm with Image Integrity Check. In: 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), Bengaluru, India, pp 98–104
64. Rhouma R, Solak E, Arroyo D, Li S et al (2009) Comment on "Modified Baptista type chaotic cryptosystem via matrix secret key". Phys Lett A 373:3398–3400
65. Roy S, Shrivastava M, Pandey CV, Nayak SK, Rawat U (2020) IEVCA: an efficient image encryption technique for IoT applications using 2-D Von-Neumann cellular automata. Multimed Tools Appl 80: 31529–31567
66. Russell A (2017) A year without a byte, Available: https://code.flickr.net/2017/01/05/a-year-without-a-byte/
67. Seyedzade SM, Mirzakuchaki S, Atani RE (2010) A novel image encryption algorithm based on hash function. In: 2010 6th Iranian Conference on Machine Vision and Image Processing, Isfahan, Iran, pp 1–6
68. Singh N, Sinha A (2010) Chaos based multiple image encryption using multiple canonical transforms. Opt Laser Technol 42:724–731
69. Somaraj S, Hussain MA (2016) A Novel Image Encryption Technique Using RGB Pixel Displacement for Color Images. In: 2016 IEEE 6th International Conference on Advanced Computing (IACC), Bhimavaram, India, pp 275–279
70. Sprott JC (2011) A proposed standard for the publication of new chaotic systems. International Journal of Bifurcation and Chaos 21(9):2391–2394
71. Sreelakshmi K, Ravi RV (2020) A Bidirectional Diffusion Based Image Encryption Scheme for Color Images. In: 2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, pp 1–6
72. Systrom K (2021) Instagram by the Numbers: Stats, Demographics & Fun Facts. Available: https://www.omnicoreagency.com/instagram-statistics/
73. Tang Z, Song J, Zhang X, Sun R (2016) Multiple-image encryption with bit-plane decomposition and chaotic maps. Opt Lasers Eng 80:1–11
74. Tedmori S, Al-Najdawi N (2012) Lossless Image Cryptography Algorithm Based on Discrete Cosine Transform. Int Arab J Inform Technol 9(9):471–478
75. Wang S-Y, Zhao J-F, Li X-F, Zhang L-T (2016) Image blocking encryption algorithm based on laser Chaos synchronization. J Electr Comput Eng 2016
76. Wang X, Zhu X, Wu X, Zhang Y (2018) Image encryption algorithm based on multiple mixed hash functions and cyclic shift. Opt Lasers Eng 107:370–379

77. Wong KW, Yap WS, Wong DCK et al (2020) Cryptanalysis of genetic algorithm-based encryption scheme. Multimed Tools Appl 79:25259–25276
78. Wu Z, Zhang X, Zhong X (2019) Generalized Chaos Synchronization Circuit Simulation and Asymmetric Image Encryption. IEEE Access 7:37989–38008
79. Xie EY, Li C, Yu S, Lü J (2017) On the cryptanalysis of Fridrich's chaotic image encryption scheme. Signal Process 132:150–154
80. Yang F (2013) Image Encryption Algorithm Based on Fractional Fourier Transform. In: 2013 International Conference on Computational and Information Sciences, Shiyang, China, pp 705–708
81. Yang B, Liao X (2018) A new color image encryption scheme based on logistic map over the finite field Z_N. Multimed Tools Appl 77:21803–21821
82. Yassein MB, Aljawarneh S, Qawasmeh E, Mardini W, Khamayseh Y (2017) Comprehensive study of symmetric key and asymmetric key encryption algorithms. In: 2017 International Conference on Engineering and Technology (ICET), Antalya, Turkey, pp 1–7
83. Ye G, Pan C, Huang X, Mei Q (2018) An efficient pixel-level chaotic image encryption algorithm. Nonlinear Dynamics 94:745–756
84. Yepdia LMH, Tiedeu A, Kom G (2021) A Robust and Fast Image Encryption Scheme Based on a Mixing Technique. Secur Commun Netw 2021
85. Yousif SF, Abboud AJ, Radhi HY (2020) Robust image encryption with scanning technology, the El-Gamal Algorithm and Chaos Theory. IEEE Access 8:155184–155209
86. Zefreh EZ (2017) An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions. Multimed Tools Appl 79:24993–25022
87. Zhang Y-Q, Wang X-Y (2014) A new image encryption algorithm based on non-adjacent coupled map lattices. Appl Soft Comput 26:10–20
88. Zhang X, Wang X (2018) Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem. IEEE Access 6:70025–70034
89. Zhang X, Zhao Z, Wang J (2014) Chaotic image encryption based on circular substitution box and key stream buffer. Signal Process Image Commun 29(8):902–913
90. Zhang Q, Han J, Ye Y (2020) Multi-image encryption algorithm based on image hash, bit-plane decomposition and dynamic DNA coding. IET Image Process 15:885–896
91. Zhu S, Zhu C, Wang W (2018) A New Image Encryption Algorithm Based on Chaos and Secure Hash SHA-256. Entropy 20(9):716–734