SURVEY ON IMAGE CRYPTO SYSTEM TECHNIQUES USING CHAOTIC MAPS

1RenukaPatel
renukapatelmca@gmail.com
Research Scholar, Computer Science
Madhyanchal Professional University,
Bhopal (M.P.)

2 Dr. Ankit Temurnikar
Assistant Professor, Computer Science
Madhyanchal Professional University,
Bhopal (M.P.)

3 Dr. Teerath Prasad Patel
teerath.patel@gmail.com
Head of Computer Science Department
Govt.College Narela ,Bhopal (M.P.)

4 Mr. Rohit Singh Thakur
rohitthakur_2006@rediffmail.com
Research Scholar, Computer Science
Ravindra Nath Tagore University,
Bhopal M.P.

5.Dr. Rais Khan
raiskh2001@gmail.com
Computer Science Department
Govt.College Narela ,Bhopal (M.P.)

Abstract

Today general problem of society is undoubtedly security of digital image. Security of image in different stages like transferred, processed and stored thought digital channels (Guided or unguided media). In this era image cryptosystem has become an attractive and interesting field for research. Image cryptography improved the security of image from unauthorized sources. There are many algorithms and methods for making transmission secure and more reliable. Image watermarking is one of the favorite methods for encrypt order cryptan image.Chaos theory, due to its randomness and unpredictable behavior is more suitable for encryption, its characteristic is quite helpful in different encryption techniques and for multimedia security. Both image watermarking and chaos theory have its own methods, pros and cons. cryptography which are based on Chaos like Chebyshev polynomials can increase security when used with traditional public key cryptography like RSA and El-gamal, despite the fact that these methods are not standardized like AES, DES, RSA, etc. While chaos-based encryption methods are generally recommended by researchers due to their high computational efficiency, encryption algorithms like AES have historically been the preferred option when it comes to images or videos. In order to facilitate comprehension, this article surveys the most recent spatiotemporal, temporal, and spatial-temporal chaos-based image encryption methods. There is a discussion of the major advancements in image encryption. Additionally, comparative analysis is carried out to verify the evaluation matrices used in recent articles to quantify the security and efficiency of encryption algorithms.

Keywords: Chaoticmaps·Spatialdomain·Transformdomain·Spatiotemporaldomain·Imageencryption

DOI: 10.53555/ecb/2022.11.12.210

Introduction

New digital communication and network technologies are developing and being adopted quickly,

Section: Research Paper
ISSN 2063-5346

and they have the ability to greatly improve data storage and transfer over the Internet. However, it is equally important to safeguard sensitive data, which is why network security and data accuracy have consistently been major concerns. Scientists have responded by taking the necessary precautions to avoid security flaws and increase visibility. Images make up the majority of the multimedia that is shared and saved online. Therefore, image encryption ensures the authenticity and security of digital images.

With the help of a mathematical algorithm, image encryption makes the original image difficult to decipher and thereby increases resistance to security attacks like brute force [1], statistical [2], and differential attacks [3]. Many industries, including business, telemedicine, medicine, biometric authentication, and military contact, use image encryption. To address these security concerns, a number of image encryption techniques have been offered, including digital watermarking [4], image scrambling [5], digital image steganography [6], and digital image cryptography [7]. Due to chaotic basic characteristic of sensitivity to initial parameters, which results in data sets that are deterministic but appear random, chaos has recently attracted a lot of attention in the field of cryptography. With regard to speed, cost, computational overhead, complexity, vulnerability, etc., chaos-based cryptosystemmethods have been used to create innovative techniques for designing effective image encryption systems.

This article provides a theoretical overview of current studies that published chaos-based image encryption techniques between 2018 and 2022. Our study divides the spatiotemporal, temporal, and spatial areas of chaos-based encryption schemes. The goal of this separation is to group the developments in chaos-based digital image cryptography techniques so that users with varying levels of expertise in this field could easily focus on the topics that were of most interest to them. This paper provides a road plan for how chaos-based cryptosystems implemented for digital data, like as images and videos. There has also been a comprehensive comparison of traditional and chaos-based cryptographic schemes. Anabstract of some recent cryptanalytic attacks has been discussed while taking into account various attack model types.An evaluation matrix for the types of attack models used to verify the suggested algorithms has been given under each group classified.The remaining part of this paper is as follows: Sect. 2 gives a summary of chaos theory. Image encryption is discussed in Section 3 along with how it relates to chaos-based cryptography. Associated activity is included in Section 4. In Section 5, evaluation criteria are covered. The survey of digital image encryption in the temporal, spatial, and spatiotemporal areas is presented in Section 6. In Section 7, the closing remarks are given.

Image Encryption

Earlier 1960s and 1970s chaotic dynamics can be linked to improve digital computer processing power. Due to this increased processing power allowed a wide range of nonlinear techniques could be investigated for the very first time. Important characteristics of these systems are the presence of unknown attractors and the dissimilar behavior of neighboring trajectories on these attractors. These characteristics work together to create a time-line that, despite being completely deterministic, looks random. Because of this perceived randomness, chaotic systems are advantageous for encryption.

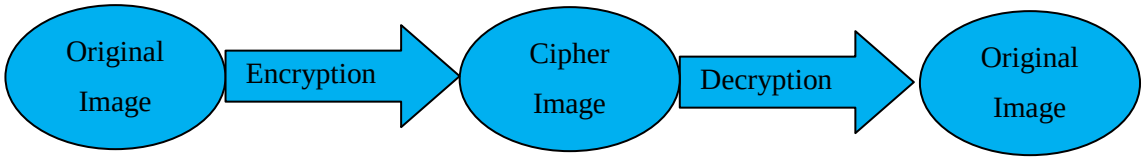


Figure 1: Cryptography

Encoding is defined in cryptography as the act of transforming usable information into an unpredictable form in order to protect it from unauthorised access. The picture content has critical qualities such as redundancy, capacity, space, and correlation among the bit pixels, necessitating the use of a few types of encryption techniques, the primary goal of which is to safely send data (the image [8]) over a network.An encryption algorithm is used to turn the original image into a cypher image, which conceals the true information from outsiders. As a result, a decoding mechanism is utilised at the receiving end to decode the picture into the original image. Furthermore, in the image cryptography process, the original picture is encoded using a key at the sender end, and for the image decryption process, a decryption mechanism is built to retrieve the image. The keys used in picture encoding and decoding are widely classified as symmetric or asymmetric (as illustrated in Fig. The same key is used for encoding and decoding in symmetric key (private key) cryptography, but distinct keys are used in asymmetric key (public key) cryptography, requiring a pair of private and public keys for encryption and decryption.

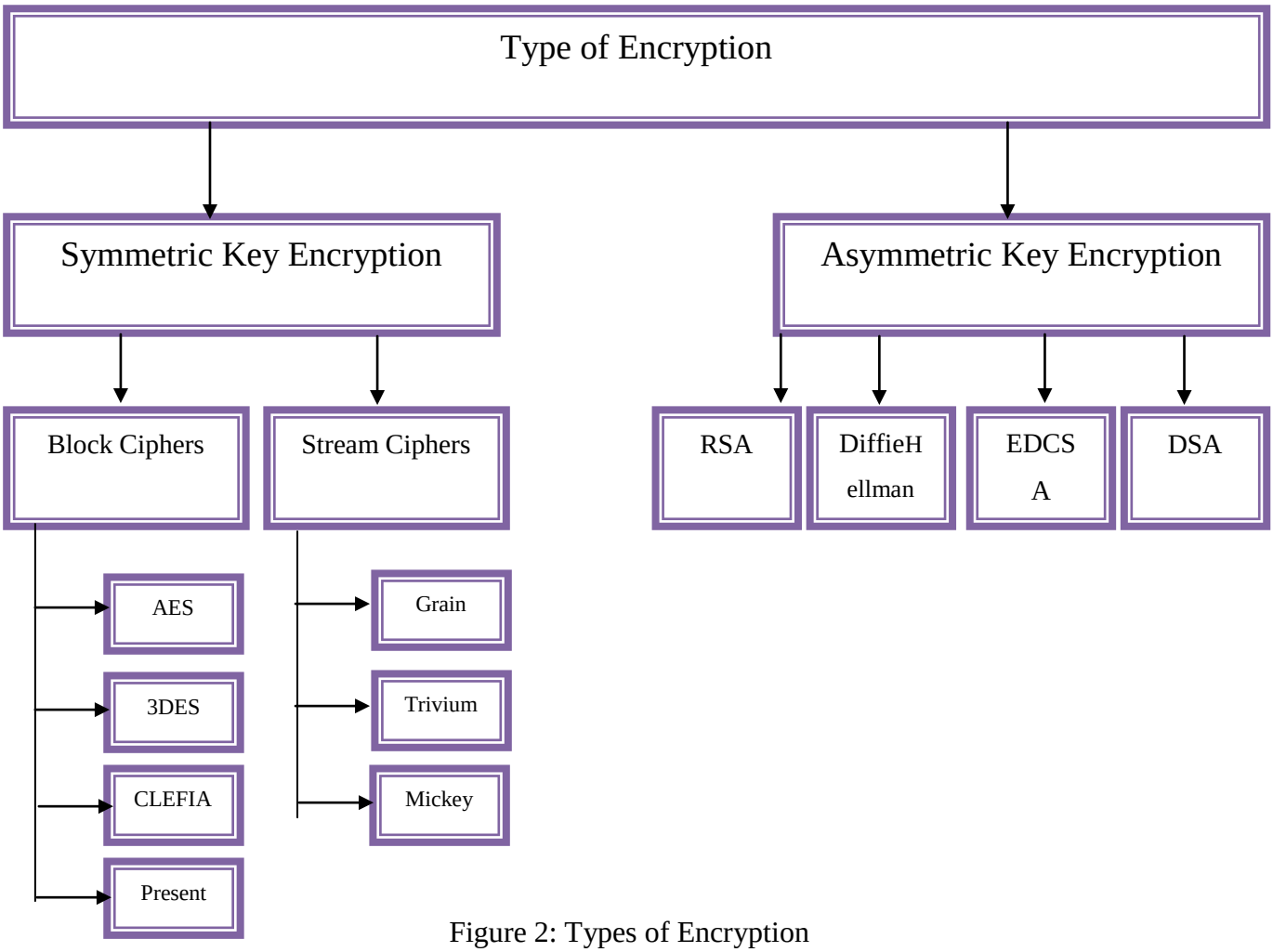


Figure 2: Types of Encryption

Cryptography using Symmetric key

Using Cryptography Because it only requires a single key for encryption and decryption, symmetric key encryption is also known as private key or secret key encryption [9]. The transmitter

encrypts the picture using a private key, which is subsequently transferred to the recipient over the transmission media. Symmetric encryption is further subdivided into Stream and Block Cyphers, as seen in Fig. Stream cyphers operate on single bits of data at a timeGrain [10], Trivium [11], and Micky [12] are examples of lightweight stream cyphers that are quicker than block cyphers. Block cyphers, on the other hand, encrypt data by encrypting a fixed-size piece of data called a block. Block cyphers utilise an initialization vector as an extra layer of defence against brute force attacks. Block cyphers include the Advanced Encryption Standard (AES) [13], Triple Data Encryption Standard (3-DES) [14], CLEFIA [15], and PRESENT [16]..

Asymmetric key cryptography

Asymmetric cryptography (public key) encrypts and decrypts using two separate keys [17].Asymmetric keys employ 2n keys, where n is the number of members in a group. Both the sender and the receiver have a pair of keys known as public and private keys. The private key is not disclosed to anyone, but the public key is disclosed to the sender. Digital Signature Algorithm (DSA) [18], ECDSA [19], Rivest Shamir Adleman (RSA) [20], and DiffieHellman [21] are examples of asymmetric key cryptographic algorithms.

Chaos-based image encryption

When developing secure picture encryption and transmission techniques in the presence of an attacker [22]. Traditional cyphers such as AES and DES are efficient for text encryption but ineffective for picture encryption due to the repeating data that pixels in related images depict. This issue is solved by chaos-based encryption algorithms, which produce randomly distributed keys that encrypt the picture data in the cypher images [23].Even though closely related, these two scientific ideas offer a good combination of enhanced performance, high levels of security, and a number of practical applications, including secure communications [26], image and video encryption [27], and the generation of pseudo-random numbers for stream and block ciphers [25]. Because these features are analogous to the confusion and diffusion aspects of an effective cryptosystem, the special characteristics of chaotic systems, such as determinacy, ergodicity, and sensitivity to beginning circumstances, make it a viable alternative for developing cryptosystems. With the continued research in the disciplines of picture encryption and cryptanalysis, several chaotic image encryption algorithms and enhanced strategies that have the ability to overcome a number of security risk shave been proposed.In designing the chaos-based algorithm, choosing the chaotic maps is the first and possibly most difficult stage [30]. Researchers started the design process by using simpler chaotic maps, like the tent map and the logistic map, which have a limited key area and provide insufficient security. Later, as encryption algorithm design progressed, chaotic maps with bigger dimensions were included, resulting in a faster, more secure, and higher-quality cryptosystem. A few chaotic maps that have been examined for picture encryption are 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].

Chaos-based image cryptosystem architecture

The two primary stages of the chaos-based image cryptosystem architecture are the diffusion phase and the confusion phase. The confusion phase, also known as the pixel per-mutation, happens when

pixel locations are randomly rearranged over the whole image but pixel values remain constant, resulting in an unrecognisable image. As a result, when the diffusion phase is carried out with the aid of a chaotic map, the sequence produced by the chaotic systems changes the values of the pixels throughout the entire picture sequentially.

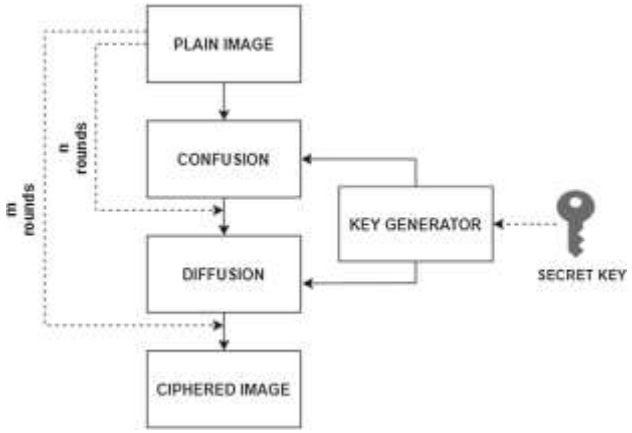


Fig.2 Chaos-basedimagecryptosystemarchitecture

Conventional Cryptography vs Chaos-Based Cryptography

Images differ from textual data in several ways, including high data redundancy, scattered information, huge size data, strong connection between neighbouring pixels, and bulk data capacity [37, 38]. A two-dimensional image must first be turned into a one-dimensional data stream in order for photo encryption to work. Text-based cryptosystems are then used to encrypt this data stream. Digital multimedia applications do not, however, need to meet this criterion because a small change in a pixel's attribute does not significantly impair the quality of the image. Additionally, the intensity values in an image's pixel data vary from [0, 255]. The encrypted value for a pixel is set when converting images using conventional algorithms according to the encryption key used, and because the pixel value appears numerous times in an image (data redundancy), the adversary can easily predict that value. The finest encryption algorithms are those that require the least amount of computation time without sacrificing security. Unfortunately, textual data is usually more effectively protected using traditional cryptographic techniques like AES, DES, TDES, IDEA, and RSA [39]. Due to the unique characteristics of images, these methods are not appropriate for real-time image encryption. Furthermore, when used with commercial software, these methods are difficult to execute and demand a lot of computational resources. In contrast, chaos-based cryptographic approaches provide a variety of advantages, including better flexibility, high security, lower computational overheads, less computer power, and ease of implementation. Furthermore, in the majority of chaos-based encryption techniques, the encryption key is confused and diffused at the pixel level [40-42].

Cryptanalysis

To this point, several picture encryption algorithms have been published in the literature. For example, Eli Biham et al. Biryukov et al. Li et al. [52] successfully decoded a chaotic permutation and diffusion-based image encryption method [53], as well as discovering the technique's sensitivity to chosen-plaintext attacks. An all-zero picture was employed in the presented work to break the original diffusion phase, and plaintext images were used to crack the original permutation phase.Similarly, Dou et al.'s [54] effective use of the 1D chaotic map and chosen-plaintext attack [33] to defeat the colour picture

Section: Research Paper
ISSN 2063-5346

encryption approach.. Wang et al. The approach presented might overcome Pak's scheme's diffusion and permutation matrices while also improving the picture encryption algorithm by including global plain information. In [56], Li et al. The chosen-ciphertext attack developed by Solak et al. was used to cryptanalyze the Fridrich technique [57] for successful chaotic picture encryption, which is based on two-dimensional Baker mapping.The authors built a causality-based tree to decompose the permutation matrix. The study presented in [47] inspired Xie et al. The research [59] explored the symmetric key picture encryption issue and discovered that it was exploitable by efficiently using the chaotic Rossler system [60]. Diab et al. [61] proposed an attack model to crack Chen's image encryption technique [62] by using multiple sets of plain/cipher pictures. Alvarez et al. [64] completely demolished the Feki et al.

Related Work

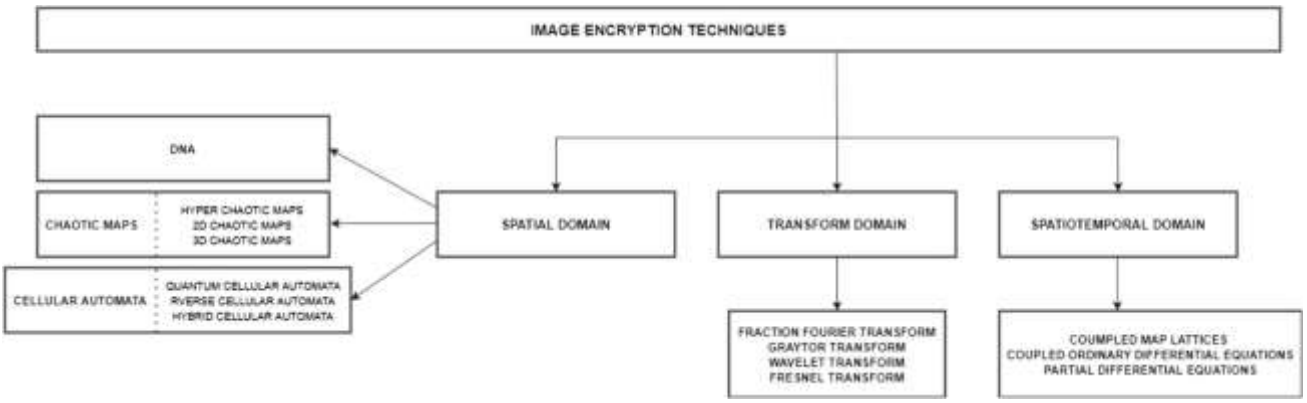
This section offers a survey of newly reported chaos-based picture encryption algorithms. Several picture encryption algorithms have been proposed, each with its own set of strengths and weaknesses. Image encryption approaches based on chaos and organised into spatial, temporal, and spatiotemporal domains are described in this study, as seen in Fig. 3.

For theoretical review and analysis, many performance metrics such as Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), Key Analysis (KA), Histogram Analysis (HA), Coefficient Correlation (CC), Information Entropy (IE), and Noise Attack (NA) are utilised. Recently [79], a review of 10 classical and five chaos-based picture encryption algorithms [65-78] was published. Additionally, they came to the conclusion that RC4 [80], AES [81], and chaotic scheme 15 image encryption proved to be computationally effective and had quicker execution periods than other encryption algorithms under consideration. While stenography techniques were used to increase the system's security, encryption techniques were used to transform the input image into a cipher image. The study also conducted a detailed evaluation of these algorithms based on several performance indicators such as UACI, histogram analysis, key analysis, NPCR, noise, coefficient correlation, information entropy, and encryption speed. The study's findings indicate that image encryption based on meta-heuristic algorithms and a range of imaging systems, such as underwater, remote sensing, multi-spectral, and 3D imaging systems, still has a lot of space for development.
The authors of [104] performed a post-quantum analysis on several traditional and current hybrid encryption methods, including 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]. [111] provided an overview of image encryption and cryptography as well as a quick review of current image encryption methods that protect sensitive data. Therefore, these methods can be improved further to create new methods to lower the danger of data security and integrity.

The authors also discussed and reviewed eleven publications dealing with picture encryption techniques in order to support future development in the functionality of these encryption methods and raise their degree of protection against security assaults. According to the author's analysis of the methods discussed in the paper, chaos-based encryption techniques are more secure and straightforward due to their rapid encryption and decryption of large images. Image encryption varies from other types of multimedia encryption owing to the large quantity of data it can carry and the high pixel correlation that renders traditional encryption approaches ineffective.To ensure the methods'

validity, each picture encryption algorithm must be assessed against security restrictions prior to creation.

[114] studied 13 articles on various elements of picture encryption methods and evaluated their usefulness based on a variety of parameters such as complexity, processing time, correlation coefficient, PSNR, entropy, NCPR, and numerous performance metrics.



Evaluation measures

The factors of performance Differential analysis, statistical analysis, information entropy, key sensitivity, and noise attack are used to assess the effectiveness of the picture encryption algorithms mentioned.

Differential analysis (DA)

Differential attack analysis is used to analyse the differences in the encrypted picture after delivering a little adjustment to a single pixel of the plain image. To evaluate differential assaults, two metrics are commonly used: the Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI).

Number of pixel change rate (NPCR)

The percentage of distinct pixel numbers between two encrypted images is determined using NCPR. A high NCPR number means that the encryption algorithm can more effectively withstand differential attacks. These steps [115] can be used to calculate the NPCR:

$$NPCR = \frac{\sum i, jD(i, j)\,\mathrm{x}100}{WXH} \qquad (1)$$

$$D(i,j)= 0 \text{ if } E(i,j)=E`(i,j) \qquad (2)$$

$$D(i,j)=1 \text{ if } E(j,j) != E`(i,j)$$

Where

E(i, j) is encrypted original image.

E t (i, j)is encrypted image.

D(i, j) indicate difference between pixels of the encrypted original and change image.

W represent width of image.

H represent height of image.

Section: Research Paper
ISSN 2063-5346

Unified Average Changing Intensity (UACI)

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

$$UACI = \frac{\sum_{i,j} \mathrm{E}(i,\ j) - \mathrm{E`(i,\ j)\ x100}}{255XWXH} \qquad (3)$$

Where
E(i,j) is encrypted image oforiginal
E`(i,j) is encrypted image of modified image

Correlation coefficient analysis (CCA)

CCA is used to determine the correspondence between neighbouring pixels in the original and encrypted images. The pixels in the initial image have strong correlations in all three planes—horizontally, vertically, and diagonally—but there should be no connection between the encrypted image's neighbouring pixels. Higher correlation between neighbouring pixels denotes statistical attack sensitivity, so good encryption algorithms tend to lower the coefficient numeric. The following algorithm is used to determine the correlation coefficient:

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

where

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

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

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

C(x, y) is the co-variance among 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.

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:

$$H(S) = -\sum_{S} (\mathrm{P(s_i)\ x log_2 P(s_i)}) \qquad (8)$$

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

Key analysis (KA)

The security keys are crucial to image encryption because they are in charge of preserving data confidentiality. Key sensitivity and key space are used to evaluate a key's power. The efficacy of the key space is indicated by the size of the secret key. The greater the key space, the larger the size, which makes it challenging for the adversary to generate a key with a comparable size. The best example of key sensitivity is when a tiny change in the key used to encrypt an image prevents the image from being decrypted. The characteristics of a successful encryption algorithm are therefore a large key space and great sensitivity.

Noise attack (NA)

Analyzing noise attacks is crucial for effective picture encryption. Here, an unintended user adds noise to the encrypted image, rendering it unrecoverable after decryption (e.g., Gaussian noise, salt and pepper noise, spackle noise, Poisson noise, etc.).

Chaos-based image encryption survey in various domains

Image encryption in spatial domain

The encryption method uses direct operations on image pixels in the spatial domain. The following sections discuss the theoretical analysis and further categories the methods based on the spatial domain into different groups.

Image encryption techniques based on Chaotic maps

The beginning circumstances and map control parameters can be utilised as keys to construct time series from chaotic maps, which look pseudo-random. The neighbouring pixels are then instantly scrambled, and pixel adaptive diffusion is employed to distribute the included random data over the whole picture.[120] proposed a picture encryption approach based on least squares approximations and chaotic maps, consisting of two basic stages, namely shuffling and masking (using 1D piece-wise linear chaotic maps).

An image encryption method based on the two-dimensional (2D) Logistic-Sine-Coupling map was introduced by Z. Hua et al. [34]. (LSCM). The 2D-LSCM is composed by combining two 1D chaotic maps, the Logistic map [121] and the Sine map [122].

The Logistic map is given as

$$x_i + 1 = 4\eta x_i (1 - x_i) \qquad (9)$$

The parameter η has the interval [0,1], while the sine map is defined as:

$$x_i + 1 = \beta \sin(\pi x_i) \qquad (10)$$

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

Section: Research Paper
ISSN 2063-5346

$$x_{i+1} = \sin(\pi(4\theta x_i(1-x_i) + (1-\theta)\sin(\pi y_i)))$$
$$y_{i+1} = \sin(\pi(4\theta y_i(1-y_i) + (1-\theta)\sin(\pi x_i + 1))) \quad (11)$$

While the latter is used to uniformly distribute minor alterations in the cypher picture over the full encrypted image, the former is used to relocate image pixels to different rows and columns. [123] proposed an image encryption approach based on the combination of the dynamic S-box, logistic map, and Lorenz system. Later, the key stages are added, and the required picture is produced as an XOR image. The proposed technique is tested using a number of performance measures, including entropy, histogram, key space, correlation, NPCR, and UACI, to demonstrate its efficacy and resilience against statistical and differential assaults. A hyper-mayhem based picture encryption procedure was proposed by Li et al. The exhibition examination shows the vigor of the recommended technique with regards to relationship, histogram, differential investigation, key awareness, and key responsiveness examination. Chunyan Han et al [125] recommend a changed strategic guide picture encryption technique to fix the imperfections of low security and restricted key space in the one-aspect calculated map when applied in picture encryption. Recreations and exploratory investigation finished up high key responsiveness and security, endless key space against measurable assaults. A 1-D cosine polynomial (1-DCP) tumultuous guide was as of late presented in picture encryption by Wang et al [126]. The strength of the proposed calculation lies in its straightforward system, bigger key space and quicker processing time than other existing 1-D guides.

Table 1:shows the comparison of a few recent papers using their own performance evaluation matrices for high security and faster chaos-based image encryption methods. The proposed scheme's robustness and effectiveness in comparison to other techniques is supported by experiments and findings. Based on the evaluation matrices they used to evaluate the effectiveness of chaos-based image encryption techniques, Table 1 compares a few recent articles.

REFERENCE	**Number of Pixel Change rate**	**Unified Average Changing Intensity**	**Key Analysis**	**Histogram Analysis**	**Correlation Coefficient Analysis**	**Information Entropy**	**Noise Attack**
118	☑	☑	☑	☑	☒	☒	☒
119	☑	☑	☑	☑	☑	☑	☒
120	☑	☑	☑	☒	☒	☒	☒
34	☑	☑	☑	☑	☑	☑	☒
123	☑	☑	☑	☑	☒	☒	☑
33	☑	☑	☑	☑	☑	☑	☒
124	☒	☒	☑	☑	☒	☒	☒
125	☑	☑	☑	☑	☑	☑	☑
126	☑	☑	☑	☑	☑	☑	☒

NCPR	-	**Number of Pixel Change rate**
UACI	-	**Unified Average Changing Intensity**
KA	-	**Key Analysis**
HA	-	**Histogram Analysis**
CC	-	**Correlation Coefficient Analysis**
IE	-	**Information Entropy**
NA	-	**Noise Attack**

DNA-based image encryption techniques

Because of its natural characteristics of incredibly low power utilization, high data thickness, and gigantic parallelism, Deoxyribonucleic Corrosive (DNA)- based picture encryption has as of late drawn interest from scientists. To make safer picture encryption methods, DNA encryption is joined with bedlam based picture encryption. The tumultuous picture is gained utilizing the key streams, and in the wake of being partitioned into equivalent blocks, alongside the permuted picture, picture encryption is done hinder by-block. While a dispersion strategy subject to the plaintext and mixed picture (DM-DPSI) is proposed for changing the permuted picture pixels and getting the code picture, a plaintext-related Latin-square-based block stage (PLBP) is given for rearranging the plain picture pixels. Turbulent examples are created by powerfully picking the seed values for the one-layered tumultuous system. Additionally, the three variety picture parts are exposed to picture stage and dispersion tasks while the beginning qualities and boundaries are figured utilizing the outside keys and the plain picture. The exploratory discoveries exhibit solid execution, a significant key space, and a more serious level of safety.The plain picture and outside keys are utilized to ascertain the beginning qualities and boundaries, and the three variety picture parts are additionally exposed to picture stage and dispersion activities.
Chai et al. [132] have proposed a variety picture cryptosystem in light of dynamic DNA and a four-wing hyper-mayhem. The variety picture is first separated into its three essential tones, and afterward turbulent groupings are made by executing the tumultuous framework. The turbulent framework's underlying qualities are determined by melding the outer keys and the plain picture's SHA-384 hash esteem. The four-wing hyper-turbulent framework is displayed in the accompanying manner:

$$x = ax + byz$$
$$y = cy + dxz$$
$$z = exy + kz + mxw$$
$$w = ny$$

where x , y and z are state variables of the hyper-chaotic

System, where w is the state feedback controller, and a, b, c, d, e, k, m, and n are system constant constants. Second, a Simultaneous Intra-Inter Component Permutation Mechanism Dependent on the Plaintext is used to combine the RGB colour picture components. (SCPMDP). Next, a diffusion mechanism based on random numbers related to plaintext (DMRNRP) is suggested to replace the DNA sequences of the plain image. The DNA decoding principles are used to divide the DNA matrix into three parts. The experimental study demonstrates that the suggested algorithm performs satisfactorily in terms of security and robustness.

Reference	**Number of Pixel Change rate**	**Unified Average Changing Intensity**	**Key Analysis**	**Histogram Analysis**	**Correlation Coefficient Analysis**	**Information Entropy**	**Noise Attack**
128	☑	☑	☑	☑	☑	☑	☑
130	☑	☑	☑	☑	☑	☑	☑
131	☒	☒	☒	☒	☒	☒	☒
132	☑	☑	☑	☑	☑	☑	☑
134	☒	☒	☒	☑	☑	☒	☒
135	☑	☑	☑	☑	☑	☑	☑

This table 2 compares recent articles using the evaluation matrices they used to assess the effectiveness of DNA-based encryption techniques.

NCPR - **Number of Pixel Change rate**
UACI - **Unified Average Changing Intensity**
KA - **Key Analysis**
HA - **Histogram Analysis**
CC - **Correlation Coefficient Analysis**
IE - **Information Entropy**
NA - **Noise Attack**

A technique to encrypt images using DNA encoding and the Rivest Cipher (RC4) was introduced in 2018 [134]. The suggested scheme raises the plain image's degree of confidentiality and randomness without lowering its quality. Analysis and simulation results demonstrate that the proposed algorithm exhibits a high level of security.

A simple image encryption method based on DNA computing and pseudo-random numbers (PRN) was proposed by the writers of [135]. The picture's pixels are permuted using a series of pseudo-random numbers, and the permuted image is then encrypted using DNA computation. Currently, the approach is only applicable to grayscale images, but it may one day be expanded to include coloured images as well. The suggested algorithm is able to withstand statistical attacks, differential attacks, and noise, according to various tests and analyses. Table 2 compares recent studies using the performance evaluation matrices they employed to assess the effectiveness of DNA-based image encryption techniques.

Cellular automata (CA) image encryption techniques

Because of their characteristics of consistency, homogeneity, parallelism, and simplicity of execution in programming and equipment frameworks, cell automata (CA) have been generally utilized for picture encryption [136]. In picture encryption, picture handling, picture scrambling, validation, and security,

CA has exhibited promising results.To resolve the issue of the limited number of inversion rules, YaghoutiNiyat et al. The proposed technique is a decent choice for scrambling computerized pictures due to its bigger key space and high protection from clamor, measurable, and differential assaults, as indicated by trial discoveries and security investigation.

A picture encryption calculation is given in [138] and depends on the memristive hyper-turbulent framework, two-layered CA, and DNA succession activities. The viability of the recommended calculation is surveyed utilizing an assortment of reproduction investigations, which show that it offers secure and powerful picture encryption and is impervious to plaintext assaults. An alternate way to deal with recently distributed variety picture encryption techniques was advanced by Li et al. The proposed strategy utilizes a comparable change key stream, which keeps up with the amount of the worth of pixels at each variety channel steady, as opposed to the past procedure, which utilized the amount of upsides of the pixel part at each highlight gauge the beginning stage for the calculated guide. Use stage dispersion in various rounds.A 2D crossover turbulent guide picture encryption method has as of late been presented [140] for sending pictures securely. The technique utilizes cell automata and a discrete framelet change to blend the places of picture pixels by utilizing various movements. The proposed strategy can effectively endure known plaintext assaults, factual assaults, differential assaults, information misfortune, and commotion, as indicated by different tests and examinations.

To get around the disadvantages of customary encryption methods, Li et al. This approach beats the innate issue of regular 2D CA cover based encoding techniques that produce level examples by disturbing the laid out request of the picture pixels

. A picture encryption calculation is depicted in [142] and depends on DNA groupings and recursive cell automata (RCA). The proposed technique comprises of two key stages. The picture's pixel values are moved involving the calculated guide in the main stage, which is known as the cycle stage. The dissemination period of the subsequent stage utilizes both DNA and RCA successions to supplant the dim level of the old cells with new ones. Recreations and security research show that the new encryption technique functions admirably.

Reference	**Number of Pixel Change rate**	**Unified Average Changing Intensity**	**Key Analysis**	**Histogram Analysis**	**Correlation Coefficient Analysis**	**Information Entropy**	**Noise Attack**
137	☑	☑	☑	☑	☑	☑	☑
138	☑	☑	☑	☑	☑	☑	☑
139	☑	☑	☑	☑	☑	☑	☑
140	☑	☑	☑	☑	☑	☑	☑
141	☒	☒	☑	☑	☒	☒	☑
142	☑	☑	☑	☑	☑	☑	☒
143	☑	☑	☑	☑	☑	☑	☒
144	☑	☑	☑	☑	☑	☑	☒

Comparing new studies using their own performance evaluation matrices for cellular automata (CA)-based image encryption techniques is shown in table 3 above.

NCPR	-	**Number of Pixel Change rate**
UACI	-	**Unified Average Changing Intensity**
KA	-	**Key Analysis**
HA	-	**Histogram Analysis**
CC	-	**Correlation Coefficient Analysis**
IE	-	**Information Entropy**
NA	-	**Noise Attack**

A vigorous and secure picture encryption method in light of a turbulent tent guide and cell automata was proposed by Naskar, PrahirKurnar, and partners [143]. [144] proposed a reversible cell automata-based picture encryption method. To characterize a similitude search on the scrambled pictures, the introduced strategy utilizes pixel-based deterministic encryption. Furthermore, in light of the practicality of pixel-based deterministic encryption, the paper proposes deterministic encryption reversible cellu-lar automata (DERCA). A two level granularity calculation has likewise been proposed in light of DERCA to ensure a comparability search on scrambled pictures.. The adequacy of cell automata-based picture encryption strategies is analyzed in Table 3.

Image encryption in transform domain

For picture encryption, change-based cryptography has been broadly utilized. The given information is changed over from the spatial space to the recurrence area in the change space utilizing the proper changes, including the discrete cosine change (DCT), discrete wavelet change (DWT), gyroscope change (GT), and Fourier change (FT). [145] proposed a picture encryption method that utilizes the benefits of the derived gyroscope change to change over a variety of pictures to dim. The picture is changed utilizing the spinner change toward the start of the encryption system, and the subsequent picture is then increased by a stage conveyance p*, trailed by a Fourier change. The arbitrary stage veil is utilized to change the RGB parts of the variety picture, which is then consolidated by convolution. Also, the backward Fourier change is utilized during the picture decoding strategy. In this work, the first picture is partitioned into low recurrence parts utilizing the discrete wavelet change, which are then joined to make the plain picture. The subsequent mixed picture is then additionally partitioned to make block pictures, which are then coordinated with the hearty turbulent guide's (RCM) abundancy boundary to make key streams. Mathematical reproductions and analyses are utilized to affirm that the proposed calculation proceeds true to form.An original unbalanced picture encryption technique in view of stage shortened discrete various boundary fragmentary Fourier change was proposed by Ren et al. Preceding being stage shortened by DMPFRFT, the underlying picture is first mixed utilizing pixel scrambling and irregular cover. [149] have fostered a better picture encryption calculation in view of tumultuous planning and the discrete wavelet change area to resolve the issues with customary turbulent picture encryption methods, like serene responsiveness and low security. Through various rounds, grayscale dispersion and picture cleaning are applied to the underlying picture. resolved the issues that are habitually present in regular picture encryption strategies, for example, pixel stowing away of the first picture with low finished districts and delayed computational time. By utilizing numerous S-boxes with dynamic replacement, this

technique resolves the issue of pixel camouflage, and DWT's deterioration of the plain picture up to the fifth level disintegration extraordinarily lessens the calculation season of the encryption technique. To assess the viability of the proposed plot, mathematical reproductions are run..
In [151], a more successful tumultuous picture encryption calculation in view of worldwide piece scrambling (GBS) and whole number wavelet change (IWT) is recommended. The first picture is deteriorated involving IWT in the proposed calculation, and the picture is encoded utilizing a strategic guide and touch mixed utilizing GBS. The new picture encryption strategy depicted in this paper utilizes the calculated guide from [152] alongside the Haar wavelet change, High-level Encryption Standard (AES), and pixel mix. The picture is initially separated into its recurrence parts utilizing the Haar wavelet change, and afterward, the picture acquired in the primary stage is scrambled utilizing AES. Afterward, the picture's pixels are rearranged utilizing the strategic guide, expanding the encryption interaction's adequacy.
Analysts in [153] gave two encryption answers for address variety pictures' shortcomings in information overt repetitiveness, which makes them helpless against factual assaults. Stage recovery calculations, irregular fragmentary Fourier changes, combined with turbulent scrambling and dissemination methods, are utilized to make the recommended security arrangement. The proposed strategy is contrasted with beforehand existing procedures concerning NPCR, UACI, and entropy, it is more flexible and competent to show that it.The 2019 exploration [154] proposed a twofold tumultuous picture encryption calculation in view of a fragmentary Fourier change to address the disadvantages of existing picture encryption calculations. In light of the assessment grids they used to survey the viability of change based picture encryp-tion methods, Table 4 thinks about late examinations.

REFERENCE	Number of Pixel Change rate	Unified Average Changing Intensity	Key Analysis	Histogram Analysis	Correlation Coefficient Analysis	Information Entropy	Noise Attack
145	☒	☒	☑	☑	☑	☒	☑
146	☒	☑	☑	☑	☑	☒	☑
147	☒	☒	☒	☒	☒	☒	☑
148	☑	☑	☑	☑	☑	☑	☑
149	☑	☑	☑	☑	☒	☑	☒
150	☒	☒	☒	☑	☑	☑	☒
151	☑	☑	☑	☑	☒	☑	☒
152	☒	☒	☒	☑	☑	☑	☑
153	☑	☑	☑	☑	☑	☑	☑
154	☑	☑	☑	☑	☑	☑	☒

The metrics used to evaluate the efficacy of transform-based image encryption methods are compared in Table 4 between recent studies.

NCPR - **Number of Pixel Change rate**
UACI - **Unified Average Changing Intensity**
KA - **Key Analysis**
HA - **Histogram Analysis**

Section: Research Paper
ISSN 2063-5346

CC	**-**	**Correlation Coefficient Analysis**
IE	**-**	**Information Entropy**
NA	**-**	**Noise Attack**

Image encryption in spatiotemporal domain

Numerous researchers have been keen on coupled map cross sections (CML)- based spatiotemporal tumultuous frameworks as of late on the grounds that they display striking characteristics in secure correspondence contrasted with single guides [155]. CMLs are viewed as an incredible choice for picture encryption.

[156] presents a variety picture encryption framework in view of disorder and tweaked universally coupled map cross sections. In the first place, the RGB picture is separated into its three parts utilizing the variety decay method, and afterward a vital picture with a similar size as the first picture is made utilizing a CML-based strategic guide. Second, the image is parted and rearranged into four indistinguishably measured pictures: a red picture, a green picture, a blue picture, and a RGB picture. The key picture will then, at that point, be chosen from the four pictures utilizing the disarray activities. The code picture is made later by consolidating the leftover three pictures. Trial investigation and programmatic experiences exhibit how very strong the given picture encryption calculation is to different security dangers and interruptions..

[157] presents one more technique for encoding variety pictures in view of a spatiotemporal tumultuous framework and DNA designs. The Calculated Sine framework (LSS) is utilized in the CML and an original spatiotemporal turbulent framework is made to create more irregular groupings. The first picture and the mystery keys given in the spatiotemporal successions are utilized to make the vital picture from the beginning. Also, heavily influenced by key streams, DNA addition and erasure apparition activities are done to befuddle the DNA encoded diffused picture. The scrambled picture is then acquired by translating the DNA encoded mage. Hypothetical investigation and trial discoveries show that the given picture cryptosystem performs with high precision and is impervious to various assaults, including differential and measurable ones.

The journalists of [158] stand out enough to be noticed to the issue of key dissemination in tumultuous picture encryption calculations and have in this way given a cure. Based on normally utilized execution measurements, an intensive investigation of current methods is likewise examined and diverged from the recommended calculation. The discoveries show that the proposed conspire works better compared to different strategies by arriving at high entropy and Brought together Normal Evolving Power (UACI) values

Different coupled map grids (MCML), a shiny new spatiotemporal turbulent framework, was advanced by Wang et al. It is exhibited in the paper that MCML highlights like Kolmogorov-Sinai entropy, bifurcation charts, and spatiotemporal conduct make it a decent possibility for picture encryption calculations through an exhaustive examination of these elements. The connection between's neighboring pixels in the plain picture and the relationship between's the RGB parts of the variety picture are both fundamentally decreased by this nonlinear dissemination method, as per trial

examination of key responsiveness, histogram investigation, connection examination, and differential assault. The trial study shows how solid, successful, and secure the proposed calculation is.

To ensure the security of clinical pictures, Hossein et al. The technique then, at that point, utilizes MGA to abbreviate the calculation's handling time and lift the entropy of the code pictures that are created. The proposed calculation produces pictures of higher lucidity in a more limited measure of time.

A spatial disarray model known as the strategic unique coupled calculated map cross section (LDCML) was advanced by Wang et al. Based on nearby pixels connection, computational intricacy, picture responsiveness, secret key space, and data entropy, the paper furnishes a short correlation of LDCML with CML. LDCML is more tumultuous and has a bigger key space than the other picture encryption plans depicted in the paper, as per the hypothetical examination and tests.

A clever twofold picture encryption technique in view of spatiotemporal disarray and DNA inclusion and erasure tasks is introduced in the article [162]. The proposed twofold picture encryption calculation exhibits that it has a huge key space, high entropy, high key responsive qualities, and is exceptionally impervious to commotion and impediment assaults.By using blended direct nonlinear (MNCML) coupling, Zhang et al. The proposed calculation is suitable for cryptography because of its different properties.Utilizing a 2D non-neighboring coupled map grid (2DNACML), a complex spatiotemporal turbulent framework is portrayed in [164].

[165] presents a clever technique for picture encryption in light of non-neighboring coupled map cross sections. To build the security of the model that is being shown, the CML is at first joined with a 3D Arnold change. The non-neighboring CML utilizes the substitute construction of change, dispersion, and replacement and every pixel is encoded just a single time, lessening the intricacy of the framework in contrast with the ordinary CML picture encryption strategy. The unchangeable in the plaintext is then supplanted by a unique S-box, which is concocted by subbing the plaintext values for the powerful hash values. The adequacy of the proposed technique is approved by reenactments.

REFERENCE	**Number of Pixel Change rate**	**Unified Average Changing Intensity**	**Key Analysis**	**Histogram Analysis**	**Correlation Coefficient Analysis**	**Information Entropy**	**Noise Attack**
156	☑	☑	☑	☑	☑	☑	☒
157	☑	☑	☑	☑	☑	☑	☑
158	☑	☑	☑	☒	☒	☑	☒
159	☑	☑	☑	☑	☑	☑	☒
160	☑	☑	☑	☑	☑	☑	☒
161	☑	☑	☑	☑	☑	☑	☒
162	☑	☑	☑	☑	☑	☑	☑
163	☒	☒	☑	☒	☒	☑	☑
164	☑	☑	☑	☑	☑	☑	☑
165	☑	☑	☑	☑	☑	☑	☑

Section: Research Paper
ISSN 2063-5346

According to the evaluation matrices they used to assess the performance of image encryption methods in the spatiotemporal domain, Table 5 compares recent papers.

NCPR	-	**Number of Pixel Change rate**
UACI	-	**Unified Average Changing Intensity**
KA	-	**Key Analysis**
HA	-	**Histogram Analysis**
CC	-	**Correlation Coefficient Analysis**
IE	-	**Information Entropy**
NA	-	**Noise Attack**

Conclusion

This paper offers an exhaustive examination of picture encryption techniques utilized in the spatial, worldly, and spatiotemporal domains. For better cognizance, an exhaustive overview of the latest papers from the past five years was led and they were gathered into relevant classifications. The writing examination prompts the end that picture encryption is still in its outset and requires development in the space of safety, computational viability, and boundary tuning. The outlines of the assessment strategies for encryption methods show that a large portion of the papers don't confirm the presentation of an encryption calculation utilizing every one of the standard checks. The viability and proficiency of as of late proposed picture encryption plans ought to be surveyed utilizing a typical benchmark. Video handling, video security, and the use of picture encryption strategies to video encryption procedures are dynamic review regions.

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 Sys- tems, pp. 149–156 (2009)
3. Lu, J., Dunkelman, O., Keller, N., Kim, J.: New impossible differ- ential 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 blockcipherclefia. 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 Crypto- graphic Hardware and Embedded Systems, Springer, pp. 450–466 (2007)
17. Tripathi, R., Agrawal, S.: Comparative study of symmetric and asymmetric CryptogrTechniq (2014)
18. Harn, L., Mehta, M., Hsin, W.J.: Integrating Diffie-Hellman key exchange into the digital signature algorithm (dsa). IEEE Com- mun. 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.: Optimiz- ing 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 algo- rithm 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 Anal- ysis 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 combina- tion 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 algo- rithm based on tent map. Control Decision 20(2), 179–182 (2005)Fang, D., Sun, S.: A new secure image encryption algorithm based on a 5d hyperchaotic map. Plos one 15(11):e0242,110 (2020)
36. 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)
37. 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)
38. 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)
39. Pisarchik, A.N., Zanin, M.: Image encryption with chaotically coupled chaotic maps. Phys. D Nonlinear Phenomena 237(20), 2638–2648 (2008)
40. Ye, R.: A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Optics Commun. 284(22), 5290–5298 (2011)
41. Koduru, S.C., Chandrasekaran, V.: Integrated confusion-diffusion mechanisms for chaos based image encryption. In: 2008 IEEE 8th International Conference on Computer and Information Technol- ogy Workshops, IEEE, pp. 260–263 (2008)
42. 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)
43. 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)
44. 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)
45. 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)
46. Solak, E., Cokal, C., Yildiz, O.T., Biyikogˇlu, T.: Cryptanalysis of Fridrich‘s chaotic image encryption. Int. J. Bifur. Chaos 20(05), 1405–1413 (2010)

47. Ben-Aroya, I., Biham, E.: Differential cryptanalysis of Lucifer. In: Annual International Cryptology Conference, Springer, pp. 187–199 (1993)
48. Alani, M.M.: Neuro-cryptanalysis of des and triple-des. In: Inter- national Conference on Neural Information Processing, Springer, pp. 637–646 (2012)
49. Fluhrer, S., Mantin, I., Shamir, A.: Weaknesses in the key schedul- ing algorithm of rc4. In: International Workshop on Selected Areas in Cryptography, Springer, pp. 1–24 (2001)
50. 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
51. ansform. IJACSA) Int. J. Adv. Comput. Sci. Appl. 3(9) (2012)