International Journal of Information Security
https://doi.org/10.1007/s10207-022-00588-5

SURVEY

Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains

Unsub Zia[1] · Mark McCartney[1] · Bryan Scotney[1] · Jorge Martinez[1] · Mamun AbuTair[1] · Jamshed Memon[1] · Ali Sajjad[2]

Abstract
Chaos-based cryptosystems have been an active area of research in recent years. Although these algorithms are not standardized like AES, DES, RSA, etc., chaos-based cryptosystems like Chebyshev polynomials can provide additional security when used with standard public key cryptosystems like RSA and El-gamal. Standard encryption algorithms such as AES have always been the primary choice, but when it comes to image or video encryption, many researchers recommend chaos-based encryption techniques due to their computational efficiency. This paper presents a survey on the most up-to-date chaos-based image encryption techniques and classifies them into spatial, temporal and spatiotemporal domains for better understanding. The significant improvements in the field of image encryption are discussed. In addition, comparative analysis is performed to validate the evaluation matrices for quantifying the encryption algorithms' security and performance in recent papers.

Keywords Chaotic maps · Spatial domain · Transform domain · Spatiotemporal domain · Image encryption

1 Introduction

The rapid progression and adoption of new digital communication and network technologies have shown enormous potential in improved data storage and electronic data exchange across the Internet. However, it is equally important to protect the confidential information and that is why network security and data integrity have always remained issues of significant importance. This has led scientists to take appropriate safety measures to gain visibility and prevent security vulnerabilities. The multimedia shared and stored over the Internet is mostly in the form of images. Hence, the confidentiality and authenticity of digital images are ensured by means of image encryption.

Image encryption uses a mathematical algorithm to convert the original image into a form that is hard to interpret; thereby increasing resistance against security attacks, for example, brute force [1], statistical [2] and differential attacks [3]. Image encryption finds its applications in many fields such as medical imaging, telemedicine, business, biometric authentication and military communication. Numerous image encryption techniques have been presented to meet these security constraints, including digital watermarking techniques [4], image scrambling methods [5], image steganography [6] and image cryptography [7]. In the last few decades, the exploitation of chaos in cryptography has shown a surge in interest due to its fundamental property of sensitivity to initial conditions leading to data sets, which while deterministic, give the appearance of randomness. Chaos-based cryptographic models have been used to develop novel methods to design efficient image encryption systems, exhibiting exceptionally good characteristics

✉ Unsub Zia
zia-smu@ulster.ac.uk

Mark McCartney
m.mccartney@ulster.ac.uk

Bryan Scotney
bw.scotney@ulster.ac.uk

Jorge Martinez
j.martinez-carracedo@ulster.ac.uk

Mamun AbuTair
m.abu-tair@ulster.ac.uk

Jamshed Memon
j.memon@ulster.ac.uk

Ali Sajjad
ali.sajjad@bt.com

1 Ulster University, Northern Ireland, UK

2 Applied Research, British Telecom, Ipswich, UK

Published online: 07 April 2022

in many aspects regarding speed, cost, computational power, computational overhead, complexity, vulnerability, etc.

This paper presents a theoretical survey of recent research papers from years 2016-2021 that published chaos-based image encryption schemes. Our survey classifies the chaos-based encryption schemes as spatial, temporal and spatiotemporal domains. The motivation behind this segregation was to group the advances in chaos-based image encryption schemes which would make it convenient for readers from beginners to expert in this field in targeting their relevant area of interest. In this paper, a roadmap has been given on the working of chaos-based cryptosystems for digital data, i.e., images and videos. A thorough comparison between traditional and chaos-based cryptographic schemes has also been provided. Considering different types of attack models, a summary of recent cryptanalytic attacks has been mentioned. Finally, under every group classified a comparison matrix has been provided to evaluate the type of attack models used to validate the proposed algorithms.

The remaining structure of this paper is as follows: An overview of chaos theory is presented in Sect. 2. Section 3 describes image encryption and its relation with chaos-based cryptography. Section 4 comprises related work. Evaluation parameters are discussed in Sect. 5. Section 6 represents the survey of image encryption in spatial, temporal and spatiotemporal domains. The concluding remarks are presented in Sect. 7.

2 Image encryption

The rise of interest in chaotic dynamics in the 1960s and 70s can be linked to the rise of the digital computer. Increased computational power allowed a wide range of nonlinear systems to be investigated for the first time. Key features of such systems are the existence of so-called strange attractors and the divergent nature of neighboring trajectories on such attractors. These features combine to give rise to time series which, though fully deterministic, give the appearance of being random. It is this apparent randomness which makes chaotic systems useful for encryption.

In cryptography, encryption is defined as the process of converting useful information into an unrecognizable form to protect it from unauthorized access. The image content occupies vital characteristics like high redundancy, space, capacity and correlation among the bit pixels, that demands some kind of encryption technique where the primary purpose is to securely transfer the image [8]. In other words, an encryption algorithm is used to transform the plain image into a cipher image, i.e., the useful actual information is obscured. The encrypted image can then be securely transmitted over the network; therefore no unauthorized person is able to decrypt the image. Hence, at the receiving end of the network, a decryption algorithm is utilized to decipher the cipher image into the original image. Moreover, in the process of image encryption, the original image is incorporated with a key to encode the image, whereas, for the image decryption process, a decryption algorithm is used to decode the encrypted image in order to recover the original image. The keys used in image encryption and the decryption process are categorized into two main types, i.e., symmetric and asymmetric keys (shown in Fig. 1). In symmetric key (private key) cryptography, the same key is used during the encryption and decryption processes, whereas in the asymmetric key (public key) cryptography; separate keys are used, i.e., a pair consisting of a private key and a public key are required together for encryption and decryption.

2.1 Symmetric key cryptography

Symmetric key cryptography is also known as private key or secret key encryption, as it requires only a single key for encryption as well as decryption of the image [9]. The sender encrypts the image with a private key which is then sent

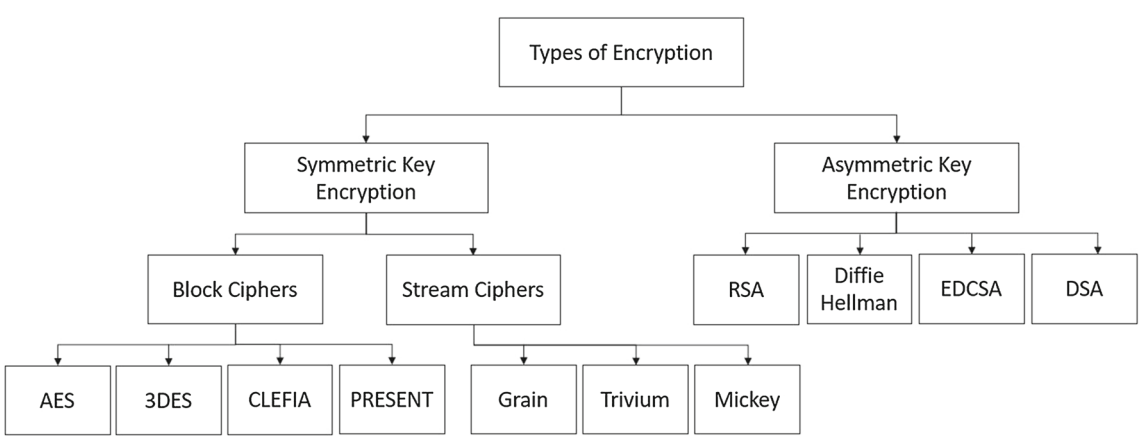

Fig. 1 Types of image encryption algorithms

over the transmission media to the receiver. At the receiving end, the encrypted image is decrypted using the same private key that was used to encrypt the image. Symmetric key cryptography has a computationally low cost and requires fewer resources. As shown in Fig. 1, symmetric encryption can further be segregated into Block and Stream Ciphers. Stream ciphers usually work by encrypting single bits of data at a time. They tend to perform encryption faster than block ciphers and are lightweight in nature, some examples of lightweight stream ciphers include Grain [10], Trivium [11] and Micky [12]. On the other hand, block ciphers encrypt data by encrypting a chunk of data (block) of chosen size. A block cipher uses an initialization vector to add extra layer of security against brute force attacks. Some examples of block ciphers are Advanced Encryption Standard (AES) [13], Triple Data Encryption Standard (3-DES) [14], CLEFIA [15] and PRESENT [16].

2.2 Asymmetric key cryptography

Asymmetric cryptography is also known as public key encryption, unlike symmetric key encryption public key encryption uses two separate keys for encrypting and decrypting the image [17]. Each sender and receiver possess a pair of keys known as public and private keys. The private key is not shared with anyone, while the public key is shared with the sender. The public key is used by the sender to encrypt the image, which is then sent to the receiver. The receiver then decrypts the image with their private key. Asymmetric cryptography has a computationally high cost and requires more resources. Examples of asymmetric key cryptographic algorithms include: Digital Signature Algorithm (DSA) [18], ECDSA [19], Rivest–Shamir–Adleman (RSA) [20] and Diffie–Hellman [21].

The image encryption can be applied in various domains namely, i.e., spatial, transform and spatiotemporal domains. The classification of image encryption schemes is depicted in Fig. 3. These image encryption techniques are discussed thoroughly in the later subsections.

2.3 Chaos-based image encryption

In recent years, researchers have been keenly observing the close correspondence between chaotic systems and cryptography, in order to design chaos-based cryptographic algorithms for secure image encryption and communication in the presence of an attacker [22]. Hence, chaotic cryptography is defined as a proportionate blend of chaos theory and the science of cryptography. The main difference is that chaotic systems are defined on real numbers, whereas cryptosystems are mapped on a finite set of integers. Traditional ciphers such as AES and DES are suitable for text but not for image encryption, due to the repetitive information pixels depict in similar images. Chaos-based encryption techniques rectify this issue by producing evenly diffused random keys that hide the image information in the cipher images [23].

Nonetheless, these two scientific notions are closely correlated and thus provide a good amalgamation of improved performance, combined with a high level of security and various useful practical applications such as pseudo-random numbers to generate stream ciphers [24] and block ciphers [25], secure communications [26], image encryption [27] and video encryption [28]. Chaotic systems are considered as a set of dynamical equations which vary with time, and time can either be discrete or continuous [29]. The unique features of chaotic systems such as determinacy, ergodicity and sensitivity to initial condition, make it a worthwhile choice for designing cryptosystems, as these properties are analogous to the confusion and diffusion properties of a good cryptosystem. With the continuous development in the field of image encryption and cryptanalysis, several chaotic image encryption algorithms and improved methods have been proposed that have potential to defeat various security threats.

The primary, and perhaps most challenging step is the selection of chaotic maps in designing the chaos-based algorithm [30]. The swiftness and robustness of a cryptosystem are one of the most important prerequisites while designing an efficient cryptographic algorithm. Therefore, researchers initiated the design using simpler chaotic maps, such as the tent map and the logistic map, which have small key space, which results in inadequate security. Later, with further development in the design of encryption algorithms, chaotic maps with higher dimensions were applied which resulted in fast, highly secure and improved quality of the cryptosystem. Several chaotic maps have been studied for image encryption such as the Henon map [31], Tinkerbell map [32], Logistic map 1D [33], Logistic map 2D [34], Tent map [35] and a 5D Hyper-chaotic map [36].

2.4 Chaos-based image cryptosystem architecture

The chaos-based image cryptosystem architecture generally comprises two phases; the confusion phase and the diffusion phase. The block diagram of the architecture is shown in Fig. 2. The confusion phase is also known as the pixel permutation, in which the pixel positions are rearranged over the whole image while the pixel values remain unchanged, converting the image into an unidentifiable form. Afterward, the diffusion phase is applied, as the former phase is not secure enough and can be easily hacked by an attacker. Hence, when the diffusion phase is executed with the help of a chaotic map, the values of the pixels of the whole image are changed consecutively by the sequence generated from the chaotic systems. Multiple iterations of the confusion–diffusion process are performed until a satisfactory level of security is attained.

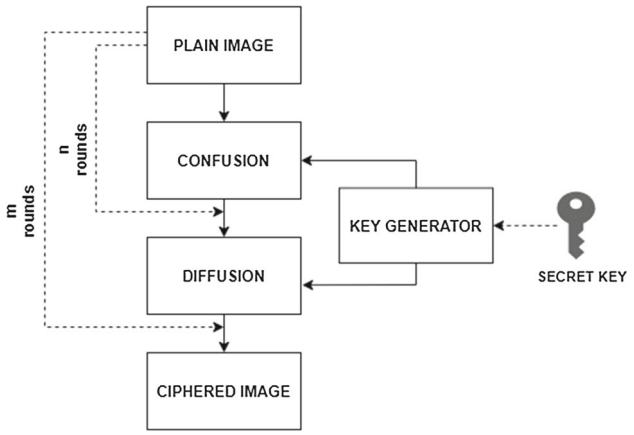

Fig. 2 Chaos-based image cryptosystem architecture

2.5 Conventional cryptography vs chaos-based cryptography

The continuous progression of multimedia technology has enhanced the accessibility of data in digital form such as image, video and audio by means of the Internet over public networks. Thus, network security has become a challenging issue in order to protect the tremendous amount of data generated over the Internet every day. Images possess certain features which are different from textual data for instance, high redundancy of data, scattered information, large size data, strong correlation among adjacent pixels [37] and bulk data capacity [38]. The basic working of image encryption is based on conversion of the two-dimensional (2D) image into a one-dimensional (1D) data stream and then encryption using textual-based cryptosystems. In text-based encryption, the decrypted text should always be identical to the original text, i.e., in order to decrypt the original message each bit must be recovered very precisely. However, there is no such requirement for digital multimedia applications, since a minute change in the attribute of the pixel of an image does not drastically degrade the quality of the image. Moreover, pixel data of an image comprises intensity values, which fall in the range [0, 255]. When using conventional algorithms to convert images, the encrypted value for a pixel is set as per the encryption key used, and as the pixel value repeats in an image multiple times (data redundancy), that value could easily be guessed by the adversary.

An encryption algorithm which is considered best is one which takes less computational time without compromising the security. Unfortunately, most conventional cryptographic schemes such as AES, DES, TDES, IDEA, RSA are typically designed to protect textual data more efficiently [39]. These techniques are not suitable for real-time image encryption, due to the inherent properties of images. Further, these methods require high computational resources and are complex to implement when undertaken by commercial software.

On the other hand, the chaos-based cryptographic methods provide several advantages such as increased flexibility, high security, less computational overheads, less computing power and ease of implementation. Also, in the majority of chaos-based encryption schemes, confusion and diffusion of the encryption key are performed at pixel level [40–42]. These characteristics make them a promising alternative to conventional cryptographic algorithms for encrypting and decrypting a wide range of digital data. Additionally, a variety of chaotic maps are available that can be incorporated in chaos-based cryptosystems, which in turn increase the options to choose from. Thus, chaotic cryptography has gained more attention than conventional methods because of its lower mathematical complexity and better security.

2.6 Attack model for cryptanalysis

A cryptosystem is considered to be secure if it is able to resist most type of known cryptanalytic attacks [43]. In general, a successful cryptanalysis on a cryptosystem means that the attacker is able to retrieve the original data without having any knowledge of the secret key used. A brief description of the four classical cryptographic attacks is given below:

1. **Chosen-plaintext attack:** In this attack model, the attacker selects one or more plaintexts to be encrypted and obtains the corresponding ciphertexts. The main purpose of the attack is to gain additional knowledge which lessens the security of the encryption scheme. This attack is one of the potential classical attacks.
2. **Chosen-ciphertext attack:** In this attack model, the cryptanalyst cleverly selects the ciphertext and acquires the associated plaintext.
3. **Ciphertext-only attack:** In this case, the attacker has access only to a collection of ciphertexts of several plaintexts and thus has less information. The cryptanalyst attempts to analyze them in order to deduce the key and if the key is deduced with this poor information then the cryptographic algorithm is fairly insecure.
4. **Known-plaintext attack:** In this case, the cryptanalyst has the access to not only the plaintext but ciphertext of those plaintext. The attacker has the liberty to deduce the key by using the pairs of plaintext and ciphertext.

2.7 Cryptanalysis

To date, a variety of image encryption techniques have been proposed in the literature. However, the cryptanalysis of the conventional and modern chaos-based techniques shows that many of these methods are proven to be vulnerable and thus cannot be applied to secure communications [44–47]. For instance, Eli Biham et al. developed a known attack capable of breaking the full 16-round DES using several

iterative characteristics out of the 2^{56} possible ASCII plaintexts [48]. The scheme obtained 2^{36} ciphertext during the data collection stage from 2^{47} plaintexts using simple bit repetition criteria in 2^{37} time. Moreover, a successful cryptanalysis was performed by Alani [49]. The scheme adopts a neural network architecture. The work claims to be capable of predicting the plaintexts from ciphertexts of DES and triple DES (3-DES) by learning from around 2^{11} and 2^{12} plaintext-ciphertext pairs, respectively. In another attack instance [50], also known as the Fluhrer, Mantin and Shamir Attack scheme, in which the authors exposed the cryptanalytic significance of RC4 by presenting several weaknesses of the key scheduling algorithm. The state and output bits are determined by extracting information from a small number of key bits from a pool of weak keys. A related key attack on AES-192 and AES-256 was presented by Biryukov et al. [51]. The attack strategy was based on the idea of finding local collisions in the block cipher along with boomerang switching techniques to gain free rounds in the middle. However, these attacks are of theoretical interest only and have no significance practically. Thus, AES remains a secure cipher for practical applications. Similarly, the literature presents an extensive trend of cryptanalytic attacks performed on chaos-based techniques. Li et al. [52] performed successful cryptanalysis of a chaotic permutation and diffusion-based image encryption scheme [53] and reveal its vulnerability against chosen-plaintext attack. In the presented work, an all-zero image was used for breaking the original diffusion phase and plaintext images used for cracking the original permutation phase. Similarly, Dou et al. [54] successfully cracked the color image encryption scheme using the combination of the 1D chaotic map with chosen-plaintext attack [33]. The Pak scheme [33] proposed an efficient image encryption system of linear–nonlinear–linear structure based on total shuffling, which was cryptanalyzed by Wang et al. [45]. The presented work could break the diffusion and permutation matrices of Pak's scheme and developed an enhanced image encryption algorithm by integrating global plain information. An efficient image encryption scheme [55] based on an improved 1D chaotic map was subsequently broken by Li et al. in [56]. The Fridrich algorithm [57] based on two-dimensional Baker mapping for efficient chaotic image encryption, was cryptanalyzed by Solak et al. in [47] using chosen-ciphertext attack. The authors built a causality-based tree to break permutation matrix. Inspired by the work presented in [47], Xie et al. [58] exposed the algebraic weaknesses of the Fridrich's scheme [57] which made it vulnerable against chosen-ciphertext attacks. The paper [59], successfully investigated the loophole of symmetric key image encryption using the chaotic Rossler system [60] and found that it was breakable. Diab et al. in [61] proposed an attack model to break Chen's image encryption scheme [62] by exploiting different sets of plain/cipher images. The scheme proposed by Feki et al. [63], using a modified Henon map was completely broken by Alvarez et al. [64] due to the lack of detailed security analysis.

3 Related work

This section covers a survey of the most recently published chaos-based image encryption techniques. Several image encryption algorithms have been proposed which vary in terms of effectiveness and robustness. In this paper, chaos-based image encryption techniques are discussed and are classified into spatial domain, temporal domain and spatiotemporal domain as represented in Fig. 3.

A theoretical survey and analysis of the above-mentioned algorithms are discussed and evaluated on the basis of various performance metrics such as number of pixel change rate (NPCR), unified average changing intensity (UACI), key analysis (KA), histogram analysis (HA), coefficient

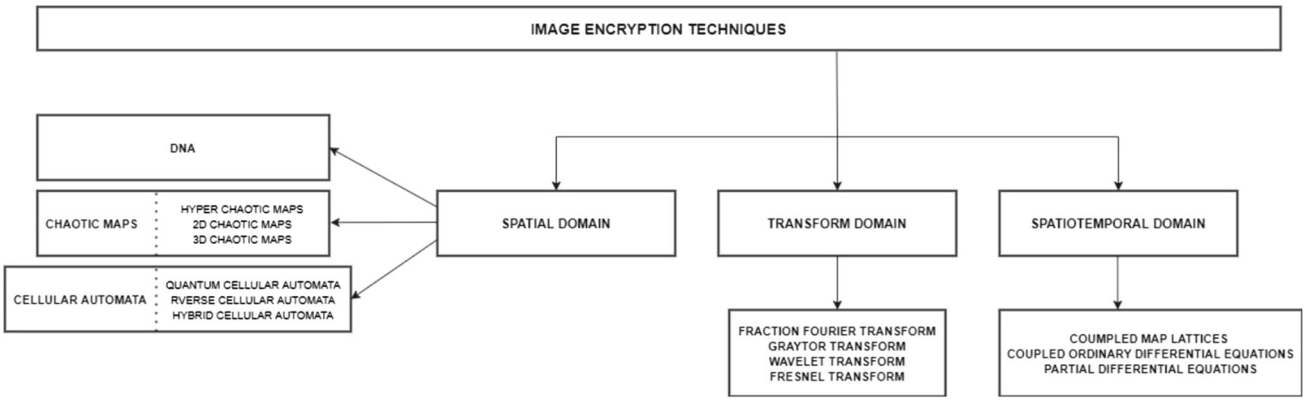

Fig. 3 Classification of image encryption techniques

correlation (CC), information entropy (IE), noise attack (NA). The literature review of the most recent papers is presented as follows:

A survey of ten conventional and five chaos-based image encryption techniques [65–78] has been presented recently [79]. The comparison performed was based on different evaluation metrics such as statistical, differential and quantitative attack analysis. In order to evaluate their effectiveness, experiments were performed on MATLAB-2015. The results exhibited resistance of the chaotic schemes against statistical attacks. The encrypted images were highly scrambled with a consistent histogram distribution and lower correlation coefficient values in all the three directions (horizontally, vertically and diagonally). Similarly, the chaotic schemes were also resistant to differential attacks due to high sensitivity to pixel and key change values. All the techniques showed significantly large key space and high information entropy values, hence providing resistance against brute force attacks. However, the conventional schemes proved to be less resistant against differential attacks as they showed poor pixel change sensitivities. In addition, they concluded that image encryption using chaotic scheme 15, RC4 [80] and AES [81] proved to be computationally efficient and had faster execution times as compared to other encryption algorithms being considered.

In another study, digital image encryption and decryption schemes are discussed [82]. These schemes exploit multiple chaotic map methods to improve the existing algorithms providing a high level of security to image data. The sensitivity of key size, key space, computational time and correlation coefficient are used to validate the protection of images. However, the techniques and methods reviewed by the authors are somewhat outdated and the outcomes of the paper are not based on analysis of latest methodologies.

Monjul Saika et al. [83] published a brief survey of chaotic map-based image encryption in the spatial domain. The authors stated that chaos-based image encryption is most suitable for encryption processes due to their high sensitivity to initial conditions. Furthermore, a general overview of chaotic maps and three different phases (selection of chaotic maps, confusion and diffusion of images) have been discussed and elaborated with the help of examples, ensuring the security of the system by providing protection to digital data against unauthorized access. The drawback of this paper is that the authors have not discussed or reviewed any research papers in the field of the spatial domain and have restricted themselves with basic chaotic maps and phases.

The authors in [84] attempt to survey image encryption and steganography. The research papers [85–102] studied in this paper encompass various image encryption and steganography techniques, used to ensure data integrity and security. The encryption techniques were used to convert the input image into a cipher image whereas stenography techniques were used to improve the security of the system. In this way, the encryption key is kept hidden in the cipher image without changing or modifying the information in it. This reduces the transmission time of key between the sender, receiver and third party distributor. Moreover, the cost of key distribution is also minimized.

An extensive analysis of several image encryption methods has been published in [103]. This paper described four image encryption techniques namely spatial, compressive sensing, optical and transform domain. The paper also performed a broad comparison of these techniques on the basis of different performance metrics such as UACI, histogram analysis, key analysis, NPCR, noise, coefficient correlation, information entropy and encryption speed. The paper mainly focused on challenges associated with digital image encryption techniques such as computational time, security risks and tuning parameters. In addition, the author discussed considerable achievements using meta-heuristic-based image encryption schemes to overcome the above-mentioned challenges. According to research, these meta-heuristic techniques suffer from premature convergence, sticking in local optima and poor convergence speed. The paper concluded that there is a significantly more work that can be done on image encryption based on meta-heuristic methods and various imaging systems such as underwater, remote sensing, multi-spectral imaging and 3D imaging systems.

The authors in [104] performed an analysis on some traditional and modern hybrid encryption techniques with post-quantum methods, such as DES–RSA [105] , 3D chaotic map techniques [106], RSA-based singular cubic curves, RSA based on ECC with AVK [107], Joint Compression and Encryption (JCE) [108] and Blowfish [109]. These encryption techniques and algorithms were compared on the basis of various performance metrics such as execution time, bit sizes, key length, possible keys and level of security. The comparison made in this paper showed that the combination of RSA-based singular cubic curve with AVK meant the time complexity was reduced to a minimal level and provided high functionality to the system in terms of security. However, in double encryption the technique appeared to be suitable for only small content. Similarly, the blend of AES–ECC hybrid techniques [110] showed a reduction in both space and time complexities as compared to other algorithms. The hybrid approach proved to be capable of providing more security. On the other hand, quantum encryption performed better in terms of key distribution also less resources were needed. Experiments concluded that Blowfish outperformed other algorithms (DES, IDEA and AES) in the analysis presented in this paper and that in comparison to other current techniques compression showed far better results in performance of encryption execution time.

Younes et al. [111] presented a general introduction to image encryption and cryptography along with a brief

survey on recent techniques of image encryption that provide security to confidential data. These image encryption techniques exhibit considerable protection of sensitive information. Hence these techniques can be further enhanced to develop new techniques to reduce the risk of data security and integrity.

In another survey, the authors highlighted the issue of co-evolution of security risks to digital images with the development of technology [112]. The authors have also discussed and analyzed ten papers dealing with image encryption techniques to encourage further improvement in the performance of these encryption methods, making them highly resistant against security attacks. The methods discussed above have used different combinational approaches to reduce the security risks by embedding and encrypting the original image and then sending it to the receiver. However, this approach still lags behind due to slower transfer time from sender to receiver. Moreover, the compression and segmentation techniques could not resolve this problem as compression techniques were not erasable or reversible whereas segmentation techniques take much longer time in the transmission of large data. Based on the survey of techniques presented in the paper, the author concluded that chaos-based encryption techniques are more secure and simple due to low consumption time during the process of encryption and decryption of a large image.

In [113], different image encryption techniques have been reviewed and analyzed in the context of parameters used to prove the efficiency of security algorithms. Different aspects of image security in general and encryption in particular are discussed. Bhat et al. have presented a general overview of image security in multimedia data and have reviewed various image encryption techniques in the context of security parameters to validate the efficacy of these algorithms to ensure the privacy and integrity of images. The analysis of the encryption techniques showed that image encryption is different from other multimedia encryption because of the large data capacity and strong correlation among the pixels which makes conventional encryption schemes unsuitable. Hence, before design, any image encryption algorithm must be analyzed against security constraints to ensure the credibility of the algorithms.

Ratheesh et al. [114] have reviewed 13 papers on different characteristics of image encryption algorithms and evaluated the performance of these algorithms on the basis of various parameters such as computational time, correlation coefficient, PSNR, entropy, NCPR, UACI, performance overhead and complexity. The paper provided comprehensive insights into image encryption and related issues including the complexity level of the algorithms, lossless information, time constraints, security attacks, subjectivity, lack of values of the analytical parameters and excessive concepts related to keys. The evaluation showed that conventional encryption schemes were vulnerable to security attacks whereas DNA-based algorithms were more efficient and highly resistant to unauthorized access. Furthermore, the integration of chaotic maps and DNA-based algorithms achieved a high level of security and surpassed all the traditional techniques including various performance metrics.

4 Evaluation measures

The effectiveness of the discussed image encryption techniques is measured through the performance parameters mentioned below namely differential analysis, statistical analysis, information entropy, key sensitivity and noise attack.

4.1 Differential analysis (DA)

Differential attack analysis is used to assess the variations in the encrypted image after providing a minute change in a pixel of the plain image. In this way, both the original image and the altered image are encrypted using the same secret key. Differential attacks are commonly analyzed by means two criteria namely, the number of pixel change rate (NPCR) and the unified average changing intensity (UACI).

4.1.1 Number of pixel change rate (NPCR)

NCPR is used to calculate the percentage of different pixel numbers between two encrypted images. A high value of NCPR indicates that the encryption algorithm can better resist the differential attacks. The NPCR can be computed as follows [115]:

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100 \tag{1}$$

where

$$D(i,j) = \begin{cases} 0 & if \quad E(i,j) = E'(i,j) \\ 1 & if \quad E(i,j) \neq E'(i,j) \end{cases} \tag{2}$$

and $E(i,j)$ and $E^{'}(i,j)$ are encrypted images of original and modified images, respectively. While $D(i,j)$ indicate difference between pixels of the encrypted original and change image. W and H represent width and height of image, respectively.

4.1.2 Unified average changing intensity (UACI)

UACI is used to measure the average intensity of difference between two encrypted images [116]. It can be defined as follows [117]:

$$\text{UACI} = \frac{\sum_{i,j} E(i,j) - E'(i,j)}{255 \times W \times H} \times 100 \tag{3}$$

where $E(i, j)$ and $E^{'}(i, j)$ are the encrypted images of original and modified images, respectively.

4.2 Statistical analysis (SA)

To validate the encryption strength of algorithms toward statistical attacks two criteria are used, correlation coefficient (CC) and histogram analysis (HA) . To compare the difference from neighboring pixels of an encrypted image HA and CC are employed .

4.2.1 Histogram analysis (HA)

A histogram reveals the frequency distribution of the pixel intensity of an image. The histogram of the encrypted image should always be entirely different from the original image. The pixels of the original image are non-uniformly distributed while the histogram of the encrypted image is uniformly distributed.

4.2.2 Correlation coefficient analysis (CCA)

CCA is used to determine the correspondence between adjacent pixels of the original and the encrypted image. In the original image, the pixels are highly correlated in all directions, i.e., horizontally, vertically and diagonally. However, there should be no correlation among the adjacent pixels of the encrypted image. Higher correlation between the adjacent pixels indicates higher sensitivity to statistical attack. Therefore, good encryption algorithms tend to reduce the coefficient value. The correlation coefficient is found using following equation:

$$r_{x,y} = \frac{C(x, y)}{\sqrt{D(x)}.\sqrt{D(y)}} \tag{4}$$

where

$$C_{x,y} = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y))}{K} \tag{5}$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K}(x_i - E(x)^2) \tag{6}$$

$$D(y) = \frac{1}{K}\sum_{i=1}^{K}(y_i - E(x)^2) \tag{7}$$

C(x, y) is the co-variance between samples x and y, and x and y are the coordinates of an image. $D(x)$ and $D(y)$ are the standard deviation of x and y, respectively. K is the number of pixel pairs x_i , y_i. $E(x)$ is the mean of (x_i) pixel values.

4.3 Information entropy (IE)

IE represents the randomness of the image, i.e., average information per bit in the given image. The information entropy range for a good encryption algorithm is [0, 8]. Information entropy can be computed as:

$$H(S) = -\sum_{s}(P(s_i) \times log_2 P(s_i)) \tag{8}$$

where $H(S)$ is the entropy of message source (S), s_i is the information source (i.e., image pixel) and $P(s_i)$ represents the probability of occurrence of s_i.

4.4 Key analysis (KA)

In image encryption, the security keys are of fundamental importance as they are responsible for maintaining the secrecy of data. The strength of keys is analyzed through key space and key sensitivity. The size of the secret key indicates the effectiveness of the key space. The larger the size, the higher the key space, which makes it difficult for the adversary to generate similar key due to the large size. Key sensitivity can be best understood from the case where an encrypted image cannot be retrieved back due to a small change in the key used for encrypting the image. Thus, large key space and high sensitivity are the attributes of an effective encryption algorithm.

4.5 Noise attack (NA)

Noise attack analysis is also very important for an efficient image encryption. Here, the unintended user adds noise (Gaussian noise, salt and pepper noise, spackle noise, Poisson noise, etc.) in the encrypted image which then becomes unrecoverable after decryption.

5 Chaos-based image encryption survey in various domains

5.1 Image encryption in spatial domain

In the spatial domain, the encryption process involves direct operations on image pixels. The techniques based on the spatial domain are further classified into various categories and the theoretical analysis is discussed in the subsequent sections.

5.1.1 Image encryption techniques based on Chaotic maps

The time series data from chaotic maps appears as pseudo-random visually and the initial conditions and control

parameters for the maps can be used as keys to generate the time series. Therefore, chaotic maps can be applicable for the encryption/decryption of data. Chaotic maps are widely used in providing security and computational efficacy in data communication systems [118]. In the next part of this section, some of the latest research findings dealing with chaos-based image encryption techniques are discussed.

Hua et al [119], proposed a medical image encryption technique using bit-wise XOR and modulo arithmetic operations to implement pixel adaptive diffusion. The encryption technique mainly comprises two steps. Initially, the image surroundings are incorporated by means of random data. Later, the adjacent pixels are shuffled by means of high-speed scrambling and the incorporated random data is propagated throughout the image by implementing pixel adaptive diffusion. The benefit of the proposed technique is that it can be applied on a medical image of any format. Experimental results indicated high efficacy and robustness in protection against data loss and impulse noise.

Based on least squares approximations and chaotic maps, M. Ghebleh et al. [120] proposed an image encryption method consisting of two major phases, i.e., shuffling and masking (using 1D piece-wise linear chaotic maps). Together both phases are implemented on the rows and columns in several rounds of the input image. The security of the presented scheme is improved by using least squares approximations, which yields a powerful blend of rows and columns of the image. Experimental analysis shows that the proposed algorithm is resistant against differential attacks.

Z. Hua et al. [34] have presented an image encryption scheme based on the two-dimensional (2D) Logistic-Sine-coupling map (LSCM). The 2D-LSCM is derived by coupling two 1D chaotic maps, the Logistic map [121] and the Sine map [122].

The Logistic map is given as:

$$x_{i+1} = 4\eta x_i(1 - x_i), \tag{9}$$

the parameter η has the interval [0, 1]. While the Sine map is defined as:

$$x_{i+1} = \beta sin(\pi x_i), \tag{10}$$

the parameter $\beta \in [0, 1]$ the combination of logistic and sine map gives the logistic-sine coupling map as shown in equation (9):

$$\begin{cases} x_{i+1} = sin(\pi(4\theta x_i(1 - x_i) + (1 - \theta)sin(\pi y_i))) \\ y_{i+1} = sin(\pi(4\theta y_i(1 - y_i) + (1 - \theta)sin(\pi x_i + 1))) \end{cases}. \tag{11}$$

Here, θ is the control parameter on the interval [0,1]. The proposed algorithm is compared with several existing 2D chaotic map techniques and the performance estimations assessment indicate higher chaotic range, complex behavior and improved ergodicity of the presented scheme. In addition, by exploiting the 2D-LSCM technique the author has further proposed another algorithm namely Logistic-Sine-coupling Map Image Encryption Algorithm (LSCM-IEA). The structure of (LSCM-IEA) is based on the classical idea of confusion and diffusion, the former is designed to shuffle pixels of the image to alternate rows/columns while later is used to propagate tiny variations of the cipher image to the entire encrypted image. Theoretical results and simulations show that the presented algorithm has better encryption efficiency and outperforms several existing algorithms.

A. Abdulbaqi et al. presented an image encryption technique based on the combination of dynamic S-box, logistic map and Lorenz system [123] . Initially, the permutation algorithm is used to permute the plain image and substitution is done block by block by implementing circular shift of the variable S-box, later the key stages are added and a resultant image is obtained, i.e., a XOR image. The key generated by the logistic map is combined with the XOR image which is then confused afterward. The proposed technique is evaluated on the basis of various performance metrics such as entropy, histogram, key space, correlation, NPCR and UACI proving its robustness and efficacy against differential and statistical attacks.

Li et al. [124] proposed a hyper-chaos-based image encryption algorithm by exploiting permutation and diffusion architecture which implements permutation at bit level and pixel level. These permutations are employed along with a 5D chaotic map to achieve a secure cryptosystem and overcome the limitations in low-dimensional chaotic maps. The performance analysis demonstrates the robustness of the proposed algorithm in terms of key sensitivity and key sensitivity analysis, correlation analysis, histogram analysis and differential analysis.

To overcome the glitches of poor security and small key space in the one-dimension logistic map when applied in image encryption, Chunyan Han et al [125] proposed a modified logistic map image encryption algorithm. Simulations and experimental analysis concluded high key sensitivity, infinite key space and high security against statistical attacks.

Recently, Wang et al [126] introduced a one-dimensional cosine polynomial (1-DCP) chaotic map in image encryption. The strength of the proposed algorithm lies in its simple framework, larger key space and faster computational time than other existing one-dimensional maps. Moreover, another image encryption scheme (1-DCPIE) based on (1-DCP) was designed in order to further improve the chaotic properties. In this algorithm, the sequential permutation was replaced with parallel permutation substitution to achieve

Table 1 Comparison of recent papers based on the evaluation matrices used by them to evaluate performance of chaos-based image encryption techniques

Ref.	NPCR	UACI	KA	HA	CC	IE	NA
[118]	Yes	Yes	Yes	Yes	No	No	No
[119]	Yes	Yes	Yes	Yes	Yes	Yes	No
[120]	Yes	Yes	Yes	No	No	No	No
[34]	Yes	Yes	Yes	Yes	Yes	Yes	No
[123]	Yes	Yes	Yes	Yes	Yes	No	Yes
[33]	Yes	Yes	Yes	Yes	Yes	Yes	No
[124]	No	No	Yes	Yes	Yes	No	No
[125]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[126]	Yes	Yes	Yes	Yes	Yes	Yes	No

high security and improved speed. Experiments and results validate the robustness and efficiency of the proposed scheme over several existing techniques. Table 1 represents the comparison of some recent papers based on the evaluation matrices they used to analyze the performance of chaos-based image encryption techniques.

5.1.2 DNA-based image encryption techniques

In recent years, the rapid development in Deoxyribonucleic Acid (DNA)-based image encryption has gained attention among researchers due to its inherent properties of ultra-low power consumption, huge information density and massive parallelism. DNA-based encryption possesses remarkable advantages over traditional techniques but taken alone it does not satisfy the need of modern encryption algorithms [127]. Therefore, DNA encryption is combined with chaos-based image encryption in order to achieve more secure image encryption methods. A cryptosystem for color images based on the combination of chaotic maps and DNA sequences is presented in [128]. Image permutation in the presented techniques is carried out by means of the key streams and chaotic arrays generated by implementing the Chen system [129], thereby reducing the time complexity. The chaotic image is obtained by the key streams, both the chaotic image and permuted images are then distributed into equal blocks and image encryption is executed block-wise. A three-dimensional logistic map is used to select DNA encoding rules, which are used for the encoding of the plain image. Theoretical and statistical analysis demonstrates the robustness of the proposed scheme against statistical and brute force attacks.

A significant number of cryptosystems have been broken using chosen-plaintext attacks. In [130] a secure plaintext related mechanism for color image encryption has been introduced. The proposed encryption algorithm adopts the confusion–diffusion structure. A plaintext-related Latin-square-based block permutation (PLBP) is presented for shuffling the plain image pixels, while a diffusion method dependent on the plaintext and scrambled image (DM-DPSI) is proposed for modifying the permuted image pixels and to attain the cipher image. The seed values for the one-dimensional chaotic system are dynamically selected to generate chaotic sequences. Furthermore, the image permutation and diffusion operations are executed on the three components of the color image while the initial values and parameters are calculated using the external keys and the plain image. To investigate the efficacy of the proposed technique various performance analyses are used, i.e., information entropy analysis, histogram analysis, key space analysis, key sensitivity analysis and time complexity. The experimental results prove good performance, large key space and higher level of security.

Chen et al. introduced a secure image encryption scheme based on the 2D Henon-Sine map and DNA coding [131]. The proposed algorithm espouses the structure of classical permutation and diffusion. Image diffusion is implemented using XOR and DNA random coding, while image scrambling is used for swap operations on the pixels of the image. The DNA coding and XOR operation encryption effects are synthesized using the substitution box (S-box). The proposed algorithm shows that the idea of generalizing DNA encryption with S-box substitution is expected to be valuable in designing image encryption techniques.

Based on dynamic DNA and a four-wing hyper-chaos a color image cryptosystem has been proposed by Chai et al. [132]. Firstly, the color image is segregated into three main colors, and then chaotic sequences are generated by implementing the chaotic system, while the initial values of the chaotic system are computed by combining the external keys and SHA 384 hash value of the plain image. The four-wing hyper-chaotic system is represented as [133]:

$$\begin{cases} \dot{x} = ax + byz \\ \dot{y} = cy + dxz \\ \dot{z} = exy + kz + mxw \\ \dot{w} = ny \end{cases} \tag{12}$$

where x, y and z are state variables of the hyper-chaotic system, a, b, c, d, e, k, m, n are system constant parameters, and w is the state feedback controller. Secondly, the color image components RGB are mixed with a Simultaneous intra-inter-Component Permutation Mechanism Dependent on the Plaintext (SCPMDP). Subsequently, to substitute the DNA sequences of the plain image a diffusion mechanism based on random numbers related to plaintext (DMRNRP) is proposed. The DNA matrix is converted into three

Table 2 Comparison of recent papers based on the evaluation matrices used by them to evaluate performance of DNA-based image encryption techniques

Ref.	NPCR	UACI	KA	HA	CC	IE	NA
[128]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[130]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[131]	No	No	No	No	No	No	No
[132]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[134]	No	No	No	Yes	Yes	No	No
[135]	Yes	Yes	Yes	Yes	Yes	Yes	Yes

components by utilizing the DNA decoding rules. The experimental study shows satisfactory performance of the proposed algorithm in terms of robustness and security.

In 2018, a method to encrypt images using the Rivest Cipher (RC4) and DNA encoding was presented [134]. The proposed scheme improves the level of confidentiality and randomness of the plain image without disturbing its quality. Simulations and analysis indicate that the proposed algorithm shows a good level of security.

The authors in [135] suggested a lightweight image encryption technique that relies on pseudo-random numbers (PRN) and DNA computing. A sequence of pseudo-random numbers is used to permute the pixels of the image while DNA computation encrypts the permuted image. Currently, the presented method is applied only on gray images, however the technique may be extended for colored images in the future. Different tests and analysis show that the proposed algorithm is able to resist statistical attacks, differential attacks and noise. Table 2 shows a comparison of recent papers based on the evaluation matrices used by them to evaluate performance of DNA-based image encryption techniques.

5.1.3 Cellular automata (CA) image encryption techniques

Cellular automata (CA) have been extensively used for encrypting images, owing to their characteristics of unpredictability, homogeneity, parallelism and easy execution in software and hardware systems [136]. CA have shown promising results in image encryption, image processing, image scrambling, authentication and security.

Yaghouti Niyat et al. have proposed an image encryption framework based on non-uniform cellular automata (CA) and hyper-chaotic functions, to resolve the issue of the limited number of reversal rules [137]. In this technique, a CA is used to relocate the pixel positions in the original image and generate confusion. The image is then encrypted by selecting random numbers through hyper-chaotic mapping, thereby enhancing the key generation process. Experimental results and security analysis show that the proposed method is a good choice for encrypting digital images due to its larger key space and high resistance against noise, statistical and differential attacks .

Based on the memristive hyper-chaotic system, two-dimensional CA and DNA sequence operations, an image encryption algorithm is presented in [138]. The secret key and the initial values of the system are generated using the SHA 256 hash value function. The paper also introduces a dynamic DNA encoding scheme. Different simulation analyses are performed to evaluate the efficacy of the proposed algorithm which show that it provides secure and efficient image encryption and its resistance against plaintext attacks.

Li et al. [139] proposed an alternative method to previously published color image encryption techniques based on cellular automata and a hybrid hyper-chaotic system. The former technique used the sum of values of the pixel component at each point to estimate the starting point for the logistic map, furthermore, the presented method uses an equivalent permutation key stream which keeps the sum of the value of pixels at each color channel constant. Moreover, the paper gives three principle strategies to attain improved image encryption: 1. Instead of calculating the key by the sum of pixels, the relevance of plaintext and secret key should be complex. 2. After implementing XOR operation add an effective diffusion. 3. Adopt multiple rounds of permutation–diffusion.

Recently, a 2D hybrid chaotic map image encryption technique has been presented for transmitting images securely [140]. The technique is based on logistic, sine and tent maps, which utilize cellular automata and a discrete framelet transform for mixing the positions of image pixels by applying various kinds of shifts. Different tests and analysis show that the proposed method can effectively resist known plaintext attacks, statistical attacks, differential attacks, data loss and noise.

Li et al. [141] proposed a holographic frames encryption scheme using cellular automata pixel-permutation encoding to overcome the limitations of traditional encryption schemes. In this technique, the established order of the image pixels is broken which thus resolves the inherent issue of traditional 2D CA mask-based encoding methods which provides horizontal patterns. Experiments and simulation results demonstrate effectiveness and security against optical and plain image attacks.

Based on recursive cellular automata RCA and DNA sequences an image encryption algorithm is presented in [142]. The presented technique comprises two main phases. In the first phase, namely the permutation phase, the pixel values of the image are shifted using the logistic map. In the second phase, both DNA and RCA sequences are employed in the diffusion phase to substitute the gray level of pixels to new ones. Simulations and security analysis demonstrate the effectiveness of the new encryption technique.

Table 3 Comparison of recent papers based on the evaluation matrices used by them to evaluate performance of cellular automata (CA)-based image encryption techniques

Ref.	NPCR	UACI	KA	HA	CC	IE	NA
[137]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[138]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[139]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[140]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[141]	No	No	Yes	Yes	No	No	Yes
[142]	Yes	Yes	Yes	Yes	Yes	Yes	No
[143]	Yes	Yes	Yes	Yes	Yes	Yes	No
[144]	Yes	Yes	Yes	Yes	Yes	Yes	No

Naskar, Prahir Kurnar et al. [143] proposed a robust and secure image encryption method based on a chaotic tent map and cellular automata. In this work, the shuffling and ciphering of the block size variable are achieved through variable key streams. The size of each block depends on the key stream. Different experiments and simulations assess the effectiveness of proposed algorithm.

Su et al. [144] proposed a reversible cellular automata-based image encryption technique for similarity research in an encrypted domain. The presented technique implements pixel-based deterministic encryption in order to define a similarity search on the encrypted images. In addition, the paper introduces a deterministic encryption reversible cellular automata (DERCA) based on the feasibility of pixel-based deterministic encryption. Furthermore, based on DERCA a two level granularity algorithm has been proposed to ensure a similarity search on encrypted images. Theoretical analysis and experiments show better performance in similarity searches as compared to existing algorithms. Table 3 shows the performance comparison of cellular automata-based image encryption techniques.

5.2 Image encryption in transform domain

Transform-based cryptography has been widely used for image encryption. In the transform domain, with the help of suitable transforms (discrete cosine transform (DCT), discrete wavelet transform (DWT), gyrator transform (GT) and Fourier transform (FT)) the given data is transformed from spatial to frequency domain. Thus, the images are encrypted by changing the positions of the coefficients of the image.

Yao et al. [145] introduced an image encryption method to encrypt color images to gray by employing the properties of the deduced gyrator transform. At the initial stage of the encryption process, the image is transformed using the gyrator transform and then the resultant image is multiplied by a phase distribution p*, later on a Fourier transform is applied. The RGB components of the color image are modified using the random phase mask which is then combined by convolution. Moreover, the decryption process of the image employs the operation of the inverse Fourier transform. Simulations and experiments demonstrate the effectiveness and feasibility of the presented scheme.

Li et al. [146], proposed a multiple-image encryption technique based on unified permutation and separate diffusion using a robust chaotic map in the wavelet transform domain. In this work, the discrete wavelet transform is used to decompose the original image into low frequency components, which are then reassembled as the plain image. After that, the Arnold cat map is employed to scramble the plain image. Subsequently, the resultant scrambled image is further decomposed to obtain block images which are then integrated with the amplitude parameter of the robust chaotic map (RCM) for producing key streams. Performance of the proposed algorithm is verified through numerical simulations and experiments.

In 2018, Ren et al. [147] proposed a unique asymmetric image encryption technique based on phase-truncated discrete multiple-parameter fractional Fourier transform (PTDMPFRFT). Firstly, the original image is scrambled using pixel scrambling and random-mask, which is then phase-truncated using DMPFRFT. Then the image is decrypted by applying inverse pixel scrambling using the phase key in the DMPFRFT domain. Results and experiments are conducted to demonstrate the recovered quality and efficacy of the presented work.

Kumar et al. [148] proposed a robust medical image encryption method to ensure the safety of medical images employing logistic arrays in fractional discrete cosine transforms (FrDCT). The FrDCT is applied on the original image and the chaotic map is employed on the FrDCT coefficients. Theoretical analysis and experimental results show that the proposed technique provides higher degree of liberty for encrypting medical images and is highly robust against differential, statistical and brute force attacks.

In addition to the issues faced by conventional chaotic image encryption techniques such as low key sensitivity and low security, Meng et al. [149] have introduced an improved image encryption algorithm based on chaotic mapping and the discrete wavelet transform domain (DCT). Image scrambling and grayscale diffusion are applied on the original image through multiple rounds. The obtained image is processed by DCT followed by chaotic mapping. Numerical analysis demonstrates that the proposed algorithm provides good real-time performance and high resistance against statistical and differential attacks.

In [150], Shafique et al. addressed the issues of pixel hiding of the original image with low textured regions and increased computational time which are often present in traditional image encryption techniques. To overcome these issues the author has proposed dynamic substitution S-box

encryption in a discrete wavelet transform (DWT). This technique resolves the issue of pixel concealment by employing multiple S-boxes with dynamic substitution, while the computational time of the encryption method is significantly reduced by DWT as it decomposed the plain image up to fifth level decomposition. The accuracy of the proposed algorithm is evaluated through different performance metrics such as MSE, PSNR, homogeneity, correlation, energy and entropy. Numerical simulations are conducted to inspect the effectiveness of the proposed scheme.

An improved chaotic image encryption algorithm based on integer wavelet transform (IWT) and global bit scrambling (GBS) is proposed in [151]. The proposed algorithm uses IWT to decompose the original image; the logistic map is employed for encrypting the image while GBS is used for bit scrambling of the image. The introduction of the GBS in the scheme provides better resistance against various attacks. The capability and efficiency of the algorithm are validated through different tests and experiments. This paper presents a new image encryption scheme based on the combination of Haar wavelet transform with the Advanced Encryption Standard (AES) and pixel shuffling using the logistic map presented in [152]. Initially, the Haar wavelet transformation is used to breakdown the image into its frequency components, followed by AES encryption which encrypts the image obtained in the first step. Thereafter, a subsequent image is transformed by applying the inverse of the Haar wavelet transform. Later the logistic map is used to shuffle the pixels of the acquired image, thereby strengthening the efficiency of the encryption process. Theoretical results and experiments performed demonstrate that the proposed method achieved a high level of encryption across a variety of test images.

Considering the weakness of color images in terms of data redundancy makes them prone toward statistical attacks, researchers in [153] presented two encryption solutions to overcome such vulnerabilities. The proposed security solution is established using the phase retrieval algorithms, random fractional Fourier transforms, in conjunction with chaotic scrambling and diffusion techniques. The paper comprises two novel encryption schemes that provide a strategy to overcome inherent weaknesses and redundancies by strengthening the security of the system. The proposed technique is evaluated in terms of NPCR, UACI and entropy which demonstrate the flexibility and capability over the previously existing techniques.

The study published in 2019 [154] aimed to solve the limitations of conventional image encryption algorithms by proposing a double chaotic image encryption algorithm based on a fractional Fourier transform. By employing the fractional Fourier transform and the Henon map an optimization algorithm is obtained from which the ciphertext is obtained. Theoretical analysis and experiments show that the proposed algorithm achieves large key space and strong key sensitivity and is highly resistant against differential, statistical and noise attacks. Table 4 represents the comparison of recent papers based on the evaluation matrices used by them to evaluate performance of transform-based image encryption techniques.

Table 4 Comparison of recent papers based on the evaluation matrices used by them to evaluate performance of transform-based image encryption techniques

Ref.	NPCR	UACI	KA	HA	CC	IE	NA
[145]	No	No	Yes	Yes	Yes	No	Yes
[146]	No	No	Yes	Yes	Yes	No	Yes
[147]	No	No	No	No	No	No	Yes
[148]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[149]	Yes	Yes	Yes	Yes	No	Yes	No
[150]	No	No	No	Yes	Yes	Yes	No
[151]	Yes	Yes	Yes	Yes	No	Yes	No
[152]	No	No	No	Yes	Yes	Yes	No
[153]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[154]	Yes	Yes	Yes	Yes	Yes	Yes	No

5.3 Image encryption in spatiotemporal domain

In recent years, coupled map lattices (CML)-based spatiotemporal chaotic systems have attracted the attention of many researchers as they have shown remarkable properties in secure communication as compared to single maps [155]. The spatiotemporal chaotic system possesses a larger parameter space, a spectrum of Lyapunov exponents and pseudo-random chaotic series. CMLs are considered a good choice for image encryption purposes.

A Color image encryption scheme based on chaos and Customized Globally Coupled Map Lattices is presented in [156]. The proposed scheme comprises four phases. Firstly, the color decomposition method is used to decompose the RGB image into its three components and a key image equal to the size of original image is generated with the help of CML-based logistic map. Secondly, the image is divided and shuffled into four images, i.e., red image, green image , blue image and RGB image, each of which is the same size. Finally, the confusion operations will be performed in order to choose the key image out of the four images. Later, the remaining three images are combined to obtain the cipher image. Experimental analysis and simulations show that the presented image encryption algorithm is highly resistant against certain security risks and attacks.

Another color image encryption technique based on the combination of spatiotemporal chaotic system and DNA sequences is presented in [157]. In order to achieve more random sequences, the Logistic-Sine system (LSS) is employed in the CML and a new spatiotemporal chaotic system is

constructed. Initially, the key image is generated from the original image and secret keys provided in the spatiotemporal sequences. The pixel values are interrupted by applying exclusive-OR operations. In addition, DNA deletion and DNA insertion pseudo-operations are performed to confuse the DNA encoded diffused image under the supervision of key streams. Lastly, the DNA encoded mage is decoded to acquire the encrypted image. Experimental results and theoretical analysis exhibit that the presented image cryptosystem achieves high accuracy in performance and is robust against various attacks including differential and statistical attacks.

In [158] the authors have highlighted the problem of key diffusion in chaotic image encryption algorithms and therefore presented a solution in this regard. The proposed algorithm replaces half of the iterations with iterations of a CML during the transient period. Various aspects of the designated scheme such as sensitivity on keys or resistance against differential attacks are presented. Moreover, a detailed analysis of recent techniques is discussed and compared with the proposed algorithm on the basis of widely used performance metrics. The results conclude that the proposed scheme outperforms other approaches by achieving high values of Unified Average Changing Intensity (UACI) and entropy.

Wang et al. have proposed a novel spatiotemporal chaos system titled multiple coupled map lattices (MCML) [159]. The paper presents a detailed analysis of MCML features like Kolmogorov–Sinai entropy, bifurcation diagrams and spatiotemporal behavior, which prove it to be quite suitable for image encryption algorithms. The proposed technique uses nonlinear diffusion and at the same time conducts shuffling and diffusion operations. With the experimental analysis of key sensitivity, histogram analysis, correlation analysis and differential attack, it can be deduced that this nonlinear diffusion technique deteriorates the correlation among the neighboring pixels in the plain image and shows significant reduction in correlation between the R, G and B components of the color image. The experimental analysis shows that the proposed algorithm is robust, efficient and safe.

Hossein et al. presented a medical encryption method to ensure the security of medical images [160]. The proposed technique is based on a hybrid model of coupled map lattices and modified genetic algorithm (MGA). Firstly, a secure number of cipher images is produced (as initial population of MGA) by using the CML. Later, the technique employs MGA to decrease the execution time of the algorithm and also increase the entropy of the generated cipher images. The proposed algorithm provides improved quality images in less computational time.

Wang et al. proposed a spatiotemporal chaos model called logistic-dynamic coupled logistic map lattice (LDCML) [161]. The paper presents a brief comparison of LDCML with CML on the basis of adjacent pixels correlation, computational complexity, image sensitivity, secret key space and information entropy. The theoretical analysis and experiments indicate that LDCML is more chaotic and has larger key space as compared to other image encryption schemes discussed in the paper.

The paper [162] presents a novel double-image encryption technique based on spatiotemporal chaos and DNA insertion and deletion operations. The images in confusion and diffusion phase are encrypted simultaneously by applying the DNA insertion and deletion operations. The non-adjacent coupled map lattice (NCML) is employed to generate the key streams. The proposed double-image encryption algorithm proves to have high key sensitivities, large key space, high entropy and is highly resistant against noise and occlusion attacks.

Zhang et al. propose a novel spatiotemporal dynamics based on two-dimensional coupled map lattices 2DCML by using mixed linear–nonlinear (MNCML) coupling [163]. In order to quantify the complexity of the proposed system different performance metrics such as Kolmogorov–Sinai entropy, snapshot pattern diagrams, space-amplitude and bifurcations analysis are employed. Furthermore, a brief comparison of both 2DCML and MNCML is also demonstrated. The numerical simulations and theoretical analysis indicate that the proposed scheme encompasses various characteristics including less regions of periodic behavior in bifurcation diagrams. These wide ranging characteristics of the proposed algorithm make it suitable for cryptography.

A high-dimensional spatiotemporal chaotic system based on a 2D non- adjacent coupled map lattice (2DNACML) is presented in [164]. The dynamics of the system are studied and analyzed using Kolmogorov–Sinai entropy calculations, Lyapunov exponent analysis and bifurcation diagrams. The analysis of the 2DNACML model indicates that range for control parameters of the system parameters is expanded using the proposed method, also each lattice is effected by other non-adjacent lattices which further increases the complexity of the system. The output of the system is then used for scrambling and diffusion of images based on chaotic and knights tour methods. The results reveal that the proposed system successfully passed randomness tests from National Institute of Standards and Technology. The presented system also showed promising results for statistical tests, information entropy tests, key sensitivity analysis and algorithm complexity analysis.

A new technique on image encryption based on non-adjacent coupled map lattices is presented in [165]. Initially, the CML is blended with a 3D Arnold transformation to improve the security of the presented model. In comparison to the traditional CML image encryption approach, the non-adjacent CML implements the alternative structure of permutation, diffusion and substitution and each pixel is encrypted only once, this mechanism minimizes the

Table 5 Comparison of recent papers based on the evaluation matrices used by them to evaluate performance of image encryption techniques in Spatiotemporal domain

Ref.	NPCR	UACI	KA	HA	CC	IE	NA
[156]	Yes	Yes	Yes	Yes	Yes	Yes	No
[157]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[158]	Yes	Yes	Yes	No	No	Yes	No
[159]	Yes	Yes	Yes	Yes	Yes	Yes	No
[160]	Yes	Yes	Yes	Yes	Yes	Yes	No
[161]	Yes	Yes	Yes	Yes	Yes	Yes	No
[162]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[163]	No	No	Yes	No	No	Yes	No
[164]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[165]	Yes	Yes	Yes	Yes	Yes	Yes	Yes

complexity of the system. Lastly, a dynamic S-box is designed by replacing the irreducible present in the plaintext with the help of dynamic hash values, these plaintext values are then substituted by dynamic S-box. The simulations validate the efficacy of proposed technique. Table 5 represents the comparison of recent papers based on the evaluation matrices used by them to evaluate performance of image encryption techniques in spatiotemporal domain.

6 Conclusion

This paper provides an extensive study on image encryption techniques performed in spatial, temporal and spatiotemporal domains. A thorough survey has been performed on the recent papers from last five years and has classified them into relevant categories for better understanding. From the literature review, it can be concluded that the field of image encryption is still in the growth stage and needs maturity in security issues, computational efficiency and parameter tuning. The summary results of evaluation methods for encryption techniques depict that the majority of the papers do not use all the standard checks to validate an encryption algorithm's performance. There should be a standard benchmark to evaluate the efficacy and efficiency of newly proposed image encryption schemes. An open area of research is video processing and video security, and how the image encryption techniques can be extended to video encryption methods.

Funding This research is supported by the BTIIC (British Telecom Ireland Innovation Centre) project, funded by British Telecom and Invest Northern Ireland.

Declarations

Conflict of Interest The authors have no conflicts of interest to declare. All co-authors have seen and agreed with the contents of the manuscript. We certify that the submission is original work and is not under review at any other publication.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent Not applicable.

Informed consent Not applicable.

References

1. Apostol, K.: Brute-Force Attack (2012)
2. Hurley, N., Cheng, Z., Zhang M.: Statistical attack detection. In: Proceedings of the Third ACM Conference on Recommender Systems, pp. 149–156 (2009)
3. Lu, J., Dunkelman, O., Keller, N., Kim, J.: New impossible differential attacks on aes. In: International Conference on Cryptology in India, Springer, pp. 279–293 (2008)
4. Shah, T., Jamal, S.S., et al.: An improved chaotic cryptosystem for image encryption and digital watermarking. Wireless Personal Commun. **110**(3), 1429–1442 (2020)
5. Zeng, W., Lei, S.M.: Digital image scrambling for image coding systems. US Patent 6,505,299 (2003)
6. Morkel, T., Eloff, J.H., Olivier, M.S.: An overview of image steganography. In: ISSA, vol 1 (2005)
7. Bhowmik, S., Acharyya, S.: Image cryptography: The genetic algorithm approach. In: 2011 IEEE International Conference on Computer Science and Automation Engineering, IEEE, vol. 2, pp. 223–227 (2011)
8. Jeyanthi, N., Thandeeswaran, R.: Security Breaches and Threat Prevention in the Internet of Things. IGI Global (2017)
9. Kumari, S.: A research paper on cryptography encryption and compression techniques. International Journal Of Engineering And Computer Science 6(4) (2017)
10. Hell, M., Johansson, T., Maximov, A., Meier, W.: A stream cipher proposal: Grain-128. In: 2006 IEEE International Symposium on Information Theory, IEEE, pp. 1614–1618 (2006)
11. De Canniere, C.: Trivium: A stream cipher construction inspired by block cipher design principles. In: International Conference on Information Security, Springer, pp. 171–186 (2006)
12. Babbage, S., Dodd, M.: The mickey stream ciphers. In: New Stream Cipher Designs, Springer, pp. 191–209 (2008)

13. Heron, S.: Advanced encryption standard (aes). Netw. Security **2009**(12), 8–12 (2009)
14. Barker, W.C.: Recommendation for the triple data encryption algorithm (tdea) block cipher (2004)
15. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher clefia. In: International Workshop on Fast Software Encryption, Springer, pp. 181–195 (2007)
16. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y., Vikkelsoe, C.: Present: An ultra-lightweight block cipher. In: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, pp. 450–466 (2007)
17. Tripathi, R., Agrawal, S.: Comparative study of symmetric and asymmetric Cryptogr Techniq (2014)
18. Harn, L., Mehta, M., Hsin, W.J.: Integrating Diffie-Hellman key exchange into the digital signature algorithm (dsa). IEEE Commun. lett. **8**(3), 198–200 (2004)
19. Johnson, D., Menezes, A., Vanstone, S.: The elliptic curve digital signature algorithm (ecdsa). Int. J. Inf. Security **1**(1), 36–63 (2001)
20. Milanov, E.: The rsa algorithm. RSA laboratories, pp. 1–11 (2009)
21. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
22. Noshadian, S., Ebrahimzade, A., Kazemitabar, S.J.: Optimizing chaos based image encryption. Multimedia Tools Appl. **77**(19):25,569–25,590 (2018)
23. Furht, B., Muharemagic, E., Socek, D.: Multimedia encryption and watermarking, vol 28. Springer Science & Business Media (2006)
24. Liu, Z., Wang, Y., Zhao, Y., Zhang, L.Y.: A stream cipher algorithm based on 2d coupled map lattice and partitioned cellular automata. Nonlinear Dyn. **101**(2), 1383–1396 (2020)
25. Xy, Wang, Xm, Bao: A novel block cryptosystem based on the coupled chaotic map lattice. Nonlinear Dyn. **72**(4), 707–715 (2013)
26. Peng, Z., Yu, W., Wang, J., Zhou, Z., Chen, J., Zhong, G.: Secure communication based on microcontroller unit with a novel five-dimensional hyperchaotic system. Arab. J. Sci. Eng., pp. 1–16 (2021)
27. Som, S., Dutta, S., Singha, R., Kotal, A., Palit, S.: Confusion and diffusion of color images with multiple chaotic maps and chaos-based pseudorandom binary number generator. Nonlinear Dyn. **80**(1), 615–627 (2015)
28. Xu, H., Tong, X., Meng, X.: An efficient chaos pseudo-random number generator applied to video encryption. Optik **127**(20), 9305–9319 (2016)
29. Lan, R., He, J., Wang, S., Gu, T., Luo, X.: Integrated chaotic systems for image encryption. Signal Processing **147**, 133–145 (2018)
30. Sankpal, P.R., Vijaya, P.: Image encryption using chaotic maps: a survey. In: 2014 Fifth international Conference on Signal and image Processing, IEEE, pp. 102–107 (2014)
31. Wei-Bin, C., Xin, Z.: Image encryption algorithm based on Henon chaotic system. In: 2009 International Conference on Image Analysis and Signal Processing, IEEE, pp. 94–97 (2009)
32. Krishna, P.R., Teja, C.V.S., Thanikaiselvan, V., et al.: A chaos based image encryption using tinkerbell map functions. In: 2018 Second International Conference on Electronics, pp. 578–582. Communication and Aerospace Technology (ICECA), IEEE (2018)
33. Pak, C., Huang, L.: A new color image encryption using combination of the 1d chaotic map. Signal Process. **138**, 129–137 (2017)
34. Hua, Z., Jin, F., Xu, B., Huang, H.: 2d logistic-sine-coupling map for image encryption. Signal Process. **149**, 148–161 (2018)
35. Shan, L., Qiang, H., Li, J., Zq, Wang: Chaotic optimization algorithm based on tent map. Control Decision **20**(2), 179–182 (2005)
36. Fang, D., Sun, S.: A new secure image encryption algorithm based on a 5d hyperchaotic map. Plos one 15(11):e0242,110 (2020)
37. Flayh, N.A., Parveen, R., Ahson, S.I.: Wavelet based partial image encryption. In: 2009 International Multimedia, Signal Processing and Communication Technologies, pp. 32–35, IEEE (2009)
38. Li, Z., Peng, C., Li, L., Zhu, X.: A novel plaintext-related image encryption scheme using hyper-chaotic system. Nonlinear Dyn. **94**(2), 1319–1333 (2018)
39. Deng, H., Qin, Z., Wu, Q., Guan, Z., Zhou, Y.: Flexible attribute-based proxy re-encryption for efficient data sharing. Inf.Sci. **511**, 94–113 (2020)
40. Pisarchik, A.N., Zanin, M.: Image encryption with chaotically coupled chaotic maps. Phys. D Nonlinear Phenomena **237**(20), 2638–2648 (2008)
41. Ye, R.: A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Optics Commun. **284**(22), 5290–5298 (2011)
42. Koduru, S.C., Chandrasekaran, V.: Integrated confusion-diffusion mechanisms for chaos based image encryption. In: 2008 IEEE 8th International Conference on Computer and Information Technology Workshops, IEEE, pp. 260–263 (2008)
43. Li, S., Zheng, X.: Cryptanalysis of a chaotic image encryption method. In: 2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No.02CH37353), vol. 2, pp. II–II, 10.1109/ISCAS.2002.1011451 (2002)
44. Feng, W., He, Y., Li, H., Li, C.: Cryptanalysis and improvement of the image encryption scheme based on 2d logistic-adjusted-sine map. Ieee Access **7**, 12,584–12,597 (2019)
45. Wang, H., Xiao, D., Chen, X., Huang, H.: Cryptanalysis and enhancements of image encryption using combination of the 1d chaotic map. Signal Process. **144**, 444–452 (2018)
46. Chen, J., Han, F., Qian, W., Yao, Y.D., Zl, Zhu: Cryptanalysis and improvement in an image encryption scheme using combination of the 1d chaotic map. Nonlinear Dyn. **93**(4), 2399–2413 (2018)
47. Solak, E., Cokal, C., Yildiz, O.T., Biyikoğlu, T.: Cryptanalysis of Fridrich‘s chaotic image encryption. Int. J. Bifur. Chaos **20**(05), 1405–1413 (2010)
48. Ben-Aroya, I., Biham, E.: Differential cryptanalysis of Lucifer. In: Annual International Cryptology Conference, Springer, pp. 187–199 (1993)
49. Alani, M.M.: Neuro-cryptanalysis of des and triple-des. In: International Conference on Neural Information Processing, Springer, pp. 637–646 (2012)
50. Fluhrer, S., Mantin, I., Shamir, A.: Weaknesses in the key scheduling algorithm of rc4. In: International Workshop on Selected Areas in Cryptography, Springer, pp. 1–24 (2001)
51. Biryukov, A., Khovratovich, D.: (2009) Related-key cryptanalysis of the full aes-192 and aes-256. In: International Conference on the Theory and Application of Cryptology and Information Security, Springer, pp. 1–18
52. Li, M., Zhou, K., Ren, H., Fan, H.: Cryptanalysis of permutation-diffusion-based lightweight chaotic image encryption scheme using cpa. Appl. Sci. **9**(3), 494 (2019)
53. Mondal, B., Kumar, P., Singh, S.: A chaotic permutation and diffusion based image encryption algorithm for secure communications. Multimedia Tools Appl. **77**(23), 31,177–31,198 (2018)
54. Dou, Y., Li, M.: Cryptanalysis of a new color image encryption using combination of the 1d chaotic map. Appl. Sci. **10**(6), 2187 (2020)
55. Pak, C., An, K., Jang, P., Kim, J., Kim, S.: A novel bit-level color image encryption using improved 1d chaotic map. Multimedia Tools Appl. **78**(9), 12,027–12,042 (2019)
56. Li, M., Wang, P., Liu, Y., Fan, H.: Cryptanalysis of a novel bit-level color image encryption using improved 1d chaotic map. IEEE Access **7**, 145,798–145,806 (2019)

57. Fridrich, J.: Symmetric ciphers based on two-dimensional chaotic maps. Int. J. Bifur. chaos **8**(06), 1259–1284 (1998)
58. Xie, E.Y., Li, C., Yu, S., Lü, J.: On the cryptanalysis of fridrich's chaotic image encryption scheme. Signal Process. **132**, 150–154 (2017)
59. Laiphrakpam, D.S., Khumanthem, M.S.: Cryptanalysis of symmetric key image encryption using chaotic Rossler system. Optik **135**, 200–209 (2017)
60. Mandal, M.K., Kar, M., Singh, S.K., Barnwal, V.K.: Symmetric key image encryption using chaotic Rossler system. Security Commun. Netw. **7**(11), 2145–2152 (2014)
61. Diab, H., El-semary, A.M.: Cryptanalysis and improvement of the image cryptosystem reusing permutation matrix dynamically. Signal Process. **148**, 172–192 (2018)
62. Jx, Chen, Zhu Zl, Fu.C., Yu, H., Zhang, Y.: Reusing the permutation matrix dynamically for efficient image cryptographic algorithm. Signal Process. **111**, 294–307 (2015)
63. Feki, M., Robert, B., Gelle, G., Colas, M.: Secure digital communication using discrete-time chaos synchronization. Chaos Solitons Fractals **18**(4), 881–890 (2003)
64. Alvarez, G., Montoya, F., Romera, M., Pastor, G.: Cryptanalyzing a discrete-time chaos synchronization secure communication system. Chaos Solitons Fractals **21**(3), 689–694 (2004)
65. Kester, Q.A.: A hybrid cryptosystem based on vigenere cipher and columnar transposition cipher. (2013) arXiv preprint arXiv:1307.7786
66. Matthews, R.: On the derivation of a chaotic encryption algorithm. Cryptologia **8**(1), 29–41 (1984)
67. Mousa, A., Hamad, A.: Evaluation of the rc4 algorithm for data encryption. IJCSA **3**(2), 44–56 (2006)
68. Basu, S.: International data encryption algorithm (idea)-a typical illustration. J. Global Res. Comput. Sci. **2**(7), 116–118 (2011)
69. Schneier, B.: The blowfish encryption algorithm. Dr Dobb's J. Softw. Tools Profess. Program. **19**(4), 38–43 (1994)
70. Mandal, S., Das, S., Nath, A.: Data hiding and retrieval using visual cryptography. Int. J. Innov. Res. Adv. Eng. **1**, 102–110 (2014)
71. Rivest, R.L.: The rc5 encryption algorithm. In: International Workshop on Fast Software Encryption, Springer, pp. 86–96 (1994)
72. Ahmed, H.E.d.H., Kalash, H.M., Allah, O.F.: Encryption efficiency analysis and security evaluation of rc6 block cipher for digital images. In: 2007 International Conference on Electrical Engineering, IEEE, pp. 1–7 (2007)
73. Rayarikar, R., Upadhyay, S., Pimpale, P.: Sms encryption using aes algorithm on android. Int. J. Comput. Appl. **50**(19), 12–17 (2012)
74. Sam, I.S., Devaraj, P., Bhuvaneswaran, R.: An intertwining chaotic maps based image encryption scheme. Nonlinear Dyn. **69**(4), 1995–2007 (2012)
75. François, M., Grosges, T., Barchiesi, D., Erra, R.: A new image encryption scheme based on a chaotic function. Signal Process. Image Commun. **27**(3), 249–259 (2012)
76. Sam, I.S., Devaraj, P., Bhuvaneswaran, R.S.: A novel image cipher based on mixed transformed logistic maps. Multimedia Tools Appl. **56**(2), 315–330 (2012)
77. Hanchinamani, G., Kulkarni, L.: An efficient image encryption scheme based on a peter de jong chaotic map and a rc4 stream cipher. 3D Research **6**(3), 1–15 (2015)
78. Bansal, R., Gupta, S., Sharma, G.: An innovative image encryption scheme based on chaotic map and vigenère scheme. Multimedia Tools Appl. **76**(15), 16,529–16,562 (2017)
79. Kumari, M., Gupta, S., Sardana, P.: A survey of image encryption algorithms. 3D Research **8**(4), 37 (2017)
80. Sriadhi, S., Rahim, R., Ahmar, A.S.: Rc4 algorithm visualization for cryptography education. In: J. Phys. Conf. Ser. **1028**, 012057 (2018)
81. Mandal, A., Parakash, C., Tiwari, A.: Performance evaluation of cryptographic algorithms: Des and aes. In2012 IEEE Students' Conference on Electrical, Electronics and Computer Science. 1 mar 2012 (pp. 1–5)
82. Kathil, P., Goyal, S., Agrawal, R.: Survey on various image encryption schemed through chaotic maps. Int. J. Adv. Res. Comput. Sci. **8**(5) (2017)
83. Saikia, M., Baruah, B.: Chaotic map based image encryption in spatial domain: a brief survey. In: Proceedings of the First International Conference on Intelligent Computing and Communication, Springer, pp. 569–579 (2017)
84. Dahiya, M., Kumar, R.: A literature survey on various image encryption & steganography techniques. In: 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), IEEE, pp. 310–314 (2018)
85. Priyanka, M., Prasad, E.L., Reddy, A.: Fpga implementation of image encryption and decryption using aes 128-bit core. In: 2016 International Conference on Communication and Electronics Systems (ICCES), IEEE, pp. 1–5 (2016)
86. Kalubandi, V.K.P., Vaddi, H., Ramineni, V., Loganathan, A.: A novel image encryption algorithm using aes and visual cryptography. In: 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), IEEE, pp. 808–813 (2016)
87. Abood, M.H.: An efficient image cryptography using hash-lsb steganography with rc4 and pixel shuffling encryption algorithms. In: 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), IEEE, pp. 86–90 (2017)
88. Ferdush, J., Begum, M., Mahmood, A.: A new image encryption technique combining the idea of one time pad with rgb value. Int. J. Comput. Appl. **178**, 12–15 (2017)
89. Singh, S., Agrawal, A., Pradhan, P.: Advanced text to image encryption by using selective encryption technique with c hash (aes encryption and cfb mode). Int. J. Innov. Res. Comput. Commun. Eng
90. Shanthi, V.P.: A novel text to image encryption technique by aes rijndael algorithm with color code conversion. Int. J. Eng. Trends Technol (IJETT) **13**(5) (2014)
91. Mishra, M., Pandit, S.: Image encryption technique incorporating wavelet transform and hash integrity. IJRET: Int. J. Res. Eng. Technol **4**(02) (2015)
92. Panchal, D., Jani, C., Panchal, H.: An approach providing two phase security of images using encryption and steganography in image processing. Int. J. Eng. Develop. Res. **3**(4) (2015)
93. Khizrai, M.S.Q., Bodkhe, S.: Image encryption using different techniques for high security transmission over a network. Int. J. Eng. Res. General Sci. **2**(4), 299–306 (2014)
94. Singh, P., Singh, K.: Image encryption and decryption using blowfish algorithm in matlab. In. J. Sci. Eng. Res. **4**(7), 150–154 (2013)
95. Khanzadi, H., Eshghi, M., Borujeni, S.E.: Image encryption using random bit sequence based on chaotic maps. Arab. J. Sci. Eng. **39**(2), 1039–1047 (2014)
96. Abusukhon, A., Talib, M.: A novel network security algorithm based on private key encryption. In: Proceedings Title: 2012 International Conference on Cyber Security, pp. 33–37. Cyber Warfare and Digital Forensic (CyberSec), IEEE (2012)
97. Ahmad, J., Ahmed, F.: Efficiency analysis and security evaluation of image encryption schemes. computing **23**, 25 (2010)
98. Radhadevi, P., Kalpana, P.: Secure image encryption using aes. Int. J. Res. Eng. Technol. **1**(2), 15–117 (2012)
99. Deshmukh, P.: An image encryption and decryption using aes algorithm. Int. J. Sci. Eng. Res. **7**(2), 210–213 (2016)

100. Karthigaikumar, P., Rasheed, S.: Simulation of image encryption using aes algorithm. IJCA Special Issue on Computational Science-New Dimensions and Perspectives NCCSE, pp. 166–172 (2011)
101. Prasad, M., Sudha, K.: Chaos image encryption using pixel shuffling. CCSEA **1**, 169–179 (2011)
102. Samson, C., Sastry, V.: A novel image encryption supported by compression using multilevel wavelet transform. IJACSA) Int. J. Adv. Comput. Sci. Appl. **3**(9) (2012)
103. Kaur, M., Kumar, V.: A comprehensive review on image encryption techniques. Arch. Comput. Methods Eng. **27**(1), 15–43 (2020)
104. Dixit, P., Gupta, A.K., Trivedi, M.C., Yadav, V.K.: Traditional and hybrid encryption techniques: a survey. In: Networking Communication and Data Knowledge Engineering, Springer, pp. 239–248 (2018)
105. Adedeji Kazeem, B., Akinlolu, P.: A new hybrid data encryption and decryption technique to enhance data security in communication networks: algorithm development. Int. J. Sci. Eng. Res. **5**(10) (2014)
106. Hossain, M.B., Rahman, M.T., Rahman, A.S., Islam, S.: A new approach of image encryption using 3d chaotic map to enhance security of multimedia component. In: 2014 International Conference on Informatics, Electronics & Vision (ICIEV), IEEE, pp. 1–6 (2014)
107. Singh, K., Samaddar, S.G.: Enhancing koyama scheme using selective encryption technique in rsa-based singular cubic curve with avk. IJ Netw. Security **14**(3), 164–172 (2012)
108. Qiu, L., Yu, Y.: An efficient scheme for joint compression and encryption. J. Discrete Math. Sci. Cryptogr. **17**(5–6), 539–548 (2014)
109. Alabaichi, A., Ahmad, F., Mahmod, R.: Security analysis of blowfish algorithm. In: 2013 Second International Conference on Informatics and Applications (ICIA), IEEE, pp. 12–18 (2013)
110. Iyer, S.C., Sedamkar, R., Gupta, S.: A novel idea on multimedia encryption using hybrid crypto approach. Proc. Compu. Sci. **79**, 293–298 (2016)
111. Younes, M.A.B.: A survey of the most current image encryption and decryption techniques. In. J. Adv. Res. Comput. Sci. **10**(1), 9 (2019)
112. Prathipa, N., Sathya, V.: A survey on image encryption techniques
113. Jasra, B., Moon, A.H.: Image encryption techniques: A review. In: 2020 10th International Conference on Cloud Computing, Data Science and Engineering (Confluence), IEEE, pp. 221–226 (2020)
114. Kumar, R.R., Mathew, J.: Image encryption: Traditional methods vs alternative methods. In: 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), IEEE, pp. 1–7 (2020)
115. Belazi, A., Abd El-Latif, A.A., Belghith, S.: A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process. **128**, 155–170 (2016)
116. Chai, X., Chen, Y., Broyde, L.: A novel chaos-based image encryption algorithm using dna sequence operations. Opt. Lasers Eng. **88**, 197–213 (2017)
117. Zhao, G., Chen, G., Fang, J., Xu, G.: Block cipher design: generalized single-use-algorithm based on chaos. Tsinghua Sci. Technol. **16**(2), 194–206 (2011)
118. Gu, G., Ling, J.: A fast image encryption method by using chaotic 3d cat maps. Optik **125**(17), 4700–4705 (2014)
119. Hua, Z., Yi, S., Zhou, Y.: Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process. **144**, 134–144 (2018)
120. Ghebleh, M., Kanso, A., Stevanović, D.: A novel image encryption algorithm based on piecewise linear chaotic maps and least squares approximation. Multimedia Tools Appl. **77**(6), 7305–7326 (2018)
121. May, R.M.: Simple mathematical models with very complicated dynamics. The Theory of Chaotic Attractors, pp. 85–93 (2004)
122. Zhou, Y., Bao, L., Chen, C.P.: A new 1d chaotic system for image encryption. Signal Process. **97**, 172–182 (2014)
123. Maryoosh, A.A., Mustafa, R.A., Dhaief, Z.S.: Image encryption techniques based on chaotic map. Int. J. Eng. Res. Adv. Technol IJERAT (ISSN: 2454-6135) **5**(9), 01–05 (2019)
124. Li, Y., Wang, C., Chen, H.: A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Opt. Lasers Eng. **90**, 238–246 (2017)
125. Han, C.: An image encryption algorithm based on modified logistic chaotic map. Optik **181**, 779–785 (2019)
126. Talhaoui, M.Z., Wang, X., Midoun, M.A.: A new one-dimensional cosine polynomial chaotic map and its use in image encryption. The Visual Computer pp. 1–11 (2020)
127. Hsu, H., Lee, R.: Dna based encryption methods. In: The 23rd Workshop on Ccombinatorial Mathematics and Computation theory, Citeseer, p. 545 (2006)
128. Niyat, A.Y., Moattar, M.H.: Color image encryption based on hybrid chaotic system and dna sequences. Multimedia Tools Appl. **79**(1–2), 1497–1518 (2020)
129. Li, C., Chen, G.: Chaos in the fractional order chen system and its control. Chaos Solitons Fractals **22**(3), 549–554 (2004)
130. Chai, X., Zheng, X., Gan, Z., Chen, Y.: Exploiting plaintext-related mechanism for secure color image encryption. Neural Comput. Appl., pp. 1–24 (2019)
131. Chen, J., Chen, L., Zhou, Y.: Cryptanalysis of a dna-based image encryption scheme. Inf. Sci. **520**, 130–141 (2020)
132. Chai, X., Fu, X., Gan, Z., Lu, Y., Chen, Y.: A color image cryptosystem based on dynamic dna encryption and chaos. Signal Process. **155**, 44–62 (2019)
133. Zhan, K., Jiang, W.: Novel four-wing hyper-chaos system and its application in image encryption. Comput. Eng. Appl. **53**(12), 36–44 (2017)
134. Hameed, S.M., Al-Ani, M., et al.: Image encryption using dna encoding and rc4 algorithm. Iraq. J. Sci. **59**(1B), 434–446 (2018)
135. Mondal, B., Mandal, T.: A light weight secure image encryption scheme based on chaos and dna computing. J. King Saud Univ. Comput. Inf. Sci. **29**(4), 499–504 (2017)
136. Jin, J.: An image encryption based on elementary cellular automata. Opt. Lasers Eng. **50**(12), 1836–1843 (2012)
137. Niyat, A.Y., Moattar, M.H., Torshiz, M.N.: Color image encryption based on hybrid hyper-chaotic system and cellular automata. Opt. Lasers Eng. **90**, 225–237 (2017)
138. Chai, X., Gan, Z., Yang, K., Chen, Y., Liu, X.: An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and dna sequence operations. Signal Process. Image Commun. **52**, 6–19 (2017)
139. Li, M., Lu, D., Wen, W., Ren, H., Zhang, Y.: Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata. IEEE Access **6**, 47,102–47,111 (2018)
140. Khedmati, Y., Parvaz, R., Behroo, Y.: 2d hybrid chaos map for image security transform based on framelet and cellular automata. Inf. Sci. **512**, 855–879 (2020)
141. Li, X., Xiao, D., Wang, Q.H.: Error-free holographic frames encryption with ca pixel-permutation encoding algorithm. Opt. Lasers Eng. **100**, 200–207 (2018)
142. Babaei, A., Motameni, H., Enayatifar, R.: A new permutation-diffusion-based image encryption technique using cellular automata and dna sequence. Optik **203**(164), 000 (2020)
143. Naskar, P.K., Bhattacharyya, S., Nandy, D., Chaudhuri, A.: A robust image encryption scheme using chaotic tent map and cellular automata. Nonlinear Dyn. (2020)

144. Su, Y., Wo, Y., Han, G.: Reversible cellular automata image encryption for similarity search. Signal Process. Image Commun. **72**, 134–147 (2019)
145. Yao, L., Yuan, C., Qiang, J., Feng, S., Nie, S.: An asymmetric color image encryption method by using deduced gyrator transform. Opt. Lasers Eng. **89**, 72–79 (2017)
146. Li, C.L., Li, H.M., Li, F.D., Wei, D.Q., Yang, X.B., Zhang, J.: Multiple-image encryption by using robust chaotic map in wavelet transform domain. Optik **171**, 277–286 (2018)
147. Ren, G., Han, J., Fu, J., Shan, M.: Asymmetric image encryption using phase-truncated discrete multiple-parameter fractional fourier transform. Opt. Rev. **25**(6), 701–707 (2018)
148. Kumar, S., Panna, B., Jha, R.K.: Medical image encryption using fractional discrete cosine transform with chaotic function. Med. Biol. Eng. Comput. **57**(11), 2517–2533 (2019)
149. Meng, L., Yin, S., Zhao, C., Li, H., Sun, Y.: An improved image encryption algorithm based on chaotic mapping and discrete wavelet transform domain. IJ Netw. Security **22**(1), 155–160 (2020)
150. Shafique, A., Ahmed, F.: Image encryption using dynamic s-box substitution in the wavelet domain. Wireless Personal Commun. **115**(3), 2243–2268 (2020)
151. Karmakar, J., Mandal, M.K.: Chaos-based image encryption using integer wavelet transform. In: 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, pp. 756–760 (2020)
152. Shakir, H.R.: An image encryption method based on selective aes coding of wavelet transform and chaotic pixel shuffling. Multimedia Tools Appl. **78**(18), 26,073–26,087 (2019)
153. Annaby, M., Rushdi, M., Nehary, E.: Color image encryption using random transforms, phase retrieval, chaotic maps, and diffusion. Opt. Lasers Eng. **103**, 9–23 (2018)
154. Li, Gd., et al.: Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform. Vis. Comput. **35**(9), 1267–1277 (2019)
155. Song, C.Y., Qiao, Y.L., Zhang, X.Z.: An image encryption scheme based on new spatiotemporal chaos. Optik Int. J. Light Electron Opt **124**(18), 3329–3334 (2013)
156. Wang, X., Qin, X., Liu, C.: Color image encryption algorithm based on customized globally coupled map lattices. Multimedia Tools Appl. **78**(5), 6191–6209 (2019)
157. Hu, T., Liu, Y., Gong, L.H., Guo, S.F., Yuan, H.M.: Chaotic image cryptosystem using dna deletion and dna insertion. Signal Process. **134**, 234–243 (2017)
158. Oravec, J., Turan, J., Ovsenik, L.: Image encryption technique with key diffused by coupled map lattice. In: 2018 28th International Conference Radioelektronika (RADIOELEKTRONIKA), IEEE, pp. 1–6 (2018)
159. Wang, X., Zhao, H., Wang, M.: A new image encryption algorithm with nonlinear-diffusion based on multiple coupled map lattices. Opt. Laser Technol. **115**, 42–57 (2019)
160. Nematzadeh, H., Enayatifar, R., Motameni, H., Guimarães, F.G., Coelho, V.N.: Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. Opt. Lasers Eng. **110**, 24–32 (2018)
161. Xingyuan, W., Le, F., Shibing, W., Zhang, C., Yingqian, Z.: Spatiotemporal chaos in coupled logistic map lattice with dynamic coupling coefficient and its application in image encryption. IEEE Access **6**, 39,705–39,724 (2018)
162. Yu W, Liu Y, Gong L, Tian M, Tu L (2019) Double-image encryption based on spatiotemporal chaos and dna operations. Multimedia Tools Appl. **78**(14), 20,037–20,064
163. Zhang, Y.Q., He, Y., Wang, X.Y.: Spatiotemporal chaos in mixed linear-nonlinear two-dimensional coupled logistic map lattice. Phys. A Stat. Mech. Appl. **490**, 148–160 (2018)
164. Yj, Sun, Zhang, H., Xy, Wang, Xq, Wang, Pf, Yan: 2d non-adjacent coupled map lattice with q and its applications in image encryption. Appl. Math. Comput. **373**(125), 039 (2020)
165. Zhang, H., Wang, X., Xie, H., Wang, C., Wang, X.: An efficient and secure image encryption algorithm based on non-adjacent coupled maps. IEEE Access **8**, 122,104–122,120 (2020)