Evolutionary Intelligence (2023) 16:801–818
https://doi.org/10.1007/s12065-021-00683-x

RESEARCH PAPER

A survey of image encryption for healthcare applications

Priyanka[1] · **Amit Kumar Singh**[1]

Received: 16 September 2021 / Revised: 29 October 2021 / Accepted: 7 November 2021 / Published online: 14 June 2022

Abstract
Recently, medical image encryption has attracted many researchers because of security issues in the communication process. The recent COVID-19 has highlighted the fact that medical images are consistently created and disseminated online, leading to a need for protection from unauthorised utilisation. This paper intends to review the various medical image encryption approaches along with their merits and limitations. It includes a survey, a brief introduction, and the most utilised interesting applications of image encryption. Then, the contributions of reviewed approaches are summarised and compared regarding different technical perspectives. Lastly, we highlight the recent challenges along with several directions of potential research that could fill the gaps in these domains for researchers and developers.

Keywords Image encryption · Security · E-Healthcare · Chaotic map · ECC · DNA · Cellular Automata · Fuzzy

1 Introduction

With the popularisation of smart and intelligent devices, the digital form of health records and more generally, electronic health records, are consistently generated and circulated online for information acquisition with accurate results [1, 2]. Electronic health records are normally composed of patient-related information, medical history, symptoms and more information, which are maintained by the involved services in healthcare. Moreover, in recent years, a lot of medical images and records have been consistently created and disseminated online among medical specialists and healthcare workers due to the appearance of COVID-19 [3, 4]. Furthermore, in [5], the high court of Bombay refused to give bail to a man who was out on temporary bail for about 10 months on the basis of forged medical documents in 2021, while in another case in 2019, IBM reported that the health industry had recorded maximum cases of data breaches and that data can be misused in several ways [6]. Moreover, in 2015, millions of people were affected by health data breaches in the US [7].

✉ Amit Kumar Singh
amit.singh@nitp.ac.in

Priyanka
priyanka.phd20.cs@nitp.ac.in

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

Therefore, due to the value of electronic health records from various perspectives, it is a great challenge for various research communities to study the situation of their illegal utilisation. Although health insurance portability and accountability act (HIPAA) provided the privacy regulation for the digital health records, it is still a challenge to address the security of these records [8].

Encryption is one of the highly recommended security solutions for medical images in healthcare [9]. In this scheme; we convert our original image in some cipher image form so that no one other than a legitimate user can access its information [10]. Given a plain image M, its ciphered image, denoted by N, is computed as follows:

$$N = E_K(M) \tag{1}$$

$$M = D_{K'}(N) \tag{2}$$

where E() and D () denotes the encryption and decryption function, respectively. In addition, K and K' denotes the encryption and decryption key, respectively. Correspondingly, Fig. 1 shows the Basic encryption/decryption procedure of medical image.

Generally, encryption techniques are broadly divided into two classes: symmetric and asymmetric techniques. Symmetric encryption requires a single key to protect the image, whereas asymmetric techniques employ two distinct keys (i.e. public and private keys for image protection) [10]. Compared to symmetric encryption, asymmetric encryption

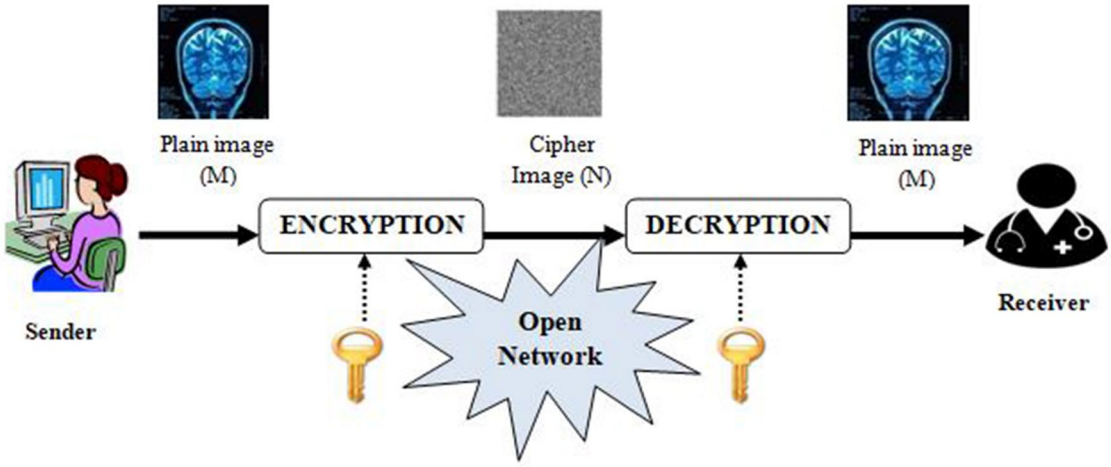

Fig. 1 Basic medical image encryption and decryption procedure

has the advantage in better security, but it takes longer in its execution time. Over the past decades, researchers have been using conventional encryption to ensure the certainty of digital images. However, these techniques are no longer applicable in practice due to the inherent nature of digital images [11].

In need of more security for images, the concept of hashing was introduced. It is a one-way function of cryptography that converts any form of data into a unique string of text known as the message digest. The hashing process is an irreversible process if the algorithm is designed properly. Its main contribution is to verify the integrity of an image to prevent any type of modification or corruption to the features of an image. Image hashing has a remarkable role in many applications such as image authentication, digital watermarking, image quality assessment, image retrieval and indexing [12]. Researchers developed the efficient encryption scheme to resolve the security issue of medical images (see Sect. 5).

Therefore, the main contribution of this article is to provide a brief introduction along with background information and evaluation metrics of image encryption. We then provide a comprehensive survey of various medical image encryption schemes along with their merits and limitations. Also, the contribution of the surveyed scheme is summarized and compared in the context of the estimation of design objectives, goals, approaches, evaluation metric and weaknesses. Lastly, we highlight the recent challenges along with several directions of potential research that could fill in the gaps of these domains for researchers and developers.

1.1 Requirements of image encryption

Security of images has become a complex problem due to peculiar features of images [13].In the following section, various essentials of image encryption for image security are summarized (Fig. 2).

- **Security**: Security is the key requirement for encryption procedure. The usage of an individual encryption process should ensure the reliability of an image feature. Generally, it incorporates perceptual security, key sensitivity and capability against probable attacks.
- **Perceptual security**: Any encryption process is secure in perception when the outcome of an encryption process produces an encrypted image in such a manner that it cannot be perceptually recognised.
- **Key space**: The possible unique encryption keys, present for the encoding process, known as the key space for a cryptosystem. A large value of key space indicates more security against exhaustive search attacks.
- **Key sensitivity**: It is the amount of resultant impact in cipher images while making only one bit change in the encryption key. Every encryption procedure should be sensitive to secret encryption keys.
- **Potential attacks**: Every image encryption method should be invulnerable to several possible attacks to an image encryption cryptosystem such as ciphertext-only attacks, known-plaintext attacks, differential attacks, etc.
- **Computational complexity**: An image has more data capacity in comparison to text. If the complete image data is encrypted with a cryptographic model, the computational complexity of the entire image is very high, so the important data bits of an image can be encrypted to ensure image protection.
- **Invariance of compression ratio**: To ensure storage size, transmission bandwidth and quality of recovered compressed image invariance in its compression ratio need to be preserved by encryption technique.

Fig. 2 Basic requirements of image encryption

- **Real-time demand**: Video conferencing and image surveillance are examples of real-time performance. It is a basic need to maintain reasonable delay during encryption and decryption.
- **Multiple levels of security**: To maintain scalability, different iterations and variable key sizes can be used, which are also useful for maintaining a higher level of security.
- **Transmission error tolerance**: Due to noisy media for image transmission, real-time data transmission also occurs in noisy media. So, a perfect encryption model should be required.

1.2 Evaluation assessment of image encryption

Different performance metrics and factors are used to measure the performance of encryption techniques [14, 15]. Some of the standard metrics are discussed below (Table 1).

1. **Visual Assessment:** Binary, grey and colour images are examined visually to discover features of an image by looking at the encrypted images.
2. **Statistical Analysis**: The analysis of the relationship between pixels of any encoded image is known as statistical analysis. The histogram and correlation coefficient are used for this analysis.
3. **Differential Analysis:** This study is used to discover the modifications in the cipher image of the same plain image after performing a single bit change in secret key or plain image pixel.
4. **Security Analysis:** For security analysis of any method, we analyse the following factors:
   a. **Key Sensitivity Analysis:** It determines the impact on the encoded image after a single bit change in the key used for the encryption process. The evaluation is done by comparing two encrypted images pixel by pixel.
   b. **Key Space Analysis:** For the feasibility against brute-force attacks of any encryption technique, this analysis plays an important role.
5. **Time Complexity Analysis:** This is the time required for a group of commands to be executed. It includes the time consumed for the encryption and decryption process of an image. Its value varies based on several factors like the system configuration and the type of image used.

Table 1 standard metrics for image encryption

Type of assessment	Description	Metric
Security	Any encryption process invulnerable to all possible attacks	Perception security, huge key space,key sensitivity, defence against possible attacks
Computational time	The required time to execute a set of instructions	-Depends on the permutation and diffusion operations -Significantly low complexity and minimum time value of image encryption and decryption
Compression ratio	To reduce storage space or bandwidth required for an image transmission lossless compression of an image required	Compression ratio = (uncompressed size image)/(compressed size image)
Robustness	Resistance against statistical and differential attack	Histogram analysis, correlation coefficient, NPCR, UACI
Quality	It is a quality assessment between the decrypted and plain images	PSNR, SSIM
Entropy [16]	It is used to estimate the randomness of information of cipher images	$H(S) = -\sum_s (P(Si) \times \log P(Si))$

Further, some standard objective measures considered for the evaluating the encryption techniques are summarized in Table 2.

1.3 Common attacks in images

Here we introduce some frequents attacks in image processing [14, 18]:

1. **Ciphertext-only**: In this attack, only some sets of cipher texts are known to cryptanalysts, they try to decrypt ciphertext to have access to the secret key or plain text.
2. **Known-plaintext**: This is an attack in which an attacker tries to find out the secret key of encryption while the attacker knows some of the plaintext and associated ciphertext.
3. **Chosen-plaintext**: This is an attack where the attacker selects their own random plain images and inserts them into the encryption process, providing a helpful way to analyse the corresponding cipher image.
4. **Brute-force**: All possible combinations of keys are attempted to crack the secret key used for encryption until it is attained.
5. **Differential attack**: It is used to analyze the sensitivity of encryption method toward small changes in original image. The attacker makes a small modification in 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.
6. **Noise**: In this, attacker tries to insert noise into an encrypted image to destroy the usable information of plain image. By this it become an unsuccessful attempt for the intended user to recover the original image after the decryption procedure.
7. **Occlusion**: This attack is applied to examine the capacity of retrieving original images from encoded images that have lost some data because of malicious activity or clogging in the network.
8. **Entropy**: In this type of attack, an intruder forges unoriginal packets (i.e. already-known packets by the system) that are trivial linear combinations of the 'stale' packets that are collected or intercepted at an earlier time. These packets with no new coding information will significantly reduce the information entropy of the system.

1.4 The state-of-the art encryption approaches

Several medical image encryption approaches have been introduced using spatial, transform, optical and compressing sensing domain schemes. In the following subsection, we elaborate on different spatial-domain-based image encryption approaches, including comparisons between discussed techniques in the tabular form.

1.4.1 Encryption based on chaotic map

Chaotic maps have numerous features like ergodicity, structural complexity and shuffling properties, which all create a table to produce unknown nonlinear deterministic pseudorandom sequences that are highly sensitive to initial conditions. The maps are categorised as discrete maps and continuous maps for secure communication applications. Chaotic maps are extensively utilised, providing high computational speed along with better security [9, 15]. Author develops a high-speed encryption method using bulbun chaotic map [15]. This map is used to randomly generate several rows and columns to overcome the slower process of pixel-wise shuffling and the substitution process. They conduct row-wise shuffling and substitution of pixels, and then the same process is conducted column-wise. To prevent any leaks of information, the methods shuffle the position of the pixels by applying a circular shift. Further, to mask the pixel value,

Table 2 Evaluation method for image encryption

Metric	Description	Formula	Highlights
Number of Changing Pixel Rate (NPCR), Unified Averaged Changed Intensity (UACI)	Assessment of the encryption technique implemented Range of NPCR: 0 to + 1 Ideal value of NPCR: + 1 Ideal value of UACI for image of size 512 × 512 ≈ 34	$D(i,j) = \begin{cases} 0, if C^1(i,j) = C^2(i,j) \\ 1, if C^1(i,j) \neq C^2(i,j) \end{cases}$ $NPCR = \sum_{i,j} \frac{D(i,j)}{Tot}$ $UACI = \sum_{i,j} \frac{\lvert C^1(i,j) - C^2(i,j) \rvert}{L.Tot}$ where, C^1 and C^2 are encrypted images before and after one pixel change, L is the maximum pixel value supported and Tot is the total number of pixels	Any encryption algorithm should have a NPCR ≥ 0.9, and UACI≈ 0.33
Correlation Coefficient (CC)	It defines the relationship between correlated pixels of a plain and encoded image It is calculated in three directions: horizontal, diagonal, vertical Range of CC: -1 to + 1	$CC(x, y) = \frac{C(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$ Here, $C(x, y) = \frac{\sum_{i=1}^{K} (x_i - E(x))(y_i - E(y))}{p}$ $D(x) = \frac{1}{p}\sum_{p=0}^{n}(x_i - E(x))^2$ $D(y) = \frac{1}{p}\sum_{i=1}^{p}(y_i - E(y))^2$ where E(x), E(y) and D(x), D(y) indicate mean and standard deviation of x and y, respectively. C(x,y) represent the covariance between coordinates x and y and p is the number of pixel pairs (x_i, y_i)	For an encoded image CC should be ≈ 0
Mean Squared Error (MSE)	Evaluation, of error values, that define distinction between plain image from decrypted image Range of MSE: 0 to ∞	$MSE = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \frac{[X(i,j) - Y(i,j)]^2}{m} \times n$ where X and Y denoted as original and decrypted image. *i* and *j* are the coordinate of pixel of image size $m \times n$	For high quality of images, MSE should be near to zero
Peak Signal to Noise Ratio (PSNR)[17]	It is a quality assessment between the decrypted and plain images It is measured in decibel (dB) Range of PSNR: 0 to ∞	$PSNR = \frac{10\log 10(2n-1)2}{MSE}$ where n is the number of bits per pixel	PSNR value should be high between original image and decrypted images
Structural Similarity Index (SSIM)	Used to compute the homogeneity between plain and associated decrypted images It is quality measure parameter of decrypted image Range of SSIM: -1 to + 1	$SSIM = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x{}^2 + \mu_y{}^2 + c_1)(\sigma_x{}^2 + \sigma_y{}^2 + c_2)}$ Where (μ_x, μ_y) indicate the average and $(\sigma_x{}^2, \sigma_y{}^2)$ indicate variance of an input x and decrypted y images, respectively. σ_{xy} represent covariance of x and y. c_1 and c_2 are regularization constant	For an identical images it should be ≈ 1
Information Entropy (IE)	It computed as the average information per bit in an image Each pixel has different value Range of IE: 0 to + 8	$H(S) = -\sum_s (P(Si) \times \log P(Si))$ Where $P(S_i)$ represents the probability of occurrence of S_i in message source (S)	Value of IE should be close to 8 for 8-bit image
Execution Time (ET)	It defines the time needed to execute an image encryption process It is aggregation of compiletime and run time It is measured in:ms, seconds, minutes	–	The value of ET should be less for any encryption technique

modular operations along with bitwise XOR operations are performed. The highest security trial result illustrates that the scheme is immensely secure against differential attacks and features a fast computational speed of approximately 80 FPS, making this method suitable for real-time applications. However, making this method compatible for real-time application on high-resolution images is the main challenge.

In [19], Author develops an image encryption scheme aimed at achieving higher security via pixel permutation using a chaotic map. The method uses pixel permutation to obtain a normalised image. Next, a key is obtained from the normalised image, and a new matrix of the same size as original is created and initialised by a key. Finally, the encrypted version of the image is found via the combination of the normalised and the newly created image. Simulation results suggest that the scheme is secure for plaintext attacks. Although the method outperformed the Arnold's scheme, security analysis of the scheme needs to be investigated for other attacks. Complexity analysis of any encryption scheme is also a significant measure for any real-time applications, which need to be investigated for the suggested method. Taking on a similar scheme, Ying, and Zhang [20] apply modified Josephus traversing to scramble the image (row-wise and column-wise) and they consider the pixel permutation and diffusion to encrypt the image. Specifically, SHA-3 is employed on the original image to obtain the binary sequence. Subsequently, the chaotic system along with the diffusion process, are used to encrypt the image. The simulation observations show that the algorithm is secureagainst plaintext and differential attacks. However, the major drawback to the scheme is high computational complexity. In [21], a highly sensitive and secure beta chaotic map function-based image encryption scheme is suggested. Two beta maps of different initial values are randomly selected for random sequence generation and key construction. With these random sequences, the methods shuffle rows and columns of plain images to create chaos in the correlation between plain and cipher images. These results remarkably increase the invulnerability to attacks. In the stage of diffusion, as per the image type, different sizes of image blocks are used in every round; these image blocks can be modified if any changes lead to the plain image. Further, the approach offers a better value of entropy and correlation coefficient than other schemes [22, 23]. On that account, the scheme is resistant to several known cryptographic attacks. However, it is necessary to further discuss its computational complexity for real-time application. A firm image encryption algorithm based on double chaotic S-boxes, which are generated by a sine tent map, is suggested [24]. In this scheme, S-boxes are able to perform confusion and substitution of image pixels simultaneously. Confusion and diffusion operations in two forward and backward rounds with double S-boxes create resistance against differential attacks. The simulation outcome verifies the better capability of suggesting schemes in real-time encryption applications. Further, the suggested scheme indicates the foremost randomness value of the encrypted image compared with other methods [25–27].

A bit-level infallible and firm image encryption scheme was developed by Li Xu et al. [28]. This technique uses a piecewise linear chaotic map, which has exceptional encryption performance only in a single round of encryption. In this method, the original image is converted into two same-size binary sequences that diffuse mutually. After this, swapping of binary elements of one bit plane to another bit plane has been done by permutation operation under the control of chaotic map. Due to multiple operations like the construction of chaotic sequence and swapping operations, this method is slower than other algorithms. Further experimental results are compared with other techniques [29–31]. In order to accomplish this, Chai and Zhang [32] have introduced a novel image encryption structure that uses Latin square along with a memristive chaotic map. This method has made a huge impact in medical field applications. The scheme mixes up the pixels of the rows and columns of the original image with the use of plain image and Latin square, which reduces the amount of correlation between neighbour pixels. The hash value of the original image is computed by SHA-256, which makes this system strong against known attacks. From the experimental results, it is shown that the algorithm accomplishes the highest speed compared to other encryption schemes [33, 34].To prevail over the weaknesses of the available image encryption algorithms, a novel image encryption algorithm has been evolved [35]. This scheme uses multiple chaotic maps in different steps. Logistic sign maps are used in the first step to scramble the original image, after which 2×2 sub blocks are created by splitting the scrambled image. In the next step, a hyper-chaotic map is used to encrypt the sub blocks until the encryption of all the boxes is finalised. The performance result indicates that the limitation of the deficiency of diffusion in sole direction encryption is overcome by this suggested scheme, which also provides better security along with robustness.

The authors presented a framework based on chaotic maps, combined with dynamic S-boxes for efficient medical image encryption [36]. In this scheme, S-boxes were arranged before and after chaotic substitution, that make the suggested method more robust against chosen plaintext as well as chosen ciphertext attacks. Further trial outcomes indicated that the suggested framework successfully cleared each of the security evaluations, regardless of any chaotic map being used for execution. For fast, efficient processing, researchers endorse the use of the Hénon map or the Classical Baker map, which help to attain encryptions throughput at about 90 mbps without any hardware modifications. The

simulation outcomes show that, compared to other schemes, the suggested framework has a great value of NPCR and UACI [37].

Yang et al. [38], perform encryption on lossless compressed image data. The image is compressed using a neural network, following which the zigzag confusion permutes the compressed image. Finally, an XOR logical operation is performed between the confused image and the sequence generated by the chaotic map. This scheme encrypts and compresses the image, offering high levels of security and reduces costs for network bandwidth.

Further, the comparison of above discussed techniques is presented in Table 3.

1.4.2 Encryption based on elliptic curve cryptography (ECC)

In 1985, Neal Koblitz and Victor S. Miller developed a novel public key cryptography based on ECC, which delivers more reliability than other cryptosystems with the same key size. ECC can be used to prevent images from unauthorised modification and preserve the integrity of this digitised medical image. The specialty of ECC encryption is that in each execution cycle the encryption process with the same key creates a totally distinct cipher image [39, 40]. In the following, we briefly introduce the chaos-based image encryption. Authors developed an image encryption method using ECC along with digital sign cipher for more authenticity and integrity [39]. Coordinate values of the elliptic curve were used to execute all functions of ECC. For secure communication, all parties agreed on the equation and generator of the elliptic curve. In this structure, a few pixel groups were used to reduce the number of executions. The procedure of image encryption with ECC coordinate values of elliptic curves were mapped with the pixel value of an image. Suggested procedure helps to avoid the utilisation of reference tables for encoding/decoding process [40, 41].

MAES-ECC based, an upgraded image encryption scheme for embedded systems, was developed [42]. This method uses modified AES for eliminating the mix column transformation step, which is replaced by a permutation-based shift of columns that results in a reduction in time complexity along with keeping the Shannon principle of diffusion and confusion intact. Due to its security, along with its time efficiency in sizable medical images, the proposed algorithm is very useful, with impressive, enhanced entropy compared to other existing methods [43–46]. Although, the method has computational complexity, it needs to be reduced without affecting the security provided, which is the main issue.

In Reference [47], a robust easy key transmission and management for encryption of an image, a novel method that combined ECC with chaotic system, was developed. In this method, both parties agree upon the coordinate of the elliptic curve, which is based on the Diffie–Hellman public key sharing method. In the next step, the image is encrypted with that coordinate and chaotic system. The outcomes suggest that the method is secure from many known cryptographic attacks. Experimental demonstrations have been compared with several existing techniques [48–50]. However, the major drawback in the scheme is high computational complexity, which needs to be reduced. In [51], the authors developed a robust encryption scheme that is most suitable for applications that require a secure communication channel for image transmission that is also able to resist chosen plaintext attacks. To overcome the problem related with key management and security, the method used EC-ElGamal combined with chaotic theory. For generating the initial value of chaotic maps, SHA-512 was used. After this, crossover permutation was performed to scramble the plain image. The experimental results have compared with different existing techniques [52–54]. Simulation results suggest that the drawbacks are time consumption, which must be reduced and encryption speed, which needs to be increased using parallel processing.

In [55], author designed a robust encryption algorithm of images that integrates the elliptic curve cryptosystem with hill cipher. Conversion of a symmetric encryption technique into an asymmetric encryption technique by Hill Cipher makes this method more firm, efficient and invulnerable to attackers. In this method, secret keys for encryption and decryption purpose a self-invertible key matrix that is used that remove the overhead to find and share the inverse key for decryption process. The key matrix based on ECC used in this method makes it difficult for intruders to solve. Simulation results have reflected that the approach is time efficient and defends against different attacks. An image encryption process that incorporates ECC along with the classical Hill cipher, Arnold's Cat map (ACM) and linear congruence generator (LCG) that mainly utilises the medical field is proposed [56]. In this method, the encoding process of the broadcasted image based on the classical Hill cipher method has been done by dynamic key, which is produced by Diffie-Hellman protocol. Next, in the confusion phase of method, Arnold's cat map is used for separating value of image pixels into blocks, size of (4×4). Then, the self-invertible secret key matrix is multiplied by each block (4×4) modulo 216 for each block, and values are taken. In the next phase of diffusion, XOR is performed with the output of the LCG. Finally, the simulation results have been compared with other similar techniques [57–60]. An ordered-elliptic-curve-based hybrid binary image encryption method that utilises dynamic S-boxes for pseudorandom numbers has been introduced by Hyatt et al. [61]. Firstly, the method defuses the plain image by masking the plane image with the proposed PRN. In the consecutive step, the diffused image is confused by the dynamic S-boxes to enhancing the security of the image.

Table 3 Summary of various encryption methods based on chaotic maps

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attack considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	CC	Histogram		
[15]	To developed a systematic image encryption scheme with high processing speed	Bülban chaotic map, Circular Shift, XOR	Y	–	2^{360}	Time	Y	Y	Y	USC-SIPI Image Database	Differential attacks
[19]	To produces an image encryption method that eluding the attacker	Logistic Map, Confusion, Diffusion	Y	–	–	–	Y	Y	–	USC-SIPI Image Database	–
[20]	To developed an secure and improve image encryption systems that can resist plaintext attacks and differential attacks	Scrambling associates Josephus traversing,Chaotic system	Y	Y	–	Time	Y	Y	Y	Lena images of size 256×256	Statistical attacks, Selective-plaintext attacks, Exhaustive attacks
[21]	To introduce an image encryption schemes that increase the protection of an image	Beta Chaotic Map,Confusion,Diffusion	Y	Y	2^{512}	–	Y	Y	Y	USC-SIPI Image Database	Brute force attacks, differential attacks
[24]	To developed an improve image encryption systems that provide more security and efficiency	Double Chaotic S -Box, Confusion,Diffusion	Y	–	2^{258}	Time	Y	Y	Y	USC-SIPI Image Database	Various notable attacks
[28]	To develop a bit-level secure and reliable image encryption method	Cyclic shift, linear chaotic maps	Y	–	2^{210}	Time	Y	Y	Y	Greyscale 8-bit images. (256×256)	Brute-force attack, statistical, differential attack attacks
[32]	To provide a reliable encryption technique to secure medical image	Permutation based image, adaptive diffusion	Y	Y	3.402×10^{94}	Time	Y	Y	Y	Various image of different sizes	Known-plaintext, Chosen-plaintext attacks, statistical attacks
[35]	To design an adaptive medical image encryption algorithm that overcomes the defects of the pre present chaotic encryption schemes	Logistic-sine chaos mapping, hyper-chaotic system	Y	–	2^{512}	–	Y	Y	–	Lena (256×256)	Differential attacks
[36]	To develop an algorithm that achieve high encryption throughput	Dynamic S-boxes, Baker map or Henon map	Y	–	128-bit	Speed	Y	Y	y	CT image (750×870), MRI image (512×512), X-ray image (1338×1094)	Chosen plaintext and ciphertext, Reset attacks

By using the group law masking, the masking process of the proposed method consumes less time as compared to other EC-based techniques. The main highlight of the algorithm is that it provides a lossless security system. The experimental result has been compared with several existing techniques [62–64]. An ECC-based novel encryption scheme which collaborates with genetic algorithm-based optimization techniques for private key generation has been used for encryption purposes [65]. In this scheme, separate blocks (4 × 4 size) of pixel value matrices were formed for each red green blue (RGB) component of the colour image. Later, these blocks were encrypted by a public key which was generated by the ECC method. For the decryption process, an optimisation-technique-generated key was used. All execution findings are to be compared with the method introduced by Shankar et. al. [66].Vulnerability analysis and complexity analysis of any encryption process are very essential for real-time applications, which need to be investigated for the suggested method.

In order to accomplish this, Ibrahim and Alharbi [67] have develop an ECC-based image encryption method that utilises the collaboration of the hash algorithm with the Hénon chaotic map. For the enhancement of the reliability dynamic, S-boxes are used to create confusion. In this method, the researchers firstly proposed a process to construct novel dynamic S-boxes by the chaotic Hénon map. In the next phase, the plain image was encrypted with the encryption key, which was generated by ECC. Dynamic S boxes were used to create more chaos in the output image of the second phase. Finally, the hash algorithm was used to identify the malformed cipher image to defend against chosen ciphertext attack. The main feature of the proposed algorithm was high computational efficiency which achieved a speed of 150 mbps. Experimental demonstration was compared with several existing techniques [68, 69]. This method was designed only to encrypt grayscale uncompressed images, which is the main drawback of the method for colour image application. Laiphakpam presented an image encryption method drive from the elliptic curve over a finite field along with the chaotic system [70]. In the first step of the method, both parties of communication agreed upon some random coordinates of the elliptic curve by the concept of Diffie–Hellman public key sharing method. Next, this coordinate was used for the generation of chaotic sequences by logistic maps. Then, these sequences were converted into the integer value known as the byte value. Finally, Arnold's transform scrambled the plain image pixel value and later these pixel values are XOR with the byte values, which were generated in the previous step to produce a cipher image. The simulation results showed that the proposed method had a good avalanche effect along with resistance to many known cryptographic attacks. The efficiency of the proposed method against real time application, compared with other existing schemes [71–73], reflect the robustness of proposed method.

Further, the comparison of above algorithms is presented in Table 4

1.4.3 Encryption based on DNA methods

A peculiar method called the DNA technique has been developed in cryptanalysis. The DNA technique is used as an information bearer in image encryption which supports high delineation and huge data consistency. The structure of DNA decides the complexity of security. Henceforth, the computation of DNA over image is very difficult [74]. Using DNA and anarchic logistic maps, a robust scheme has been developed [75]. The method first combines a DNA-encoded input image and a 1D chaotic map mask by using DNA addition. After the first step, to receive the cipher image, the resultant matrix is permuted using a 2D-chaotic map pursued by DNA decoding. The suggested method provides a completely invertible method which can resist known attacks (i.e. statistical, plaintext and differential attacks). A robust logistic map-DNA method for colour image encryption was initiated by Suri et al. [76]. The suggested research was a combination of intertwining logistic map (ILM) that works as a location map along with other approaches for generating initial value. ILM-generated 3D chaotic sequences were used to permute the pixels of the original image; meanwhile, the SHA-256 function was deployed to produce the initial values for chaotic sequences creation. Hereafter, DNA XOR operation was executed to diffuse the permuted pixels of the previous step. The calculated output reflected a remarkable enhancement in the entropy value and high defence against various differential and statistical attacks. The simulation resulted in an improvement in encryption efficiency compared to other techniques [77, 78].

In [79], a "permutation–diffusion–scrambling" structure based on an image encryption method was developed. This SHA-3 algorithm was used to compute the hash value of a plain image that utilised the seed of the hyperchaotic system, along with the chaos-generated sequence as the initial value, to produce the Hill cipher matrix that changed pixel positions in the image. In this chronology, image encryption was done on the grounds of Feistel network and dynamic DNA encoding. To minimise the number of rounds of encryptions, DNA sequence was used. The reliability analysis of suggested methods indicated that the use of Feistel transformation, along with scrambling and DNA encoding/decoding technology, made the method completely resistant to several known attacks in comparison to other schemes [80, 81]. Computational complexity needs to be discussed for any image encryption method. In this progression, "DNA-complementary" rules-based colour image encryption process along with pair-coupled chaotic maps was proposed [82]. As per the process, the image was split into RGB components, which were converted into three distinct DNA matrices with the help of DNA encoding rules. After the DNA addition

Table 4 Summary of ECC based encryption

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attack considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	CC	Histogram		
[39]	To develop a method that digitally signs the cipher image to provide authenticity and integrity	12 bit Standard Elliptic curve	–	–	2^{512}	Time	Y	Y	Y	Lena (1024×1040) Pepper (512×520) Mandrill (256×260	Known Plaintext attack
[42]	To introduce a method that encodes largesize images with high security in efficient time	ECC (Elliptic curve),MAES (Modified AES)	Y	–	2^{128}	Time	Y	Y	Y	Lena (512×512×3) Peppers (512×512×3) Baboon (512×512×3) 3D scanner ankle (1080×1920×3)	Statistical attacks, Noise attack, Differential attacks, Brute force attack
[47]	To develop a secure key transmission and management method	ECC, Chaotic System	Y	–	2^{512}	Time	Y	Y	Y	Airfield (512×512)	Various notable attacks
[51]	To develop a robust encryption method with time efficiency	Elliptic curve ElGamal, chaotic theory, SHA-512 hash	Y	Y	2^{100}	Time	Y	Y	Y	Lena (512×512) Barbara (512×512) Peppers (512×512) Baboon (512×512) Car (512×512)	Various notable attacks
[55]	To develop a method that resists various attacks and exhibits better security features	ECC, Hyper chaotic Lorenz generator (HCLG), Arnold cat map, Hill cipher	Y	Y	–	Time	Y	Y	Y	Lena (512×512)	Exhaustive search attack, data losses attacks, noise attacks, Differential-statistical attacks, occlusion attacks
[56]	To propose a scheme that is applicable for secure image communication	ECC, Hill cipher, Arnold, Linear congruence generator	Y	Y	–	Time	Y	Y	Y	Lena (512×512) DICOM (512×512)	Differential, Statistical attacks
[61]	To develop a method that is resistant against cryptographic attacks without losing information	ECC, Dynamic S-boxes, pseudo random numbers (PRN)	Y		2^{128}		Y	Y	Y	Circuit (450×600) Boat (256×256) Lena (256×256) Pepper (512×512)	Various notable attacks
[65]	To introduce a n efficient method which provides secure transmission, without losing confidentiality of image	ECC, Genetic Algorithm (GA)	–	Y	–	–	–	Y	–	USC-SIPI Image Database	Breach of confidentiality
[67]	To develop firm and structured image encryption procedure	ECC, Henon Chaotic map,Dynamic S-Boxes	Y		10^{62}	Time	Y	Y	Y	USC-SIPI Image Database	Chosen-plaintext, Chosen-ciphertext attacks, Brute-force attacks

Table 4 (continued)

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attack considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	CC	Histogram		
[70]	To develop a secure and fast encryption process that utilize for real-time image operations	ECC, Chaotic system, Arnold's transform, Diffie-Hellman public key		Y	2^{512}	Time	Y	Y	Y	Lena (512×512) Plane (512×512) Baboon (512×512)	Chosen-plaintext attack, Brute force attack, Occlusion attack

of RGB components was implemented via the pair-coupled chaotic maps, pixels were permuted. Experimental demonstration was compared with several existing techniques [83, 84]. However, processing speed was the fundamental issue related to the suggested scheme. A robust image encryption process in which image pixels are dispersed by the DNA approach and permuted by a two-dimensional Hénon-Sine map is recommended to save image content when an image is transmitted over the internet [85]. Initially, 2D-HSM is created in such a manner that it acquires better ergodicity and pseudo randomness. Thereafter, a DNA encoding and a DNA- XOR operation applied over image encryption improves the efficiency of image permutation and diffusion. Further, the preliminary analysis against various attacks and performance metrics are compared with several methods [86, 87]. After all, the fundamental drawback of the recommended scheme is designed basically for grey image. The multimedia data or the coloured images must be converted into the same pattern of grey images and thereafter will be encrypted with the scheme, which will increase the computational complexity of the method.

Further, the comparison of above discussed techniques is presented in Table 5.

1.4.4 Encryption based on miscellaneous schemes

A mathematical model which works on discrete input/output is known as cellular automata. This is used to indicate the sequential behaviour of interconnected cells organised in a regular manner, all of which have a finite set of possible values [88].

A spatial domain secure and robust image encryption scheme that uses eliminatory cellular automata (ECA) combined with the chaotic tent map was developed [89]. In this method, the plain image is divided into blocks. Later, these individual blocks are encrypted with a distinct key stream by using ECA with a chaotic tent map. In the next phase of the method, the shuffling process of bytes of encrypted blocks is done to generate more diffusion. The main uniqueness of the proposed method is using variable sizes of blocks and keys for all operations like encryption and shuffling. Further, the preliminary analysis against various attacks and performance metrics are compared with several methods [90–92]. However, the method is not feasible for real-time application. Reference [93] developed an encryption process that is helpful for encrypting images of all dimensions. In the method, the correlation between the neighbor pixels was removed by permuting the pixels of the plane image with PRNS, which is generated by CA. After this, with the use of a single random number that is generated by skew tent map, encryption of permuted images was performed. Experimental demonstration was compared with several existing techniques [94–96].The method has the key benefit of large key

Table 5 Summary of DNA based encryption

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attack considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	CC	Histogram		
[75]	To develop a robust image encryption algorithm which provides a totally invertible method that can resist various attacks	DNA,1D & 2D Chaotic maps	Y	Y	10^{96}	Time	Y	Y	Y	USC-SIPI	Known plaintext attack, Statistical attacks, Differential attacks
[76]	To suggest a method that ensures a secure transmission of image information	DNA,ILM,SHA-256	Y	–	2^{256}	–	Y	Y	Y	Lena (256×256) Bungee (256×256) Baboon (256×256)	Differential attack, Statistical attack, Brute-force attack
[79]	To introduce a reliable image encryption method based on the Feistel network	Feistel network, dynamic DNA encoding, Hill matrix, chaotic sequence	Y	–	10^{100}	–	Y	Y	Y	Lena (256×256) gray scale	Exhaustive attack, Plaintext attack, Differential attack, Statistical attack,
[82]	To develop a high-speed image encryption and decryption method	DNA encoding, Pair coupled Chaotic map	–	–	10^{450}	–	Y	Y	Y	Lena (256×256)Color image	Statistical attack, Differential attack, Exhaustive attack
[85]	To introduce a secure encryption method for robust transmission	DNA sequence, 2D Henon- Sine map	Y		10^{112}	Space	Y	Y	Y	Lena (256×256) (512×512) cameramen (256×256)(512×512) Baboon (256×256) (512×512)	Exhaustive attack, Robustness against noise, Anti noise attacks, statistical attack, differential attack

space and better encryption effects, along with drawback of a limit on the amount of data to be handled.

Focusing on reliability of digital image, a novel structure for image encryption based on DNA and recursive cellular automata was developed [97]. In this scheme, a logistic map was employed at the permutation phase for circular shift in the image rows and columns, and then DNA and RCA at the diffusion phase were used to modify the grey level of the pixel to new values. The use of RCA and DNA increased the security of cryptography systems and made it more resistant to all kinds of attacks. Computational complexity analysis should be discussed by any encryption algorithm, which needs to be investigated for the suggested method. In [98], a non-uniform cellular automata (CA) structure was proposed that used chaotic maps for performing confusion in the plane image by randomly changing the position of pixels in the image. This permutation was done in a row/column-wise manner for the colour component of the image. To create rules for CA, logistic maps were used, which have a unique characteristic in that a tiny change in a CA parameter results in a new and different CA. These rules were employed on the sales of CA that generate key images. In the next step, with the use of a hyper chaotic map, the method selects a random key image for encryption. Experimental outputs indicate that the suggested scheme has great resistance against noise attacks and has a large key space that makes the suggested method more robust compared to other schemes [99–101].

To overcome the issues related to the secret key generation, a new image encryption method which uses CA along with memristive hyperchaotic system was proposed by Chai et al. [102]. In the diffusion phase, the scheme used two different DNA rules for encoding the plain image into blocks. In the next step, these diffuse image blocks were combined with two-dimensional CA for encryption. There are so many discrete numbers of DNA-encoding regulations available for unique original images. This structure can be useful in many real-time applications like video communication and secure image transmission. To check the effectiveness of the scheme, it has been compared with the existing method [103–105].

A secured lightweight keyed transposition structure is drafted to derange the correlation of pixels of plain image [106].This method execute lookup table operations to decrease computational complexity, power consumption and resource requirement. The proposed scheme uses Hénon chaotic map along with ECA, which has dynamic properties for extracting and analysing the lookup table for each pixel of an image. For the encryption process, bitwise XOR operations are performed on plain image pixels. This scheme is useful for both colour and grayscale images. Simulation results indicate that the reliability and robustness of the method are also embraced in the IoT and sensor networks [93, 107, 108]. However, the method has the disadvantage of small rule space and low diffusion. In order to this, Ping and Wu [109] developed a low computational cost encryption algorithm which uses cellular automata with 2D logistic-adjusted-sine chaotic map (2D-LASM). In the phase of confusion, the positions of image pixels were permuted or shuffled by 2D LASM with chaotic attributes. After the permutation phase, the diffusion phase substitution of pixels was accomplished by a rule of reversible life-like CA. Simulation results were compared with the existing method [110, 111], which showed the superiority of the proposed method. However, the security analysis of the scheme needs to be investigated for other attacks. A new approach to upgrade the cryptographic features of S-boxes used as a basis of the Choquet Fuzzy Integral (CFI) and the DNA method has been proposed [112]. First of all, suggested methods construct a strong structure of four S-boxes using CFI, which are also encoded using the DNA method. These encoded S-boxes are known as DNAFZ S-boxes. After this, the plain image is shuffled by M sequences and sampled into four sub images for the encryption process. After this the pixel value of all sub images are replaced with one of four DNA FZ S-boxes, which are diffused with unique DNA encoded chaotic sequences from Chen's hyper chaotic map. In the final step the four DNAFZ Sub images are combined to construct the final cipher image. The suggested method has excellent statistical characteristics and better encryption efficiency compared to many other methods based on Arnold transform, Hénon map and hybrid chaotic map. A robust image encryption system based on B-spline function along with CFI to perform confusion and diffusion of pixels in plain image has been suggested [113]. The method uses a 3D hybrid chaos system to produce pseudorandom numbers. Further CFI with B-spline function is used to initialise the key to iterate the chaos system for every round. The use of a special type of shifting operation of CFI makes the suggested method more defensive against several types of cryptographic attacks like data loss attack and noise attack compared to other methods [114, 115]. In [116], researchers proposed a new procedure to generate a random key stream for image encryption purposes that utilises the CFI characteristics. The method first splits the colour image pixels into three grey-level components. After this, bits of these grey-level components are randomly shifted with these pseudorandom generators CFI. Finally, the output component of colour image (i.e. colour pixels) and the generated key stream are combined to encode the permuted components. CFI has very high randomness of sequence generated, which is very effectively regarding the security, reliability and sensitivity of the suggested method. For the protection of image data, which is distributed over the internet, the suggested method performs very effectively [117–119]. The execution speed analysis of the encryption/decryption process need to be investigated for the suggested method. Further, the comparison of above discussed techniques is presented in Table 6.

Table 6 Summary of various encryption methods based on miscellaneous schemes

Ref	Objective	Used approaches	Evaluation metric used							Database information	Attack considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	CC	Histogram		
[89]	To evolve a robust unique image encoding scheme	Cellular automata,Chaotic tent map	Y	–	2^{576}	Time	Y	Y	Y	Eight different-sized images Lena (256×256)	Various popular attacks
[93]	To develop a novel image encryption that can resist most known attacks	A skew tent, CA	Y	Y	2^{256}	Time	Y	Y	Y	Lena, Checkbox, Airplane, Baboon, Barbara, Ship, Pepper, Nike logo	Various popular attacks
[97]	To propose a scheme that uses RCA and DNA increases the security	Deoxyribonucleic Acid (DNA), Recursive Cellular Automata (RCA)	Y		–	Time	Y	Y	Y	Lena, Baboon, Cameraman, House, Jet Plane, Lake,(512×512) (256×256)	Brute-force attacks
[98]	To design a method that protects the content of image with high efficiency	Hyper chaotic functions, non-uniform CA	Y		2^{128}		Y	Y	Y	Lena, Peppers, Baboon images (256×256×3)	Statistical attacks, data loss attack, Noise attack, Brute-force attacks, differential attack
[102]	To propose a secure and robust image encryption scheme	Cellular automata, Memristive hyper chaotic system, DNA sequence operations	Y		2^{128}		Y	Y	Y	Lena (256×256)	Various popular attacks
[106]	To develop a lightweight scheme that is secure from statistical attacks	Elementary cellular automata with novel permutation box	Y	Y	$\mathbf{2}^{64\times64\times8}$		Y	Y	Y	Lena, Baboon, Airplane,Peppers Barbara (256×256)	Statistical attacks
[109]	To design secure and a high sensitivity system	Choquet fuzzy integral (CFI)	Y		2^{128}	Time	Y	Y	Y	CVG-UGR, PSU	Statistical analysis attack, entropy attack, brute-force attack, plaintext attack
[112]	To design an encryption method that resists various attacks	CA combined with chaotic map, 2D-LASM	Y		2^{512}	time	Y	Y	Y	CVG-UGR image database	Chosen-plaintext, known-plaintext attacks, brute-force attack, statistical attack
[113]	To introduce an encryption scheme that overcomes security shortcomings	Choquet Fuzzy Integral, DNA	Y	Y		time	Y	Y	Y	Lena (256×256)	Chosen plaintext attack, Differential attacks

Table 6 (continued)

Ref	Objective	Used approaches	Evaluation metric used						Database information	Attack considered
			NPCR and UACI	PSNR	Key space	Complexity (time or space)	Entropy	CC	Histogram	
[116]	To develop an algorithm of encryption that provides high key sensitivity and least information loss	3D hybrid chaos map, Choquet Fuzzy Integral, B-spline functions	Y				Y	Y	Y	Lena ($256\times256\times3$), Sailboat, Panda	Various attacks

2 Potential challenges

A lot of efficient encryption techniques have been developed in medical-domain. After doing the complete literature survey for the encryption of medical images, we highlight some of potential challenges to medical image encryption:

1. Our aim should be to preserve the accuracy of the encoded medical images, so for this it is very much needed to maintain the quality of the medical images without modifications.
2. Most of the encryption schemes have focused on one or two performance measures and have not addressed the issue of how to achieve a good trade-off between competing parameters such as security and complexity.
3. Ordinary encryption may seriously damage the availability of data, as the original data is only available to the user encrypting it.
4. In E-Healthcare application, any types of tempering in medical images are not acceptable. Only the best qualities of images are required. So the procedure of medical image encryption requires being resistant to any type of attacks on images over the network.
5. In ECC, the compulsion of the sender and receiver systems to have the same processor and precision value restrict the use of algorithms.
6. Cellular automata have small rule space and low diffusion power that limits the diversity in encryption/decryption algorithms.
7. The structure complexity of DNA decides the security which also causes the computation of DNA over image is very difficult.
8. To find an effective way to merge compression and encryption of animage for effective bandwidth utilisation is an interesting subject for future research.

3 Conclusion

Medical image encryption has great potential to provide valuable solutions to a variety of issues for E-health applications. The issues include E-health data storage, management, sharing of private data, identity theft and data security. This paper presents an extensive survey of several different image encryption schemes of spatial domain for e-health applications. Further, we have elaborated security components, different attacks, novel applications, security methods and different kinds of encryption systems. Finally, we have summarised the notable encryption techniques in tabular form. With the help of our survey, researchers may propose a suitable encryption technique to address the variety of issues for e-health applications.

References

1. Parah SA, Sheikh JA, Ahad F, Loan NA, Bhat GM (2017) Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimed Tools Appl 76:10599–10633
2. Giustini D, Ali SM, Fraser M, Boulos MNK (2018) Effective uses of social media in public health and medicine: a systematic review of systematic reviews. Online J Public Health Informatics 10(2).
3. de Almeida BA, Doneda D, Ichihara MY, BarralNetto M, Matta GC, Rabello ET, Gouveia FC, Barreto M (2020) Personal data usage and privacy considerations in the COVID-19 global pandemic. Cienc. e SaudeColetiva 25:2487–2492. https://doi.org/10.1590/1413-81232020256.1.11792020
4. Wu F, Zhao S, Yu B, Chen Y-M, Wang W, Song Z-G, Hu Y, Tao Z-W, Tian J-H, Pei Y-Y, Yuan M-L, Zhang Y-L, Dai F-H, Liu Y, Wang Q-M, Zheng J-J, Xu L, Holmes EC, Zhang Y-Z (2020) A new coronavirus associated with human respiratory disease in china. Nature 579:265–269
5. https://www.hindustantimes.com/cities/mumbai-news/bombay-hc-junks-bail-plea-based-on- forged- medical-reports-101615348407718.html
6. https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.148238199.1762516747.1577395260-1128561362.1577395260
7. https://www.statista.com/statistics/798564/number-of-us-residents-affected-by-data-breaches/
8. Cao F, Huang HK, Zhou XQ (2003) Medical image security in a HIPAA mandated PACS environment. Comput Med Imaging Graph 27(2–3):185–196. https://doi.org/10.1016/S0895-6111(02)00073-3
9. Dagadu JC, Li JP, Aboagye EO (2019) Medical image encryption based on hybrid chaotic DNA diffusion. Wireless Pers Commun 108(1):591–612
10. Dey S, Ghosh R (2018) A review of cryptographic properties of S-boxes with generation and analysis of crypto secure S-boxes. PeerJ Preprints
11. Chen Y, Tang C, Ye R (2020) Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Processing 167:107286.
12. Singh SP, Bhatnagar G, Singh AK (2021) A New Robust Reference Image Hashing System. In: IEEE Transactions on Dependable and Secure Computing.
13. Su Z, Zhang G, Jiang J (2012) Multimedia security: a survey of chaos-based encryption technology. In: Karydis I (ed) Mutimedia: a multidisiplinary approach to complex issues. InTech, pp 99–124.
14. Kumari M, Gupta S, Sardana P (2017) A survey of image encryption algorithms. 3D Res 8(4):37.
15. Talhaoui, Mohamed Zakariya, Xingyuan Wang, and Mohamed Amine Midoun (2020) Fast image encryption algorithm with high security level using the Bülban chaotic map. J Real-Time Image Process, pp 1–14.
16. Seth B et al (2020) Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies, e4108.
17. Srivastava G et al (2020) Two-stage data encryption using chaotic neural networks. J Intell Fuzzy Syst 38(3):2561–2568
18. Kaur M, Kumar V (2020) A comprehensive review on image encryption techniques. Arch Comput Methods Eng 27(1):15–43
19. Anwar Shamama, Solleti Meghana (2019) A pixel permutation based image encryption technique using chaotic map. Multimedia tools and applications 78(19):27569–27590.
20. Niu Ying, Xuncai Zhang (2020) A novel plaintext-related image encryption scheme based on chaotic system and pixel permutation. IEEE Access 8:22082–22093.
21. Zahmoul, Rim, Ridha Ejbali, Mourad Zaied (2017) Image encryption based on new Beta chaotic maps. Opt Lasers Eng 96:39–49.
22. Wang X, Teng L, Qin X (2012) A novel colour image encryption algorithm based on chaos. Signal Process 92(4):1101–1108
23. Wang X, Liu L, Zhang Y (2015) A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 66:10–18
24. Zhu S, Wang G, Zhu C (2019) A secure and fast image encryption scheme based on double chaotic s-boxes. Entropy 21(8):1–20
25. Zhang X-P, Guo R, Chen H-W, Zhao Z-M, Wang J-Y (2018) Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes. Chin Phys B 27:080701. [CrossRef]
26. Wang X, Çavu¸so ˘glu Ü, Kacar S, Akgul A, Pham V-T, Jafari S, Alsaadi F, Nguyen X (2019) S-box based image encryption application using a chaotic system without equilibrium. Appl Sci 9:781. [CrossRef]
27. Çavu¸so ˘glu, Ü, Kaçar S, Pehlivan I, Zengin A (2017) Secure image encryption algorithm design using a novel chaos based S-box. Chaos Solitons Fractals 95:92–101. [CrossRef]
28. Xu L, Li Z, Li J, Hua W (2016) A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 78:17–25
29. Xiao GZ, Lu MX, Qin L, Lai XJ (2006) New field of cryptography: DNA cryptography. Chin Sci Bull 51(12):1413–1420
30. Wang XY, Zhang YQ, Bao XM (2015) A novel chaotic image encryption scheme using DNA sequence operations. Opt Lasers Eng 73:53–61
31. Wang X, Zhang H-l (2015) A color image encryption with heterogeneous bit-permutation and correlated chaos. Optics Communications 342:51–60
32. Chai X, Zhang J, Gan Z, Zhang Y (2019) Medical image encryption algorithm based on Latin square and memristive chaotic system. Multimed Tools Applications 78(24):35419–35453
33. Ahmad J, Hwang SO (2016) A secure image encryption scheme based on chaotic maps and affine transformation. Multimed Tools Appl 75(21):1–26
34. Anees A, Ahmed F (2014) Chaotic substitution for highly auto correlated data in encryption algorithm. Commun Nonlinear Sci 19(9):3106–3118
35. Chen X, Hu CJ (2017) Adaptive medical image encryption algorithm based on multiple chaotic mapping. Saudi J Biol Sci 24(8):1821–1827
36. Ibrahim S, Alhumyani H, Masud M, Alshamrani SS, Cheikhrouhou O, Muhammad G, Abbas AM (2020) Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps. IEEE Access 8:160433–160449
37. Banik A, Shamsi Z, Laiphrakpam DS (2019) An encryption scheme for securing multiple medical images. J Inf Secur Appl 49, Art. no. 102398.
38. Yang F, Mou J, Sun K, Chu R (2020) Lossless image compression-encryption algorithm based on BP neural network and chaotic system. Multimed Tools Appl 79(27):19963–19992
39. Singh LD, Singh KM (2015) Image encryption using elliptic curve cryptography. Proc Comp Sci 54:472–481
40. 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
41. Behnia, Sohrab, et al. (2013) Image encryption based on the Jacobian elliptic maps. J Syst Softw 86(9):2429–2438.
42. Hafsa A, Sghaier A, Malek J, Machhout M (2021) Image encryption method based on improved ECC and modified AES algorithm. Multimedia Tools Appl, pp 1–33.
43. Bentoutou Y, El Bensikaddour H, Taleb N, Bounoua N (2020) An improved image encryption algorithm for satellite applications. Adv Space Res 66(1):176–192. https://doi.org/10.1016/j.asr.2019.09.027

44. Laiphrakpam DS, Khumanthem MS (2017) Medical image encryption based on improved ElGamal encryption technique. Optik 147:88–102. https://doi.org/10.1016/j.ijleo.2017.08.028
45. Lin Z, Liu J, Lian J, Ma Y, Zhang X (2019) A novel fast image encryption algorithm for embedded systems. Multimed Tools Appl 78:20511–20531. https://doi.org/10.1007/s11042-018-6824-5
46. Liu J, Ma Y, Li S, Lian J, Zhang X (2018) A new simple chaotic system and its application in medical image encryption. Multimed Tools Appl 77:22787–22808. https://doi.org/10.1007/s11042-017-5534-8
47. Zhang X, Wang X (2018) Digital image encryption algorithm based on elliptic curve public cryptosystem. IEEE Access 6:70025–70034
48. Singh LD, Singh KM (2015) 'Image encryption using elliptic curve cryptography.' ProcediaComput Sci 54:472–481
49. Laiphrakpam DS, Khumanthem MS (2018) A robust image encryption scheme based on chaotic system and elliptic curve over finite field. Multimedia Tools Appl 77(11):8629–8652
50. Zhu G, Zhang X (2008) Mixed image element encryption algorithm based on an elliptic curve cryptosystem. J Electron Imag 17(2):1–5
51. 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
52. Sun Shuliang (2018) Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules. Optical En 56(11):116117.
53. Liu Z, Xia T, Wang J (2018) Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and MenezesVanstone elliptic curve cryptosystem. Chin Phys B 27(3):1–16
54. Dawahdeh ZE, Yaakob SN, bin Othman RR (2018) A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. J King Saud Univ Comput Inform Sci 30(3):349–355
55. Benssalah, M., & Rhaskali, Y. (2020). A Secure DICOM Image Encryption Scheme Based on ECC, Linear Cryptography and Chaos. In: 2020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP). IEEE, New York, pp. 131–136
56. Akram B, Muhammad T, Sofiane K, Wei X (2019) Novel medical image encryption scheme based on chaos and dna encoding. IEEE Access 7:36667–36681.
57. Hua Z, Yi S, Zhou Y (2018) A new plaintext-related image encryption scheme based on chaotic sequence. Signal Process 144:134–144
58. Hua Z, Zhou Y (2017) Design of image cipher using block-based scrambling and image filtering. Inf Sci 396:97–113
59. Shang M, Yan Z, Zeguo Y, Jianhao H, Xin L (2019) A new plaintextrelated image encryption scheme based on chaotic sequence. IEEE Access 7:30344–30360.
60. Hayat U, Azam NA (2019) A novel image encryption scheme based on an elliptic curve. Signal Process 155:391–402
61. Wu J, Liao X, Yang B (2017) Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. Signal Process 141:109–124
62. Rehman A, Khan JS, Ahmad J, Hwang SO (2016) A New Image Encryption Scheme Based on Dynamic S-Boxes and Chaotic Maps, 3D Res7:7
63. Tong XJ, Zhang M, Wang Z (2016) A joint color image encryption and compression scheme based on hyper-chaotic system. Nonlinear Dyn 84(4):2333–2356
64. Shankar K, Eswaran P (2016) An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm. In: Artificial intelligence and evolutionary computations in engineering systems. Springer, New Delhi, pp. 705–714.
65. Shankar K, Eswaran P (2015) ECC based image encryption scheme with aid of optimization technique using differential evolution algorithm. Int J ApplEng Res 10(55):1841–1845
66. Ibrahim S, Alharbi A (2020) Efficient image encryption scheme using Henon Map, dynamic S-boxes and elliptic curve cryptography. IEEE Access 8:194289–194302
67. Wang X, Guan N, Zhao H, Wang S, Zhang Y (2020) A new image encryption scheme based on coupling map lattices with mixed multichaos. Sci Rep 10(1):9784. https://doi.org/10.1038/s41598-020-66486-9
68. Ismail, SM, Said LA, Radwan AG, Madian AH, Abu-ElYazeed MF (2020) A novel image encryption system merging fractional-order edge detection and generalized chaotic maps. Signal Process 167, Art. no. 107280. https://doi.org/10.1016/j.sigpro.2019.107280.
69. Laiphrakpam DS, Khumanthem MS (2018) A robust image encryption scheme based on chaotic system and elliptic curve over finite field. Multimedia Tools and Applications 77(7):8629–8652
70. Mushin S, Nasharuddin Z (2015) Decomposition by binary codes-based speedy image encryption algorithm for multiple applications. IET Image Process 9(5):413–423
71. Mariusz D, Michal P, Roman R (2015) A new quaternion-based encryption method for DICOM images. IEEE Trans Image Process 24(11):4614–4622
72. Akram B, Ahmed AAE, Safya B (2016) A novel image encryption scheme based on substitution permutation network and chaos. Signal Process 128:155–170
73. Liu Y, Tang J, Xie T (2014) Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map. Journal of Optics and Laser Technology 60:111–115
74. Jain A, Rajpal N (2016) A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. Multimedia Tools Appl 75(10):5455–5472
75. Suri S, Vijay R (2019) A synchronous intertwining logistic map-DNA approach for color image encryption. J Ambient Intell Humaniz Comput 10(6):2277–2290
76. Khan JS, ur Rehman A., Ahmad J, Habib Z (2015) A new chaos-based secure image encryption scheme using multiple substitution boxes. In: 2015 Conference on information assurance and cyber security (CIACS), pp. 16–21. IEEE, New York
77. Khan FA, Ahmed J, Khan JS, Ahmad J, Khan MA (2017) A novel image encryption based on Lorenz equation, Gingerbreadman chaotic map and S 8 permutation. J Intell Fuzzy Syst 33(6):3753–3765
78. Zhang X, Zhou Z, Niu Y (2018) An image encryption method based on the Feistel network and dynamic DNA encoding. IEEE Photonics J 10(4):1–14
79. Liu H, Wang X, Kadir A (2012) Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 12(5):1457–1466
80. Lian S, Sun J, Wang Z (2005) A block cipher based on a suitable use of the chaotic standard map. Chaos Solitons Fractals 26(1):117–129
81. Azimi Z, Ahadpour S (2020) Color image encryption based on DNA encoding and pair coupled chaotic maps. Multimedia Tools Appl 79(3):1727–1744
82. ur Rehman A, Liao X, (2019) A novel robust dual diffusion/confusion encryption technique for color Image based on Chaos, DNA and SHA-2. Multimed Tools Appl 78:2105–2133
83. Wu X, Kan H, Kurths J (2015) A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. Appl Soft Comput 37:24–39

84. Wu J, Liao X, Yang B (2018) Image encryption using 2D Hénon-Sine map and DNA approach. Signal Process 153:11–23
85. Niyat AY, Moattar MH, Torshiz MN (2017) Color image encryption based on hybrid hyper-chaotic system and cellular automata[J]. Opt Lasers Eng 90:225–237
86. Li C, Luo G, Qin K et al (2017) An image encryption scheme based on chaotic tent map[J]. Nonlinear Dyn 87(1):127–133
87. Wolfram S (1983) Statistical mechanics of cellular automata. Rev Mod Phys 55(3):601–644
88. Naskar PK, Bhattacharyya S, Nandy D, Chaudhuri A (2020) A robust image encryption scheme using chaotic tent map and cellular automata. Nonlinear Dyn 100:2877–2898
89. Luo Y, Zhou R, Liu J, Cao Y, Ding X (2018) A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map. Nonlinear Dyn 93(3):1165–1181
90. Ye G, Pan C, Huang X, Mei Q (2018) An efficient pixel-level chaotic image encryption algorithm. Nonlinear Dyn 94(1):745–756
91. Enayatifar R, Abdullah AH, Isnin IF (2014) Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt Lasers Eng 56:83–93.
92. Mondal B, Singh S, Kumar P (2019) A secure image encryption scheme based on cellular automata and chaotic skew tent map. J Inform Security Appl 45:117–130
93. Li Y, Wang C, Chen H (2017) A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Opt Lasers Eng 90:238–246
94. Fu C, Lin Bb, Miao Ys, Liu X, Chen Jj (2011) A novel chaos-based bit-level permutation scheme for digital image encryption. Opt Commun 284(23):5415–5423.
95. Tong XJ, Wang Z, Zhang M, & Liu Y (2013) A new algorithm of the combination of image compression and encryption technology based on cross chaotic map. Nonlinear Dyn 72(1):229–241
96. Babaei A, Motameni H, Enayatifar R (2020) A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence. Optik 203: 164000.
97. Niyat AY, Moattar MH, Torshiz MN (2017) Color image encryption based on hybrid hyper-chaotic system and cellular automata. Opt Lasers Eng 90:225–237
98. Xingyuan W, Yuanyuan Z, Huili Z, Kang G (2016) A novel color image encryption scheme using alternate chaotic mapping structure. Opt Lasers Eng 82:79–86
99. Xingyuan W, Hui-li Z (2015) A color image encryption with heterogeneous bitpermutation and correlated chaos. Opt Commun 342:51–60
100. Wu X, Kan H, & Kurths J (2015) A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. Applied Soft Computing 37:24-39.
101. Chai X, Gan Z, Yang K, Chen Y, Liu X (2017) An image encryption algorithm based on the memristivehyperchaotic system, cellular automata and DNA sequence operations. Signal Process Image Commun 52:6–19
102. Wang Y, Wong KW, Liao X, Chen G (2011) A new chaos-based fast image encryption algorithm. J Appl Soft Comput 11:514–522
103. Xiao D, Liao XW (2009) Analysis and improvement of a chaos-based image encryption algorithm. Chaos SolitonsFract 40:2191–2199
104. Zhang S, Xiao D (2014) An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Commun Nonlinear Sci Numer Simul 19:74–82
105. Kumar A, Raghava NS (2021) An efficient image encryption scheme using elementary cellular automata with novel permutation box. Multimedia Tools Appli, pp 1–24
106. Roy S, Rawat U, Sareen HA, Nayak SK (2020) IECA: an efficient IoT friendly image encryption technique using programmable cellular automata. J Ambient IntellHumanizComput 11:5083–5102. https://doi.org/10.1007/s12652-020-01813-6
107. Li C, Luo G, Qin K, Li C (2016) An image encryption scheme based on chaotic tent map. Nonlinear Dyn 87(1):127–133
108. Ping P, Wu J, Mao Y, Xu F, Fan J (2018) Design of image cipher using life-like cellular automata and chaotic map. Signal Process 150:233–247
109. Souyah, Amina, Kamel Mohamed Faraoun (2016) An image encryption scheme combining chaos-memory cellular automata and weighted histogram. Nonlinear Dyn 86(1):639–653.
110. Chai X, Gan Z, Yang K, Chen Y, Liu X (2017) An image encryption algorithm based on the memristivehyperchaotic system, cellular automata and DNA sequence operations. Signal Process Image Commun 52:6–19
111. Mohamed AG, Korany NO, El-Khamy SE (2021) New DNA coded fuzzy based (DNAFZ) S-boxes: application to robust image encryption using hyper chaotic maps. IEEE Access 9:14284–14305
112. Hosseinzadeh R, Zarebnia M, Parvaz R (2019) Hybrid image encryption algorithm based on 3D chaotic system and choquet fuzzy integral. Opt Laser Technol 120:105698.
113. Kadir A, Hamdulla A, Guo W (2014) Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. Optik 125(5):1671–1675
114. Wu X, Wang D, Kurths J, Kan H (2016) A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. Inform Sci 349:137–153
115. Seyedzadeh SM, Norouzi B, Mirzakuchaki S (2014) RGB color image encryption based on Choquet fuzzy integral. J Syst Softw 97:128–139
116. Bakhshandeh A, Eslami Z (2013) An authenticated image encryption scheme based on chaotic maps and memory cellular automata. Opt Lasers Eng 51:665–673
117. El-Latif AAA, Li L, Wang N, Han Q, Niu X (2013) A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. Signal Process 93:2986–3000
118. Liu H, Wang X, Kadir A (2013) Color image encryption using Choquet fuzzy integral and hyper chaotic system. Optik 124:3527–3533
119. Wang J, Zheng N, Chen B, Principe JC (2017) Associations among image assessments as cost functions in linear decomposition: MSE, SSIM, and Correlation Coefficient. arXiv:1708.01541