3D Res (2014) 5:29
DOI 10.1007/s13319-014-0029-0

A Literature Review on Image Encryption Techniques

Majid Khan · Tariq Shah

Received: 29 June 2014 / Revised: 24 September 2014 / Accepted: 2 October 2014

Abstract Image encryption plays a paramount part to guarantee classified transmission and capacity of image over web. Then again, a real-time image encryption confronts a more noteworthy test because of vast measure of information included. This paper exhibits an audit on image encryption in spatial, frequency and hybrid domains with both full encryption and selective encryption strategy.

Keywords Image encryption · Domains of image encryption · Full and selective image encryption techniques

1 Introduction

Cryptography is about correspondence in the region of an adversary. It joins various issues like encryption, check, and key assignment to name a couple. The field of current cryptography gives a theoretical stronghold centered around which one can fathom what definitely these issues are, the best approach to evaluate traditions that infer to light up them and how to gather traditions in whose security one can have conviction [1].

Advanced automated advances have made media data by and large available. Starting late, media procurements get essential in practice and along these lines security of sight and sound data has gotten standard concern. The central issues identifying with the issue of encryption has been inspected and moreover an outline on picture encryption strategies centered on chaotic techniques have been overseen in the present correspondence.

The chaotic image encryption could be made by using properties of chaos including deterministic elements, erratic conduct and non-straight change. This thought prompts routines that can in the meantime give security limits and a general visual check, which may be suitable in a couple of demands.

Automated pictures are for the most part used as a piece of diverse orders, that join military, genuine and helpful frameworks and these procurements need to control access to pictures and give the means to affirm uprightness of images.

The most aged and fundamental issue of cryptography is secure communication over a shaky channel. Party A needs to send to gathering B a mystery message over a correspondence line, which may be tapped by an enemy. The late developments in engineering, particularly in machine industry and correspondences, permitted possibly tremendous business for appropriating computerized interactive media content through the Internet.

Then again, the multiplication of advanced archives, picture handling apparatuses, and the overall accessibility of Internet access has made a perfect medium for copyright misrepresentation and wild

M. Khan (✉) · T. Shah
Quaid-i-Azam University, Islamabad, Pakistan
e-mail: mk.cfd1@gmail.com

Published online: 22 October 2014

appropriation of media, for example, picture, content, sound, and feature content [2].

An alternate significant test now is the manner by which to secure the licensed innovation of media substance in sight and sound systems.

To manage the specialized difficulties, the two significant picture security advances are underutilize: (a) Image encryption procedures to give end-to-end security when dispersing advanced substance over a mixture of disseminations systems, and (b) watermarking systems as an instrument to accomplish copyright insurance, proprietorship follow, and verification. In this paper, the flow research endeavors in picture encryption procedures focused around chaotic plans are examined.

Interactive media security as a rule is given by a system or a set of techniques used to secure the sight and sound substance. These systems are intensely focused around cryptography and they empower either correspondence security, or security against robbery (Digital Rights Management and watermarking), or both.

Correspondence security of computerized pictures and text based advanced media could be fulfilled by method for standard symmetric key cryptography. Such media could be dealt with as parallel grouping and the entire information might be encoded utilizing a cryptosystem, for example, Advanced Encryption Standard (AES) or Data Encryption Standard (DES) [3]. As a rule, when the interactive media information is static (not a continuous streaming) it can treated as a standard binary information and the accepted encryption procedures might be utilized. To distinguish an ideal security level, the expense of the sight and sound data to be ensured and the expense of the insurance itself are to be looked at deliberately. At present, there are numerous accessible picture encryption calculations, for example, Arnold map, Tangram algorithm [4], Baker's transformation [5], Magic 3D square transformation [6], and affine transformation [7] and so on.

In a few calculations, the mystery key and calculation can't be differentiated viably. This does not fulfill the prerequisites of the cutting edge cryptographic instrument and are inclined to different ambushes. Lately, the picture encryption has been created to overcome above detriments as talked about in [2, 3, 8–10].

The paper is organized as follows: In Sect. 2, we discussed some preliminaries of cryptography. In Sect. 3 we have discussed the literature review on image encryption techniques based on full and selected algorithms. Moreover, we have presented classification of image encryption schemes in three domains. The conclusion is presented in last section.

2 Preliminaries

2.1 Plain Text

The original message that the person wishes to communicate with the other is defined as plain text. In cryptography the actual message that has to be send to the other end is given a special name as plain text.

2.2 Cipher Text

The message that cannot be understood by anyone or meaningless message is what we call as cipher text. In cryptography the original message is transformed into non-readable message before the transmission of actual message.

2.2.1 Ciphers

A cipher encrypts a single letter or group of letter as a unit, regardless of meaning.

2.2.2 Codes

A code encodes a word or phrase at a time usually in a fixed way (no keys).

2.3 Encryption

A process of converting plain text into cipher text is called as encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things—an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

2.4 Decryption

A reverse process of encryption is called as decryption. It is a process of converting cipher text into plain text. Cryptography uses the decryption technique at

the receiver side to obtain the original message from non-readable message (cipher text). The process of decryption requires two things—a decryption algorithm and a key. A decryption algorithm means the technique that has been used in decryption. Generally the encryption and decryption algorithm are same.

2.5 Key

A Key is a numeric or alpha numeric text or may be a special symbol. The key is used at the time of encryption takes place on the plain text and at the time of decryption take place on the cipher text. The selection of key in cryptography is very important since the security of encryption algorithm depends directly on it.

2.6 Purpose of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

2.6.1 Confidentiality

Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

2.6.2 Authentication

The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity.

2.6.3 Integrity

Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

2.6.4 Non Repudiation

Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

2.6.5 Access Control

Only the authorized parties are able to access the given information.

2.7 Classification of Cryptography

Encryption algorithms can be classified into two broad categories—Symmetric and Asymmetric key encryption.

2.7.1 Symmetric Encryption

In symmetric cryptography the key used for encryption is similar to the key used in decryption. Thus the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e., the key length etc. There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6, BLOWFISH [2]. The symmetric algorithms are of two types [3]:

2.7.1.1 Block ciphers
2.7.1.2 Stream ciphers

2.7.1.1 Block ciphers A block cipher is a function which maps n bit plain text blocks to n bit cipher text blocks; n is called the block length. It may be viewed as a simple substitution cipher with large character size. The function is parameterized by a k bit key K, taking values from a subset K (the key space) of these to fall k bit vectors V_k. It is generally assumed that the key is chosen at random. Use of plain text and cipher text blocks of equal size avoids data expansion.

2.7.1.1.2 Definition An n bit block cipher is a function $E{:}V_n \times K \rightarrow V_n$ such that for each key $\mathbb{K} \in K$, $E(P;\mathbb{K})$ is an invertible mapping (the encryption function for $\mathbb{K}$) from V_n to V_n, written $E_{\mathbb{K}}(P)$. The inverse mapping is the decryption function, denoted by $D_{\mathbb{K}}(C)$. $C = E_{\mathbb{K}}(P)$ denote that cipher text C results from encrypting plain text P under $\mathbb{K}$ [3].

2.7.1.1.3 Definition A random cipher is an n-bit block cipher implementing all $2^n!$ bijection on 2^n elements. Each of the $2^n!$ keys specifies one such permutation.

2.7.1.2 Stream Ciphers Stream ciphers are an important class of encryption algorithms. They encrypt individual characters (usually binary digits) of a plain text message one at a time, using an encryption transformation which varies with time. Stream ciphers are generally faster than block ciphers in hardware, and have less complex hardware circuitry. They are also more appropriate, and in some cases mandatory (e.g., in some telecommunications applications), when buffering is limited or when characters must be individually processed as they are received. Because they have limited or no error propagation, stream ciphers may also be advantageous in situations where transmission errors are highly probable. Stream ciphers are commonly classified as being synchronous or self-synchronizing.

2.7.1.2.1 Synchronous Stream Ciphers A synchronous stream cipher is one in which the key stream is generated independently of the plain text message and of the cipher text. The encryption process of a synchronous stream cipher can be described by the equations [3]:

$$\begin{aligned} \beta_{i+1} &= f(\beta_i, K), \\ \alpha_i &= g(\beta_i, K)\ , \\ c_i &= h(\alpha_i, m_i), \end{aligned} \tag{2.1}$$

where β_0 is the initial state and may be determined from the key K, f is the next-state function, g is the function which produces the key stream α, and h is the output function which combines the key stream and plain text m to produce cipher text c.

2.7.1.2.2 Self-synchronizing Stream Ciphers A self-synchronizing or asynchronous stream cipher is one in which the key-stream is generated as a function of the key and a fixed number of previous cipher text digits. The encryption function of a self-synchronizing stream cipher can be described by the equations [3]:

$$\begin{aligned} \beta &= (c_{i-t}, c_{i-t+1}, \ldots, c_{i-1}), \\ \alpha &= f(\beta_i, K)\ , \\ c_i &= g(\alpha_i, m_i), \end{aligned} \tag{2.2}$$

where $\beta_0 = (c_{-t}, c_{-t+1}, \ldots, c_{-1})$ is the (non-secret) initial state, K is the key, f is the function which produces the key stream α, and g is the output function which combines the key stream and plain text m to produce cipher text c.

2.7.2 Asymmetric Encryption

Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access too [3].

2.8 Diffusion and Confusion

Shannon, in one of the fundamental papers on the theoretical foundations of cryptography [1, 2], gave two properties that a good cryptosystem should have to hinder statistical analysis: diffusion and confusion. Diffusion means that if we change a character of the plain text, then several characters of the cipher text should change, and similarly, if we change a character of the cipher text, then several characters of the plain text should change. This means that frequency statistics of letters in the plain text are diffused over several characters in the cipher text, which means that much more cipher text is needed to do a meaningful statistical attack. Confusion means that the key does not relate in a simple way to the cipher text. In particular, each character of the cipher text should depend on several parts of the key.

2.9 Spatial and Frequency Domain

2.9.1 Spatial Domain

In the spatial domain method, the pixel composing of image details are considered and the various procedures are directly applied on these pixels. The image processing functions in the spatial domain may be expressed as

$$g(x, y) = T[f(x, y)], \tag{2.3}$$

where $f(x, y)$ is the input image, $g(x, y)$ is the processed output image and T represents an operation

on f defined over some neighborhood of (x, y). Sometimes T can also be used to operate on a set of input images. The spatial domain is the normal image space, in which a change in position in image I directly projects to a change in position in scene S. Distances in I (in pixels) correspond to real distances (e.g., in m) in S. We can also discuss the frequency with which image values change, that is, over how many pixels does a cycle of periodically repeating intensity variations occur. One would refer to the number of pixels over which a pattern repeats (its periodicity) in the spatial domain.

2.9.2 Frequency Domain

The frequency domain is a space in which each image value at image position F represents the amount that the intensity values in image I vary over a specific distance related to F. In the frequency domain, changes in image position correspond to changes in the spatial frequency, (or the rate at which image intensity values) are changing in the spatial domain image I. In simple spatial domain, we directly deal with the image matrix, whereas in frequency domain, we deal an image like this.

2.9.2.1 Frequency Components Any image in spatial domain can be represented in a frequency domain. But what do these frequencies actually mean. We will divide frequency components into two major components.

2.9.2.2 High Frequency Components High frequency components correspond to edges in an image.

2.9.2.3 Low Frequency Components Low frequency components in an image correspond to smooth regions.

2.9.3 Difference Between Spatial Domain and Frequency Domain

In spatial domain, we deal with images as it is. The values of the pixels of image change with respect to scene, whereas in frequency domain, we deal with the rate at which the pixel values are changing in spatial domain.

3 Literature Review of Image Encryption Techniques

In this segment, a couple of recently proposed strategies for image encryption, taking into account chaotic plans which will enhance the multifaceted nature of algorithm and also make the key stronger has been presented. To start with segment manages officially existing image encryption procedures focused around chaotic plans in spatial space while recent part manages some paper in recurrence area.

3.1 Full Encryption

Information privacy is an essential part of image encryption. The secrecy of the encrypted data with a parity in time and cost productivity of the encryption method will be the test still confronted in image encryption. These challenges have been distinguished in a number of works spanning the spatial, frequency and the hybrid domain techniques in full encryption schemes. In resulting segments, we will accentuate on the techniques in these literature works on the premise of the domains of execution and the encryption approaches such as block cipher and stream cipher approaches, utilized within addressing the test [11–30].

3.1.1 Spatial Domain

In 1989, Robert and Matthews proposed new encryption algorithms determined from chaotic systems and owning to the critical properties of chaotic systems, such as the delicate reliance on beginning conditions and pseudo-irregular cluster which is difficult to foresee after a certain times of iteration chaotic encryption [11].

Habutsu et al. have proposed another secret key cryptosystem by repeating a chaotic map. In the proposed plan they utilized tent map as a chaotic map to focus the parameter sizes to forestall statistic attacks by Chi square test, whose result is that the times of mapping ought to be bigger than 73 if the key size and the plain text size are both 20 digits. In the proposed framework, a plain text has $2n$ cipher texts and one of $2n$ cipher texts is sent to the receiver. Regardless of the fact that the cipher text is picked by any self-assertive way, the receiver can acquire the plain text just utilizing the secret key [12].

Schwartz proposed a scrambling strategy to encrypt image. Its first step is to produce a grouping of random points on the original image. These random points are strikingly controlled by the seed of the irregular number generator; the seed is the private key of this strategy. Next, this strategy draws some graphical lines between every two continuous purposes of this sequence. In addition, its attracting pen is the inverted mode, which changes each one white pixel to dark and the other way around. In the wake of drawing numerous opposite lines on the original image, the plain image is consequently encrypted [13].

Bourbakis and Alexopoulos created an alternate image encryption system. It changes over a 2D image into 1D list, and utilizes a SCAN language to depict the changed over result. In this language, there are a few SCAN letters. Each one SCAN letter speaks to one sort of sweep request. Various types of blending of SCAN letter may produce different sorts of secret image. In the wake of deciding the synthesis of SCAN letters, the composition then produces a SCAN string. This string defines sweep request of the original image. Next, this system examines the original image in the decided request and, in addition, encodes the SCAN strings by utilizing business cryptosystems. Since the illicit clients can't acquire the right SCAN string, the original image is thusly secure. There is no image clamping in this technique, therefore it is wasteful to encode or unscramble the image straightforwardly [14].

Kuo proposed an encryption method that alluded to the image distortion. This method acquires the encrypted image by including the phase spectra of the plain image with those of an alternate key image. Since the phase spectra of the encrypted image are arbitrarily changed, the figure image is unrecognizable. Along these lines this method is sheltered; however no image compression is considered [15] (Figs. 1, 2, 3, 4, 5).

Chang and Liu proposed an encryption method for images. This method utilizes two advances to attain the compression and encryption purposes. They are quad tree data structure and the SCAN dialect, separately. This method first clamps the original image by utilizing a quad tree, and after that encodes the compressed data by SCAN. Along these lines, this method can layer and scramble images synchronously. Quadtree is quite a lossless data layering engineering, hence this method is likewise lossless, it may not be secure enough to oppose some illicit assaults, for example, jigsaw riddle assault and neighbor assault and so on [16]. Alexopoulos et al. displayed an encryption method for scrambling 2D gray scale images by utilizing a bigger class of fractals [17].

Yang and Kim [18] proposed image encryption and comparing interpreting method applicable to security check. This method exploits a holographic process in that an encoded image could be viewed as a 3D image example coming about because of impedance between two waves transmitted through an essential ID image and a reference image serving as an encryption key. They have demonstrated that their proposed method delivers a genuine esteemed encoded image, which encourages card fabricating.

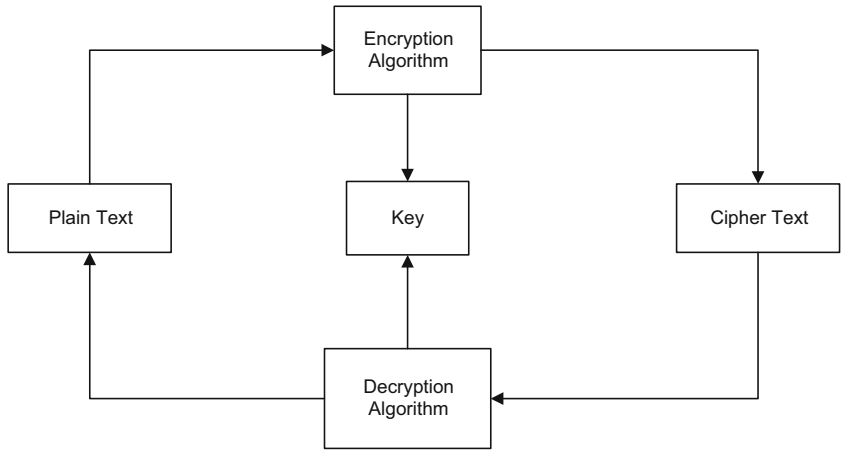

Fig. 1 Block diagram for encryption and decryption

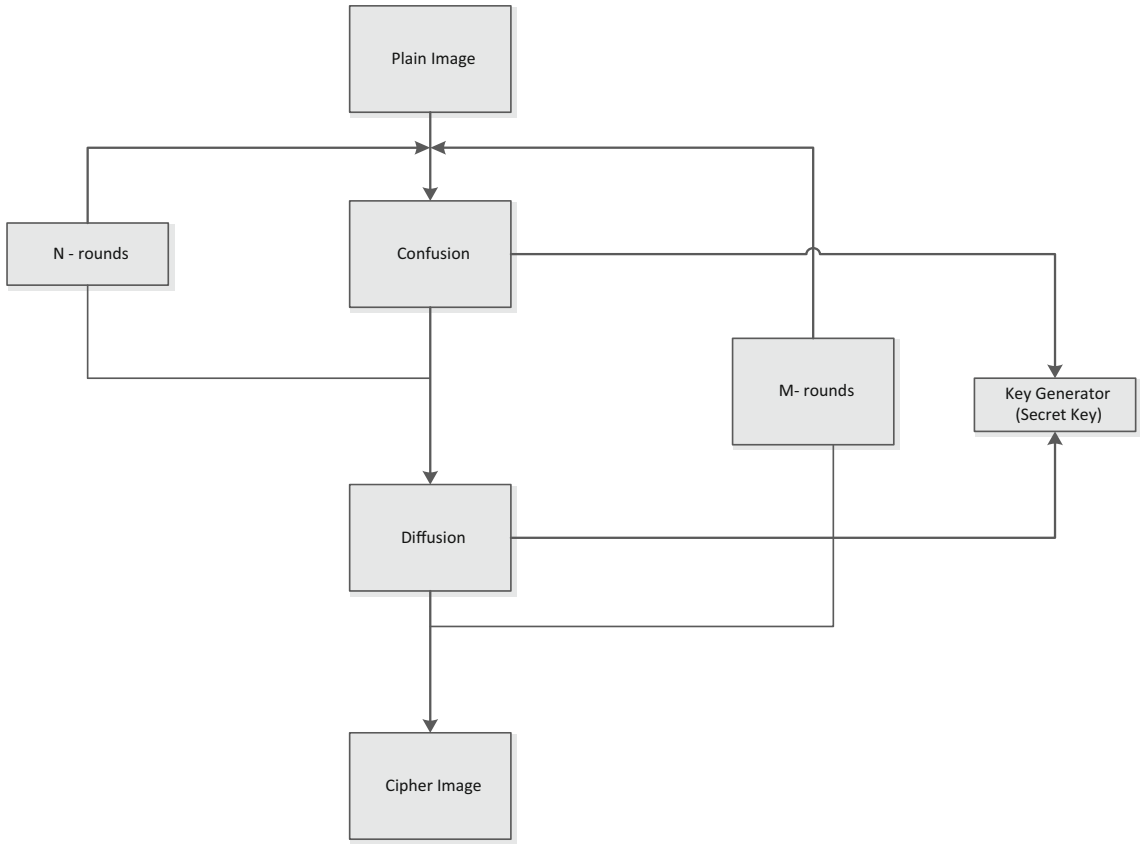

Fig. 2 Architecture for chaotic image encryption technique

In 1996 [19], Scharinger and Pichler presented another item figure which scrambles huge pieces of plain content by rehashed entwined application of substitution and permutation operations. The proposed plan utilized parameterizable changes on extensive data-pieces, (for example, images) incited by particular disordered frameworks.

Fridrich [20] exhibited an encryption algorithm that adjusted certain invertible disorderly two-dimensional maps to make new symmetric block encryption schemes. This scheme is particularly valuable for encryption of substantial measure of data, such as digital images. In 1998, Baptista proposed a searching based chaotic block ciphers [21].

Guo and Yen in [22] have introduced an effective mirror-like image encryption algorithm. Taking into account a twofold succession created from a chaotic system, an image is mixed as per the algorithm. This algorithm has low computational multifaceted nature, high security and no contortion.

Yen and Guo [23], proposed an image encryption/decoding algorithm and its VLSI structure. As indicated by a chaotic binary sequence, the gray level of every pixel is Xored or Xnored bit by-bit to one of the two foreordained keys.

In this paper [24], Sobhy utilized Lorenz mathematical statement for encryption, making secure databases; secure email, actualized in FPGA for ongoing images. In this paper the chaotic algorithm is utilized for encoding content and images. Numerous kinds of chaotic cryptosystems have been proposed. Chaotic structures scatter data because of orbital unsteadiness with positive Lyapunov exponents and ergodicity. In the event that these properties are fittingly used, chaotic cryptosystems should acknowledge high security. Notwithstanding, the vast majority of the current secure correspondence strategies utilizing chaos don't have enough security. For instance, secure correspondence conventions focused on chaos synchronization oblige robustness which

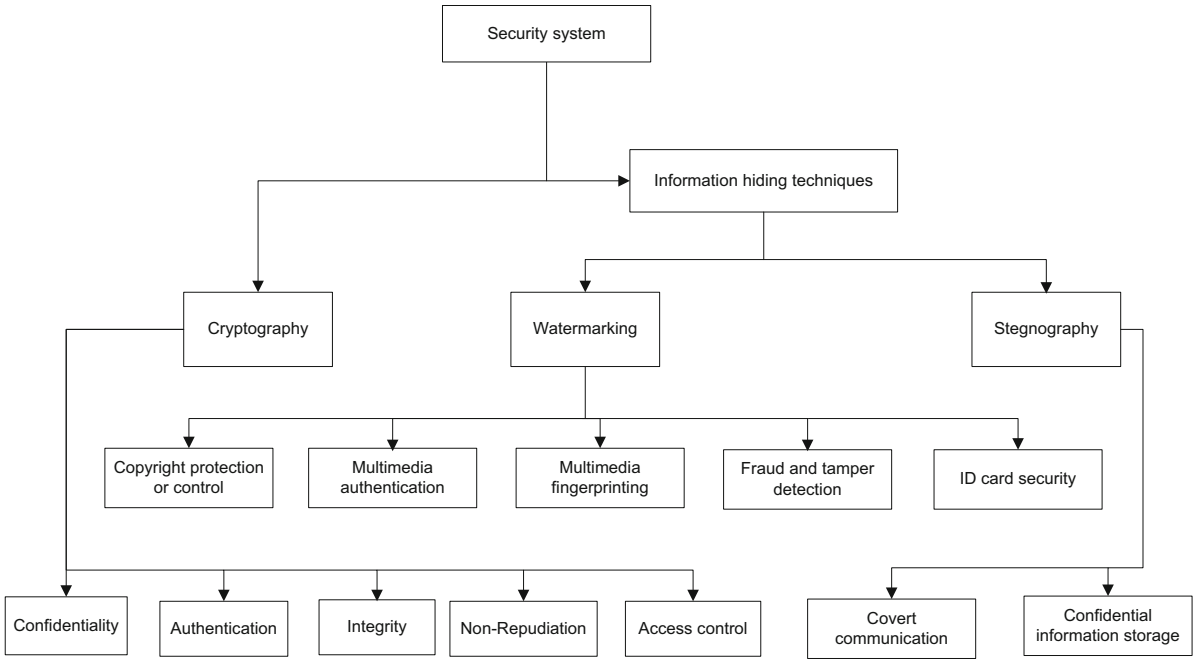

Fig. 3 Classification of information security techniques and its applications

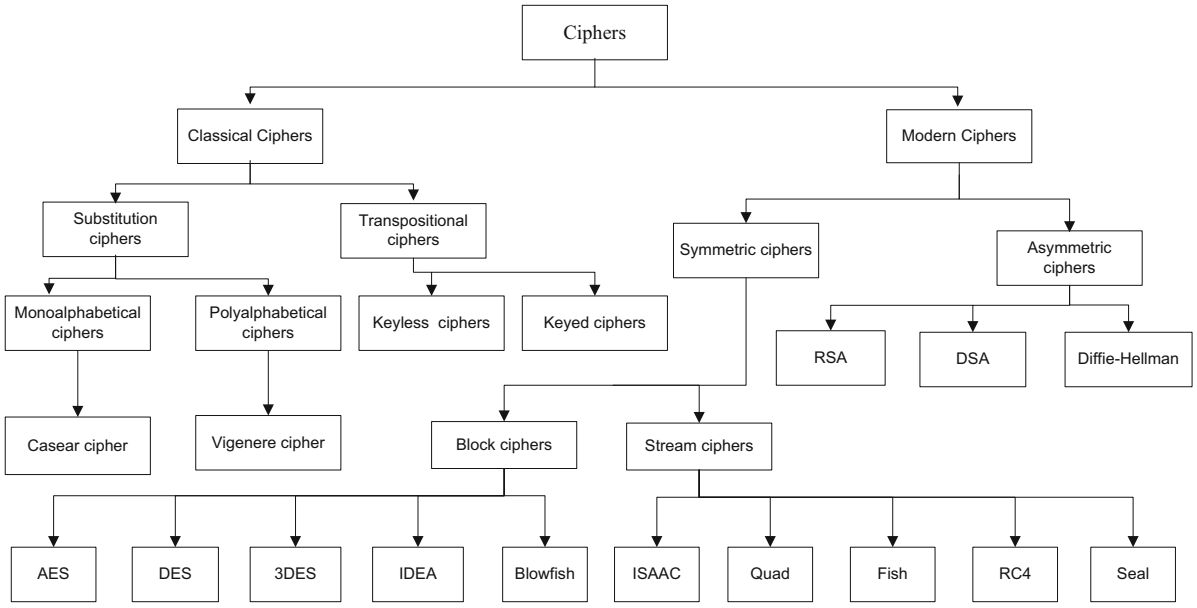

Fig. 4 Classifications of cryptographic algorithms

gives valuable information to attackers. The cryptosystems focused around immediate applications of chaotic maps have been frail against linear and differential cryptoanalysis. Masuda and Aihara proposed another sort of chaotic cryptosystem which defeats these troubles to some degree. The cryptosystem is focused around a discretization of the skew tent map. They likewise demonstrate a percentage of the alluring properties of the proposed cryptosystem utilizing dynamical qualities. These properties in

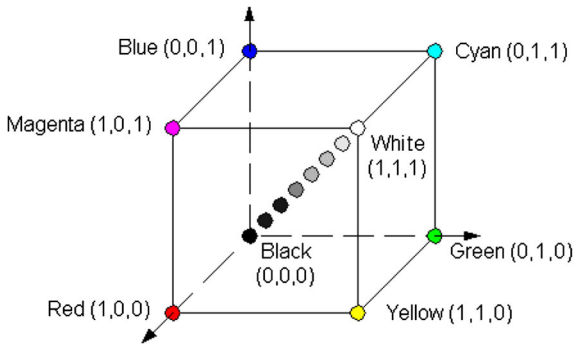

Fig. 5 RGB color space

regards to ciphertext irregularity may be nearly identified with the cryptological security. The new cryptosystem utilizes one stage to associate the theory of commonly used cryptosystems and dynamical system theory [25].

Sinha and Singh [26] have proposed another procedure to scramble an image for secure image transmission. The advanced signature of the original image is added to the encoded variant of the original image. Image encoding is carried out by utilizing a suitable lapse control code, for example, a Bose–Chaudhuri Hochquenghem (BCH) code. At the receiver end, after the decryption of the image, the computerized mark has been utilized to confirm the credibility of the image.

Sallen et al. [27], proposed novel chaotic image encryption based on Baker's map. This improved symmetric-key algorithm can support a variable-size image as opposed to the algorithm which is primarily based on Baker's map that requires just square image for encryption. Furthermore, the algorithm also includes different functions such as password tying and pixel shifting to further strengthen the security of the figure image. The algorithm also supports two modes of operation specifically EBC and CBC. The quantity of iterations to be performed can change relying upon the security level needed by the user. The paper also includes a sample of image encryption. From the analysis done, it shows that the security level is high despite the fact that keys that are discovered to be powerless keys for Baker's map algorithm are constantly used in the algorithm.

Shin et al. [28], proposed the multi-level image encryption by using binary phase exclusive OR operation and image dividing technique. The multi-level image might be separated into binary images that have same gray levels. They changed over binary images to binary phase encoding and then encode these images with binary random phase images by binary phase XOR operation. Encrypted gray image was then acquired by joining every binary encrypted image.

In 2003 [29], Belkhouche and Qidwai used one dimensional chaotic map. It has been shown that the method could be used for binary images encryption with the possibility of using several keys such as the beginning state, the outside parameters and the quantity of iterations. It is also shown that the sensitivity to introductory state plays a paramount part in chaotic encryption.

Wang Ying et al. [30], used first permutation transform and then nonlinear map to circularly repeat pixel values. Disappointment of encryption owing to self-similarity and visional psychological characteristics of image.

Zhang et al. [31], used a T-matrix for image scrambling and its periodicity has been demonstrated. The T-matrix has a simple compliance and a period twice the length of the Arnold matrix. It might be connected to image encryption and preprocessing in image processing such as image watermarking algorithms.

Deng et al. [32] completed an image encryption by a chaotic neural system and the cat map. In this paper neural networks have been used for making the technique chaos.

Gu and Han [33], use permutation and substitution methods together, to present a strong image encryption algorithm. An improved treatment and a cross-sampling disposal have been presented for upgrading the spasmodic and pseudorandom characteristics of chaotic sequences.

Xiao and Zang [34], proposed scheme using two chaotic systems based on the possibility of higher secrecy of multi-system. One of the chaotic systems is used to produce a chaotic sequence. At that point this chaotic sequence was transformed into a binary stream by a threshold function. The other chaotic system was used to construct a permutation matrix. Firstly, the pixel values of a plain image have been adjusted randomly using the binary stream as a key stream. Secondly, the changed image was encrypted again by permutation matrix.

The stream cipher approach has been used in various writing, some of which we will be discussing in this subsection. Nien et al. [35], used a hybrid encryption technique for the color image based on the

multi-chaotic system. They consolidated the Pixel-Chaotic-Shuffle (PCS) and Bit-Chaotic-Rearrangement (BCR) methods. First, the PCS, a fast encryption method that can fluctuate the positions of every pixel, is connected to completely dispense with the original image outlines using four third-request chaos' such as Henon, Lorenz, Chua and Rȍssler chaos maps. Second, the BCR, which uses chaos system to make chaotic codes modification in pixels, are connected. The combo of the PCR and the BCR increases the key space of images to 10,180 and totally eradicates the outlines of the encrypted images, blurs the distribution characteristics of RGB-level matrices, and successfully protects against the decryption of exhaustive attack.

Rhouma et al. [36], proposed a piecewise linear chaotic map (PWLCM) to construct another advanced chaotic cryptosystem. The characteristics of PWLCM are exceptionally suitable for the design of encryption schemes. This method transformed the color image into three vectors then mapping the whole number values of them into the phase space of the skew tent map. At the point when the phase space of the skew tent map is isolated into 256 equivalent width subintervals. The correctness, proficiency and security of the proposed encryption scheme are altogether investigated and its sufficiency for image encryption is demonstrated. The key space is 1,093, which is moderately small key space size, yet its resistance against animal power assault is clear because of high values of NPCR and UACI attained. Moreover the entropy is 7.9551 that indicates just small measure of data loss.

In Musheer et al. [37], proposed encryption algorithm that exploits three diverse chaotic maps. First, they apportioned the image into blocks of 8×8 pixels, all blocks is shuffled using Cat map. Second, the Cat map is connected again to distribute all the blocks. Third, a shuffling is made again using the Cat map, yet this time, it is the final image pixels. At that point the final image is encrypted using one dimensional Logistic map. Their test result revealed that the technique obliged incredible key space, which is around 10112, and are of high sensitivity to minor changes in secret keys. The correlation between the encrypted image and the original image is around 0.0095, which shows that the encrypted image is free of the original image. The encrypted image entropy reported is of greatest quality 7.9992 that indicates just minor measure of data loss.

In similar way Wei et al. [38], approached image encryption from the perspective of [37], yet contrasted by the 4D hyper chaos used. They produced four chaotic sequences from 4D hyper chaos. At that point encryption is completed on every R, G, and B color channels of the image based on the first three sequences with inter-cross cipher-block chaining mode. The encrypted image is then shuffled by means of every three color channels. After numerous rounds of encryption, the cipher image is accomplished. From [38], it is obvious that correlation coefficients of the encrypted image are significantly lessened and is also worth bringing up that a small change in secret key can result in a totally diverse unscrambled image.

Kamali et al. [39], created an encryption scheme that is a modification of advanced encryption standard (AES), which is a well-known block cipher technique in data encryption. The modification is accomplished by using shift and row transformations: if the values of first row and column will be even, the first and forward rows are unaltered, then every byte in the second and third rows is shifted to the right, cyclically. Then again, if the first and third rows are unaltered, every byte of the second and fourth rows is shifted to the left. The technique shows strong execution against statistical attacks.

Aihong et al. [40] proposed a defensive transmission of RGB color image based on Logistic map and LSB concealing algorithm. First of all, Logistic map used three chaotic sequences and the R, G and B matrices were permuted by the chaotic sequences. At long last, the LSB concealing algorithm is used to insert encrypted image in the bearer image through transmission. This method has high security, fast operation speed with less secret key for any color image. It is suitable for the huge color image security transmission over a system.

In [41] a color image encryption method that applies Logistic chaotic map in two iterative steps was proposed. For the first step, the logistic map is used to permute pixels of the original image. For the second step, the logistic map is used in the diffusion process. As indicated by the execution analysis reported in [41], it might be presumed that the technique satisfied high security level requirements which worthy encryption speed for variable size of image. Evidently, it is also observed that encryption quality was achieved with moderately small key

space. Moreover it is observed that the original image is autonomous of the encrypted image with high safety for diverse attacks because of the minimum correlation estimation of 0.0013 achieved.

Mastan et al. [42] proposed a nonlinear color image encryption technique that comprised matrix transformations such as pixel diffusion and permutation. The technique firstly applies diffusion autonomously for each one channel of color image using both single pixel and block pixel diffusion. At that point the permutation between three channels R, G, and B is connected interdependently between pixels. This technique is specifically designed for sensitive fields such as medicine where misinterpretation could result in loss of life. It is faster than AES and could be used continuously in secure image transmission.

In [43], Pareek et al. proposed another lossless image encryption algorithm that is based on pixel substitution, which divides the image into blocks of color components. The color part in each one block of the color images is then altered by exclusive-OR operation. The algorithm is simple, fast, yet sensitive to the secret key, because of the key space of 2,120 that it uses, which makes their technique more suitable for storing/transmitting images of high security prerequisite.

A methodology to image encryption that is based on sifting rows and columns of image was proposed by Abugharsa et al. [44]. Using a shifting table that is produced by hash function, the original image is partitioned into block of 3×3 pixels. At that point the blocks are further shifted through rows and columns before scrambling. We observe from [44] that there is a close relationship between the original image and the encrypted image, which is affirmed by the correlation coefficient value i.e., -0.0078. This implies that the neighborhood pixels in the unique image have nearest value than the neighborhood pixels of the encrypted image, which is a decent evidence that consistency is low. On the other hand, because of the high entropy value is achieved, it might be said that the technique in [20] is against differential in terms of security.

The technique used in [45] joined shift image blocks and AES. First, the hash function is used to create a shift table for shifting the image blocks. Second, the shifted image is encouraged into the AES encryption algorithm. Their technique shows the capability to scramble expansive data sets proficiently and progressively, since the NPCR and UACI values are close standard values, which are 99.6689, and 27.7599 %, respectively. Moreover, correlation value shows that the original image has nearest values between its neighborhoods than the encrypted image neighborhood pixels, which is proof of less consistency by outsider.

Confidentiality is a critical issue in transmitting advanced images over open systems such as internet. Image encryption is a helpful answer for attain confidentiality. Among existing encryption plans, confusion based methodology has recommended quick, efficient and very secure algorithms. As of late an efficient image encryption system based on chaos and permutation–diffusion structural planning is recommended in [46]. On the other hand, the plain-message affectability, as reported by the creators, is not fulfilling and it is proposed to repeat the algorithm more than twice to get a decent capacity to oppose differential attack. The point of this paper is to push the plain-message affectability of their methodology. Subsequently, the dispersion execution is significantly upgraded and the general security of the image cryptosystem is made strides. The after effect of different investigates and machine reproductions confirm that the new algorithm has high security and is suitable for practical image [47].

In [48], an optical color image cryptosystem based on position multiplexing system and stage truncation operation is proposed. Compared and the described color image encryption technique, authors utilized the position multiplexing procedure to encode the color image in only in spatial channel. Then, the proposed strategy can keep up the nonlinear characteristics for the cryptosystem and evade different sorts of the presently existing attacks, particularly the iterative attack. Recreation results are displayed to show the security and vigor execution of the proposed system.

A novel image encryption plan focused around rotation matrix bit-level permutation and block diffusion is proposed in [49]. Firstly, divide plain image into non-covering 8×8 pixels blocks with a random matrix, then change each one block into a $8 \times 8 \times 8$ three-dimensional (3D) parallel matrix, which has six directions generally as a cube. Permutation is performed by duplicating the 3D matrix by the rotation matrix that depends on plain image as per diverse heading. Furthermore, utilize block diffusion to further change the measurable attributes of the

image after confusion. Investigation results and analysis demonstrate that the plan can attain an attractive security execution, as well as have the suitability for a parallel mode and the robustness against noise in correspondence system.

3.1.2 Frequency Domain

Sinha et al. [50] proposed another strategy for gray scale image encryption using 3D jigsaw transform. To start with, the image is transformed to bit planes, where every bit plane is separated into more diminutive blocks. The 3D jigsaw transform translocate each block to diverse area in 3D square. They utilized two fractional Fourier transforms (FRFT), the first FRFT is utilized to encode image, and the yield is then reproduced with a random stage code, while the second FRFT is utilized to obtain the encrypted image. By using FRFT and the random stage codes, security is given.

In [51] the encrypted procedure includes three expressions, called color space rotation. The color space of original the color image is initially turned through converting the color image from RGB space to RGB supplement space. Then the individual color part will be transformed using their proposed reality preserving fractional Mellin transform on distinctive fractional requests of the image. Finally, on the premise of achieving high security, the scrambling of pixels will be done three dimensionally. Our perception will be that the vast key space due to their strategy can make the encryption touchy to security risk.

Abuturab [52] proposed a system that secures color images built in light of Arnold transform in gyrator transform domain. For their strategy, the color image is divided into their individual R, G and B parts and then the individual segment will be independently encrypted by applying first random phase mask and then first-order Arnold transform and finally, the gyrator transform. The second random phase mask will be put on the gyrator transformed plane and a further transformation using the second-order Arnold transform and gyrator transform are performed. These enhancing techniques; the Arnold transform and the gyrator transform utilized in [52] are utilized as extra keys within the encryption and unscrambling, which may likely offer vigor against impediment assaults and clamor assaults and high security.

In [53], a single channel color image encryption system was proposed. The strategy will be built with respect to orthogonal composite grating and twofold random phase encoding. A color image first will be deteriorated into R, G and B parts, which accordingly will be adjusted into an orthogonal composite grating. The twisted composite grating is then encrypted by a regular twofold random phase encryption method. It will be watched that combining the two-fold random phase encoding and orthogonal composite grating decreases the multifaceted nature and cost of encryption.

In [54] a color image encryption algorithm that uses the affine transform in the gyrator transform domains, was proposed. Firstly, the affine transform is connected on the RGB parts of the color image and the real and imaginary parts of their frequency segment are concentrated. Second, the R, G, B image pixel qualities are interchanged by scrambling using a random angle approach. Then, the resulting image is transformed using the gyrator transform and mixed again by a second affine transform. Their test results indicated that high security is attainable by using proposed algorithm.

A solitary channel color image encryption is proposed focused around iterative fractional Fourier transform and two-coupled logistic map. Firstly, a gray scale image is constituted with three channels of the color image, and permuted by a succession of chaotic sets which is created by two-coupled logistic map. Firstly, the permutation image is deteriorated into three parts once more. Furthermore, the first two parts are encoded into a solitary one focused around iterative fractional Fourier transform. Essentially, the interim image and third part are encoded into the final gray scale cipher text with stationary white noise distribution, which has camouflage property to some degree. At present encryption and portrayal, chaotic permutation makes the ensuing image nonlinear and disorder both in spatial domain and frequency domain and the proposed iterative fractional Fourier transform algorithm has quicker united rate. Furthermore, the encryption plan amplifies the key space of the cryptosystem. The simulation results and security dissection confirm the achievability and adequacy of this system [55].

In some unique interactive media applications, just the regions with semantic data ought to be given better security while the other smooth areas could be free of encryption. Notwithstanding, the vast majority

of the current media security plots just consider bits and pixels instead of semantic data amid their encryption. Roused by this, authors have proposed an edge-based lightweight image encryption plan utilizing chaos based reversible concealed transform and numerous request discrete fractional cosine transform. An image is first completed by the edge recognition focused around developed CNN structure with versatile limits to survey information significance in the image. The discovery yield is a twofold image, in which a "1" reflects the detected pixel though a "0" is opposite. Both the detected image and the original image are separated into non-covering pixel blocks in the same way, separately. Whether each one block is scrambled or not relies on upon the significance judged by the comparing distinguished block. The significant block is performed by reversible hidden transform took after by different order discrete fractional cosine transform parameters and order of these two transforms are controlled by a two-dimensional cross chaotic map. Analysis results demonstrate the significant form gimmicks of an image that have been generally hidden just by encoding about half pixels in the normal sense. The keys are to a great degree touchy and the proposed plan can oppose noise attack to some extent [56].

A new scheme for optical data concealing (encryption) of two-dimensional images by joining image scrambling methods in fractional Fourier spaces is proposed in [57]. The image is at first randomly moved utilizing the jigsaw transform algorithm, and then a pixel scrambling method focused around the Arnold transform is connected. The mixed image is then encoded in a randomly picked fractional Fourier domain. These methods can then be iteratively rehashed. The parameters of the building design, including the jigsaw permutation lists, Arnold frequencies and fractional Fourier orders, structure a vast key space improving the security level of the proposed encryption framework. Optical executions are talked about as numerical execution algorithms. Numerical simulated results are introduced to exhibit the framework's flexibility and strength [57].

To upgrade the security of double random phase encoding, a sort of amplitude scrambling operation is outlined and brought into an image encryption process. The random information of the second phase mask in double random phase encoding is additionally utilized for scrambling sufficiency appropriation so as to spare the space of capacity and transmission of the key data. The scrambling operator is unpredictable for producing the key. Some numerical reproductions have been accommodated trying the legitimacy of the image encryption plan [58].

A novel double-image encryption algorithm is proposed by utilizing chaos-based nearby pixel scrambling system and gyrator transform. Two unique images are first viewed as the amplitude and phase of a complex capacity. Arnold transform is utilized to scramble pixels at a neighborhood the complex capacity, where the position of the mixed territory and the Arnold transform recurrence are created by the standard map and logistic map separately. At that point the changed complex capacity is changed over by gyrator transform. The two operations specified will be executed iteratively. The framework parameters in neighborhood pixel scrambling and gyrator transform serve as the keys of this encryption algorithm. Numerical reenactment has been performed to test the legitimacy and the security of the proposed encryption algorithm [59].

A single-channel color image encryption is proposed focused around a phase recover algorithm and a two-coupled logistic map. Firstly, a gray scale image is constituted with three channels of the color image, and then permuted by an arrangement of chaotic sets created by the two-coupled logistic map. Also, the permutation image is deteriorated into three new parts, where every part is encoded into a phase-only capacity in the fractional Fourier space with a phase recover algorithm that is proposed focused around the iterative fractional Fourier transform. At last, a between time image is shaped by the synthesis of these phase-only capacities and scrambled into the final gray scale cipher text with stationary background noise by utilizing chaotic diffusion, which has camouflage property to some degree. At the present time encryption and unscrambling, chaotic permutation and diffusion makes the resultant image nonlinear and issue both in spatial space and recurrence area, and the proposed phase iterative algorithm has speedier joined velocity. Moreover, the encryption plan augments the key space of the cryptosystem. Experimental results and security examination check the practicability and viability of this technique [60].

Image encryption and decoding are crucial for securing images from different sorts of security

attacks. In [61], a first approach for a RGB image encryption and unscrambling utilizing two stage random matrix affine figure connected with discrete wavelet transformation is proposed. Prior proposed plans for encoding and unraveling of images talked about only about the keys, yet in our proposed approach, keys and the game plan of RMAC parameters are mandatory. Authors also figured a recipe for all the conceivable reach to pick keys for scrambling and decoding a RGB image. The computer simulations with standard sample and results are given to investigate the ability of the proposed methodology. We have given security examination and correlation between our proposed method and others to backing for power of the methodology. This methodology could be utilized for transmission of image information efficiently and safely [61].

A double image encryption conspires by utilizing random pixel trading and phase encoding in gyrator spaces is proposed. Two unique images are viewed as the adequacy and phase of a capacity in the encryption algorithm. The pixels of the two images are exchanged randomly by controlling of a matrix. The same random matrix is utilized as a part of the methodology of pixel trading and phase encoding for sparing space in the application of transmission and stockpiling of key. Some numerical reenactment results are made for showing the execution and security of the double image encryption [62].

A multiple-image encryption plan based on the optical wavelet transform (OWT) and the multichannel fractional Fourier transform (Mfrft) is proposed in [63]. The plan can make full utilization of multi-determination deterioration of wavelet transform (WT) and multichannel handling of Mfrft. The specified properties can attain the encryption of multi-image and the encryption of single image. At the point when encryption finished, each one image gets it fractional request and autonomous keys. Examination of scrambled impacts has been finished. Moreover, the influence of WT type and order are examined, and the application and examination of Mfrft are proficient too. Numerical reenactment verifies the practicality of the plan and demonstrates that the issue of insufficient limit is better fathomed, and the flexibility of plan increments. A straightforward opto-electronic mixed device to understand the plan is proposed [63].

In [65], a multiple-parameter fractional Fourier transform with its transform order being a real vector, taking into account which a high-security image encryption plan is additionally given. This novel fractional Fourier transform has evacuated the limitation on the measurement of transform order and exceedingly upgrades the security of image encryption plan proposed in this paper without expanding the computational many-sided quality and fittings cost. The numerical results check the efficacy and security of this image encryption technique. The vector power multi-parameter fractional Fourier transform is a summed up type of the traditional fractional Fourier transform with all the past fractional Fourier transform as its extraordinary cases and has hypothetical significance in data handling and data security [64].

An innovative impedance based technique for multiple-image encryption by phase-only mask (POM) multiplexing is designed [65]. The data of multiple images could be scrambled into two POMs (i.e., cipher texts) without any iterative methodology. For right decoding, one ought to hold the cipher texts and in addition the private keys, which are additionally POMs got diagnostically. Also, the annoying form issue can likewise be completely determined amid the era technique of these POMs. The recovered images by this technique are completely free from the cross-talk noise that riddles past obstruction based multiple-image encryption strategies. Numerical results are exhibited to check the legitimacy of the proposed methodology [65].

As of late, a double-image encryption plan utilizing nearby pixel scrambling procedure and gyrator transform has been proposed [65]. Through author's representations, there is serious cross-talk unsettling influence in the phase-based image when the encoded information experiences noise bother or impediment attack. The unsettling influence will result in genuine crumbling in the recovered phase-based image and realize visibility ambiguities to the recipient, and consequently downsize the practicability of the cryptosystem. In this paper, point by point dissection of the cross-talk aggravation in the original structure will be firstly given out, and then the comparing change is along these lines proposed. Numerical recreations results demonstrate that the enhanced plan well address the cross-talk unsettling influence

and further upgrade the security of the first cryptosystem [66].

3.1.3 Hybrid Domain

In [67] the proposed encryption strategy is built with respect to wavelet transformation and chaotic map. The image is transformed using wavelet deterioration so as to map all critical information to the low frequency sub-band. Along these lines, a high quality chaotic encryption is embraced to scramble the low frequency wavelet coefficients, while the XOR is worked on the image districts in the high frequency band. A further wavelet recreation is embraced for distributing the encrypted information of the low frequency band to the image all in all. After Arnold scrambling of the resultant wavelet reproduced image, the image is then diffused to smooth out the areas of encryption. The strategy's execution is seen to be sensible focused around the reported encryption time of 0.266 s and a key space of 2,128.

El-Latif et al. [68] proposed the combination of the linear feedback shift register (LFSR) and chaotic systems in hybrid domains. First, permutation is performed on the input image pixel positions based on 2D chaotic map in the frequency domain. Second, the resultant image is diffused by applying the cryptographic primitive operations combined with the LFSR and chaotic map. On the basis of the result reported in [53], their method can be said to be immune from brute force attacks. It was also observed that a large key space of 2,256 was obtained. They also recorded the encryption time of 0.023 s, which shows that their method is very fast and appropriate for real-time application. With the entropy value of 7.999, their method can be said to be robust to exhaustive attack and the possibility of threat is minimal.

The existing ways to encrypt images based on compressive sensing usually treat the whole measurement matrix as the key, which renders the key too large to distribute and memorize or store. To solve this problem, a new image compression–encryption hybrid algorithm is proposed to realize compression and encryption simultaneously, where the key is easily distributed, stored or memorized. The input image is divided into four blocks to compress and encrypt, then the pixels of the two adjacent blocks are exchanged randomly by random matrices. The measurement matrices in compressive sensing are constructed by utilizing the circulant matrices and controlling the original row vectors of the circulant matrices with logistic map. And the random matrices used in random pixel exchanging are bound with the measurement matrices. Simulation results verify the effectiveness, security of the proposed algorithm and the acceptable compression performance [69].

Remote-sensing technology plays an important role in military and industrial fields. Remote-sensing image is the main means of acquiring information from satellites, which always contain some confidential information. To securely transmit and store remote-sensing images, we propose a new image encryption algorithm in hybrid domains. This algorithm makes full use of the advantages of image encryption in both spatial domain and transform domain. First, the low-pass sub-band coefficients of image DWT (discrete wavelet transform) decomposition are sorted by a PWLCM system in transform domain. Second, the image after IDWT (inverse discrete wavelet transform) reconstruction is diffused with 2D (two-dimensional) Logistic map and XOR operation in spatial domain. The experiment results and algorithm analyses show that the new algorithm possesses a large key space and can resist brute-force, statistical and differential attacks. Meanwhile, the proposed algorithm has the desirable encryption efficiency to satisfy requirements in practice [70].

Security of data is very important, when it comes to digital images the bulkiness of the data makes the standard data security methods unsuitable, so novel techniques have to be proposed to secure the image data. Image scrambling is one of the methods, however it does not change the pixel value rather it just changes its position making it prone to attacks. In this paper we have made use of Image scrambling technique in our framework, which results in encrypting the digital images to make them more secure. Earlier to this Non-sinusoidal transforms were used; here we have explored all the combinations of hybrid transforms using Kekre transform as the base transform with other non-sinusoidal transforms. The experimental results obtained are good when compared to individual non-sinusoidal transforms [71].

Security of image is the serious issue now-a-days because of ever increases in multimedia development and brute force attacks. In this paper we are introducing a best hybrid model for image encryption

composed of genetic algorithm and chaotic function. In the first stage of proposed method number of encrypted images is constructed using secret key and chaotic function. In the next stage, these encrypted images are used as initial population for genetic algorithm. In this proposed method genetic algorithm is used to obtain optimum result and in the last stage best cipher image is selected based on calculation of correlation coefficient and entropy. The image having lowest correlation coefficient and highest entropy is selected as best cipher image. In this paper first time we are using genetic algorithm for encryption of images. Entropy and correlation coefficient obtained by using this method are 7.9978 and −0.0009 respectively [72].

Krishnamoorthi and Murali proposed a new hybrid-domain image encryption technique that uses the frequency-domain encryption with Discrete Cosine Transform (DCT) incorporating multi resolution approach and spatial domain for pixel shuffling. First, original image divided into significant and insignificant blocks using Prewitt's edge detector operator and significant blocks are encrypted using Arnold cat map and Logistic map. Next, insignificant blocks are shuffled in the DCT domain using Arnold cat map then inverse DCT applied and pixels in the blocks are XORed with discretised output of logistic map. Finally, diffusion process is applied to get final encrypted image and the numerical simulations have demonstrated the security and robustness of the proposed encryption scheme [73].

All image encryption systems are in the single domain. Hybrid domain (frequency and time domain) system is proposed to make the system more secured. We use the chaotic maps to generate pseudo random images. Since the chaotic maps have very good properties, it will help us to encrypt the image in more secured manner. In our proposed system we employ two units: Transformation and substitution unit. We perform discrete Fourier transform and discrete wavelet transform for the image. Transformation unit uses the tent map and substitution unit uses Bernoulli map [74].

3.2 Selective Encryption

In customary image and video content insurance schemes, called fully layered, the entire substance is encrypted. Selective encryption is a strategy which just encodes a segment of a compressed bitstream. It comprises of encrypting just a subset of the data. Thusly, selective encryption is now and again called partial encryption. An essential property of the selective encryption is that the encrypted bitstream could be decoded by standard decoders so that both the encrypted and unencrypted bits of the layered bitstream might be precisely decoded and showed. Therefore, selective encryption is additionally alluded to as configuration consistent encryption. With the capacity of selective encryption, numerous purposes could be accomplished. The selective encryption system dissimilar to the full encryption strategy, encodes just noteworthy locales in a given image. The main value of the selective encryption strategy will be that it can give just as, security and computational necessities without tradeoffs [66]. The favorable circumstances of the selective encryption method are fundamentally progressively applications, where privacy is imperative and gigantic measure of data becomes possibly the most important factor. Progressively, a vital inquiry is normally how to minimize the computational necessities for secure mixed media. Addressing this worry from the partial encryption point of view is one of the basic answers for computational intricacy issue.

The partial image encryption techniques are determined from the process of separating information into perceptually delicate and insensitive data focused around recognition. Here, we present literature works that tended to the central prerequisite of a partial encryption plan, which is that the encrypted region must be independent of the unencrypted areas. Therefore, the proposed schemes in the writing that we will audit in the resulting dialogs will be investigated on the premise of their approach in meeting the partial encryption prerequisites. Otherwise, their strategies will be finished up to be inclined to attack on the premise of the connections between the encrypted and unencrypted pixels [75].

In this segment, partial encryption plan is portrayed with numerous research endeavors in this classification envelops all domains to be specific, spatial, frequency and hybrid. In ensuing areas, we will accentuate on the techniques in these studies on the premise of the domains of usage and the encryption approaches, for example, block cipher and stream cipher approaches.

3.2.1 Spatial Domain

In 2002, van Droogenbroeck and Benedett proposed the selective encryption methods for uncompressed (raster) images and compressed (JPEG) images [77]. According to van Droogenbroeck and Benedett, at least 4–5 least significant bitplanes should be encrypted to achieve the satisfactory visual degradation of the image.

Podesser, Schmidt and Uhl [78] proposed a selective encryption algorithm for the uncompressed (raster) images, that is inverse from the first system by van Droogenbroeck and Benedett. In the raster image that comprises of 8 bit planes, Schmidt and Uhl's algorithm encodes just the most significant bitplanes. The proposed underlying cryptosystem for this technique was AES. Then again, without loss of generality, any quick traditional cryptosystem may be picked instead.

Rao et al. [79] the image is initially isolated into connected and uncorrelated data by separating it into initial four MSB planes and last four LSB planes. Then a pseudo random succession on the uncorrelated data is utilized to scramble the corresponded data. And in the meantime, the uncorrelated data still remains unencrypted, thereafter the connected data is combined with uncorrelated data using cipher to obtain the final image. It is watched that the encrypted image seems loud, which increases detectable quality of the encrypted district, thereby increasing risk. All the more along these lines, the computational unpredictability issue is not tended to.

In [80], Wong and Bishop proposed a multi-level ROI image encryption general structural engineering, for biometric data. In their work, the multi-level ROI encryption and RC4 were utilized to encode an uncompressed raster image. The thought behind their technique is that for an approved viewer, just the indicated regions could be seen. In pith, just an approved individual can view the substance of the encrypted image, however this is fundamentally for the biometric system. At the initial step, various ROIs will be chosen for every image, which are then encrypted at three levels of power using RC4 and fingerprint matching algorithm. We watched that their technique can give image information security; however the key space size (2,128) is substantial, which demonstrates that the system could be touchy to little change in secret key.

In [81], the advanced encryption standard AES-Rijndael was actualized focused around five criteria, which are plain data clamping, block sizes, selectable round, programming execution enhancement, and entire routine choice technique. These criteria structure the premise of their purported SEA selective encryption system, which is a change of the AES algorithm. We examined that their procedure decreased execution time by half, the locale on the encrypted data is over 35 % and the entropy quality is about 7.9892. Thus, in view of these values, it might be derived that the security level of their system is on the normal level.

Kumar [82], improved the RC4 algorithm for increased security of the RC4 against attacks. The improved RC4 was then actualized with the selective image encryption technique. The selective image encryption technique is of two steps; (1) for choice of significant image area, and (2) for encrypting the chose locales of the image. On the premise of the selection approach, it could be said that less security and less time during encryption is obtainable. Notwithstanding, with the little locale on the original image, where the encryption is performed, security may be bargained.

Rad et al. [83], proposed another image encryption technique by combining a few secured algorithms: Blowfish, AES, Serpent and RC6. The strategy encodes the touchy blocks while insensitive block will be rescanning using four distinctive pattern types. Each one block is named significant or insignificant block by means of edge recognition technique. In encryption phase, the combination method was received for ensuring that different security levels are attained on the premise of the imperativeness of the block. The proposed system gives diverse levels of security to the blocks of varying vitality in request to lessen computational assets. This strategy offers a tiny level of consistency where attacker is hard to break cipher image.

Panduranga and Naveenkumar [84] proposed two selective image encryption systems. By first system, the image is separated into sub blocks. The selected blocks are then encrypted by image mapping that is utilized as input to the selected blocks. The full encryption of selected blocks is additionally conceivable, and every block can use the separate map image. Second technique, the position of items in a given image is identified naturally using the

morphological techniques, which place the positions of the objects of the given image. Then encryption of information is made on the distinguished article, which is then mapped to the original image. These two approaches will be extremely appropriate for uncommon applications such as therapeutic image and satellite image. These techniques utilized here will be most valuable when the range or locale of interest is known.

3.2.2 Frequency Domain

Rodrigues et al. [85] proposed a technique that is based on AES stream ciphering using variable length coding (VLC) of the Huffman's vector. To start with, the input image is partitioned into blocks of 8 × 8 pixels. Second, each block is transformed from the spatial domain to the frequency domain using discrete cosine transform (DCT). Third, the quantization is connected on the resultant image using Zigzag scan system then applying AES encryption strategy. The benefits observed for the technique in [29] is that there is the possibility of identifying one or two regions for each block of 8 × 8 pixels or assembly of them. This comes from the fact that they have utilized the AES as a part of CFB (cipher feedback block) mode, and have connected it over each block. It is vital to note that the ROI must be defined in unit of block of 8 × 8 pixels as a default of JPEG arrangement. Their strategy is seen to have substantial key space of 2,128 that gives the encryption system high affectability to a little change in secret key.

Ou et al. [85], proposed the region-based selective encryption strategy, which will be basically for encrypting medical data. Firstly, two MSBs within the region of interest (ROI) will be converted to coefficients using the wavelet transform. Then the AES in CFB (cipher feedback block) mode is utilized to encrypt only certain regions of the data in code-stream. Based on the fact, the size of the encrypted bit-stream remained unchanged. Their trial results disclose that the technique gives low security level.

Yekkala et al. [86], utilized DCT transformation and scalable lightweight encryption technique to encrypt selected blocks that contain edges. The thought behind their selection approach is to encrypt selected blocks with crucial information by utilizing the limit values at a particular range, while the blocks belonging to other ranges are unencrypted. The PSNR esteem of 14.46 db will be obtained, which translates that an intruder or attacker cannot decipher the secret key utilized for the encryption.

Brahimi et al. [87], proposed a novel selective encryption of image plane based on JPEG2000, which encrypts only the code-blocks corresponding to some subtle terrain. The permutation of blocks code elected in the selected precinct is utilized to enhance the security. AES symmetric encryption will be utilized with CFB mode to encrypt the exchanged code blocks. The measure of data processed in the encryption is minimized through permutation and selective encryption together. This algorithm work with any standard ciphers and requires less computational cost. The encrypted territory is around 11.64 % when this range of original image is little with less time for encryption yet security is great when the encrypted image will be independent to the original image because PSNR has little value, around 6.74 db with difficulty to recover the original image without knowing the secret key.

In [88], the new technique is introduced using three levels of permutation on selected blocks and coefficients of orthogonal polynomials transform domain. The original image will be first isolated into blocks of 4 × 4 pixels and scrambled them in three times. Firstly, scrambling selected bits through applying the orthogonal polynomials based transform (OPT) then compute the block of OPT coefficients. Then the low level coefficients in OPT of each block will be orchestrated into a one dimensional zigzag sequence. The blocks to be rearranged are selected according to a pseudo-random sequence created using a secret sub-key as the seed. Finally, the blocks are part into subsets and rearranged. This shuffling changes the high state spatial configuration of the content, which is much harder for an attacker to break down. The OPT is configured as an integer transform for less computation time. To reduce the encryption time the scrambling of bits, coefficients and blocks are also controlled. The OPT is accounted for to have huge key space which will be known to increase chances of risk. And with the reported 0.0366 correlation coefficient value, OPT assumed to be powerful against brute force statistical and differential attacks. The technique is additionally reported to have used standard size of 25 % for the region of encryption, which is a decent indication that the encrypted image is independent of the original image.

In Kulkarni et al. [89], a selective encryption approach was proposed. The selection uses five level wavelet transformations to decompose the input image by applying the wavelet filter banks. To orchestrate the image in hierarchal structure, the high pass band and low pass band filters are utilized so each structure is of diverse significance. According to human visual system (HVS), the debased version of original image by the proposed technique gives a sufficient level of transparency. This system selecting the high correlation coefficient of five level sub-bands to control the security with transparency. Furthermore, PSNR has little esteem, around 3.448 db that is difficult for the intruder to recover the original image without knowing the secret key.

Younis et al. [90], proposed a new encryption technique; a critical part of image level two sub-band will be utilized by employing fuzzy c-means (FCM), an advanced technology for clustering examination combined with the permutation cipher. Only 6.25–25 % of the original data is encrypted with a significant reduction in the time of encryption and decryption. The encryption algorithm include: wavelet packet transform, quantization by FCM, permutation cipher and arithmetic coding to level-two sub-band images. The proposed partial encryption strategy will be quick and secure. "Wavelet based on vector quantization and permutation is more suitable for normal level of security because the PSNR of the reconstructed image is expansive. But, when the quantity of clusters increases, both PSNR and execution time are increase too." It can be seen that large key space should reduce danger and increases the insusceptibility from attacker.

Flayh et al. [91] proposed an efficient partial image encryption technique that utilizes three levels of the discrete wavelet transform (DWT) with the AES cipher and stream cipher. The image is smoothened using a smoothing filter in request to shroud points of interest of cipher image so that perceptibility of the encrypted regions in the image is reduced. It will be watched that the reconstructed image is very nearly the same as the original image. Their technique reduced encrypted regions by 1.5625 %, which therefore cut down the execution time for the encryption process. It can likewise be noted that the little portion encrypted increases the correlation of the cipher image, which may make the image to be prone to danger. All the more likewise, it is watched that AES, which is known to be of substantial key space, brought about the key space of 2,128 and when combined with cipher of 216 key space, an extensive key space is inevitable. Therefore, it ought to be noted that the size of the key space assumes a crucial part in ensuring that the encrypted information is secured.

Richard et al. [92] proposed a new selective regional encryption algorithm. The algorithm is utilized to partially encrypt the original image by permutation the coefficients in the DCT domain. Edge detection algorithm is utilized to separate image regions. This algorithm uses thresholding to separate thick image regions from more regrettable image regions. Then the median filter is connected on the resultant image to reduce commotion components in the image. A basic encryption strategy, which utilizes the properties of vitality compaction of a shape versatile cosine transformation, is then connected in the DCT domain. The encrypted territory is around 10 % with multi region for image encryption, which may increase security of encrypted data.

Sasidharan and Philip [93] proposed a quick partial image encryption scheme using Rc4 stream cipher and discrete wavelet transform (DWT). In their proposed technique, the encryption is carried out at the most reduced frequency band using the stream cipher. Their basic thought of the stream cipher was to retain all the image information. Be that as it may, using the stream ciphers consumes more time, since it typically encrypts one byte at a time. The bitwise exclusive-OR (XOR) will be utilized to combine between key stream and original image while the previous is produced by random numbers. At the point when edges are encountered, a shuffling algorithm is utilized. The encryption time is reduced by encrypting only the most minimal frequency band of the image and maintains an abnormal state of security by shuffling whatever remains of the image using the shuffling algorithm with an extensive key space estimation of around 2,256. It can be seen in [73] that the entropy consequence of the encrypted image, which is around 4.7807, gives a more liberated stage for an intruder to decipher the secret key used to encrypt the image. At the same time it is strong against statistical attack because PSNR has high esteem, around 20.7056 db.

Kuppusamy and Thamodaran [94] proposed a partial image encryption optimization scheme using

high vitality coefficients of the transformed image, which were selected by employing the particle swarm optimization (PSO) technique within the daubechies4 domain for encryption. Our observation is that with the key space of 2,256 and the capacity to increase the key space by increasing the number of permutation for each permutation round, reaches to the normal level of security. The encrypted range of the image is about 33 %, which will be a little rate that indicates medium speed for encryption.

In [95], a technique that applies the Arnold Cat map permutation on low frequency sub-band of the DCT transformed image for encryption was proposed. Their main idea for selecting the low frequency sub-band of the DCT transformed image is attributed to the fact that the human visual system (HVS) is more drawn to information at the lower frequencies than the higher frequency information. Important information such as object, shape, etc. is presented in low frequency sub-bands, while the detailed information is contained in higher frequency sub-bands. Our inference is that, since only the DCT coefficient of the low frequency sub-bands is encrypted, the likelihood of predicting the encrypted information is reduced. The technique in [96] is considered to be robust against noise, though to some extent since the decrypted image shows some presence of noise.

An image encryption plan is proposed focused around fractional Mellin transform and phase recovery method. Any image might be picked as cipher text, the chose annular space of the specified image is first transformed by fractional Mellin transform. With the transformed result and original image, phase-key could be concentrated by utilizing phase recovery procedure as a part of fractional Fourier space. The proposed plan can diminish the load of transmission, extend key space, and might be stretched out to numerous image encryptions. The results of proposed technique show the attainability and adequacy of the proposed plan [96].

A new method for image encryption by selecting specific higher frequencies of DCT coefficients that taken as the characteristic values, encrypting them and the resulted encrypted blocks are shuffled according to a pseudo-random bit sequence is proposed. Selective encryption is a recent approach to reduce the computational requirements for huge volumes of images. Image Encryption is a wide area of research. Encryption basically deals with converting data or information from its original form to some other form that hides the information in it. The protection of image data from unauthorized access is important. Encryption is employed to increase the data security. The encrypted image is secure from any kind cryptanalysis. In the proposed work, the image to be encrypted is decomposed into 8×8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT then only selected DCT coefficients i.e., the DCT coefficients correlated to the higher frequencies of the image block are encrypted. For encryption the DCT coefficients are Xored with pseudorandom bit, pseudorandom bit is generated by nonlinear shift back register. The bits generated by nonlinear shift back register cannot be predicted so cryptanalysis becomes difficult. To enhance the security further the unencrypted DCT coefficients are shuffled, since some information may also be stored in DCT coefficient correlating to lower frequency, While encrypting selected DCT coefficients alone will provide complete perceptual encryption, it would be possible for an attacker to gain information about the image from the other coefficients, especially in images that have a lot of edges [97].

Another strategy for image encryption by selecting particular higher frequencies of DCT coefficients that taken as the trademark qualities, scrambling them and came about scrambled blocks are rearranged as indicated by a pseudo-random bit arrangement is proposed. Partial encryption is a late approach to diminish the computational prerequisites for colossal volumes of images. Image Encryption is a wide region of examination. Encryption fundamentally bargains with changing over information or data from its original structure to some other structure that conceals the data in it. The insurance of image information from unapproved access is paramount. Encryption is utilized to build the information security. The encoded image is secure from any sort cryptanalysis. In the proposed work, the image to be encoded is disintegrated into 8×8 blocks, these blocks are transformed from the spatial space to recurrence area by the DCT then just chose DCT coefficients i.e., the DCT coefficients related to the higher frequencies of the image block are scrambled. For encryption the DCT coefficients will be Xored with pseudorandom bit, pseudorandom bit will be

created by nonlinear movement back register. The bits created by nonlinear movement back register can't be anticipated so cryptanalysis gets to be troublesome. To upgrade the security further the decoded DCT coefficients are rearranged, since some data might likewise be put away in DCT coefficient corresponding to lower recurrence, while scrambling chose DCT coefficients alone will give complete perceptual encryption, it would be conceivable for an aggressor to pick up data about the image from the other coefficients, particularly in images that have a ton of edges [97].

In [98], a method for quicker image encryption is proposed. Here authors have been receiving fractional image encryption to diminishing the time needed for encryption and unscrambling, instead of scrambling the entire image just the chose bit of the image are scrambled, this makes the encryption quicker and diminishes the time intricacy. Compression is excluded in this system since compression necessity for each one image is not novel. To add extra security to the image in the cryptosystem, in the wake of scrambling the chose higher coefficients, all the coefficients could be mixed. The thought behind scrambling all the coefficients is to withstand any kind of attack.

3.2.3 *Hybrid Domain*

Yen and Guo [23] proposed partial encryption routines that are suitable for images compacted with two particular classes of compression algorithms: (a) quad tree compression algorithms and (b) wavelet compression algorithms based on zero trees.

One of the writings that investigated the benefits of combining the spatial and frequency domain for successful encryption method is Taneja et al. [99]. In their work the fractional wavelet was utilized to encode only significant sub-bands using Arnold Cat map and logistic map. They most importantly encrypted the significant piece of the image in spatial domain and then the insignificant parts will be partially encrypted in the wavelet based frequency domain. Preceding the frequency processing the Prewitt edge indicator is utilized to remove edges in the image, which speak to the significant piece of the image. The security analysis of the proposed technique is an indication that their system guarantees better perceptual and cryptography because of the less computational time required to encode the image. It might be concluded that the encrypted image attained in the hybrid domain using the strategy is independent of the original image and is additionally hard to adjust.

A novel concept that combines phase manipulation and sign encryption in partial image encryption system was proposed by Parameshachari et al. [100]. The encryption procedure consists of two stages: in the first stage, the phase and size of the input image are determined using the fast Fourier transform (FFT) then the phase component of the image is mixed former of the inverse fast Fourier transformation (IFFT) in request to obtain the adjusted version of the image. For the second stage, the changed image is partially encrypted by using sign encryption. The sign encryption is obtained by extracting the sign bits of the changed image in the partially encrypted image. It could be concluded that the proposed strategy is quick and of low security for the encrypted data. It is likewise obvious that the encrypted image is independent of the original image and will be troublesome for an intruder to know the secret key given the medium estimation of the entropy and more risk prone accomplished.

Karl Martin et al. proposed a partial image encryption system utilizing Color-SPIHT compression. Image encryption is attained by scrambling just bits of individual wavelet coefficients for k iterations of the C-SPIHT algorithm. Fluctuating k transforming overhead and level of secrecy is attained [101].

4 Conclusions

In this paper, large portions of the current essential image encryption methods have been exhibited and examined. In this review report, at first the stress have been made on officially existing image encryption algorithms in light of the fact that the most ideal method for ensuring media information like images is by method for the gullible algorithm; i.e., by scrambling the whole sight and sound bit succession utilizing a quick conventional cryptosystem. A great part of the past and momentum exploration targets scrambling just a deliberately chose piece of the image bit-stream keeping in mind the end goal to decrease the computational burden, and yet keep the security level high. Huge numbers of the proposed plans could just accomplish moderate to low level of security, which

may discover applications in which quality debasement is favored over outright security. Then again, just few of the proposed strategies guarantee to attain considerable security, which is the prime prerequisite in numerous media applications. Secondly, we evaluated a wide-run of image encryption algorithms and ordered them on the premise of full and partial image encryption procedures under spatial space, frequency domain and hybrid domain categories. In the process of this survey, a few perceptions were made, which are that full encryption plan guarantees high state of security of encoded information because of the way that they encode the whole image, however much time is used in such a procedure. On account of selective image encryption, just a locale or some piece of the image is scrambled. The time used in encoding the region of investment is less in contrast to the full encryption procedures. Hence, the partial encryption scheme is more suitable for constant applications. Therefore, partial image encryption scheme proved to be encouraging in term of encryption time, attaining an encryption procedure that adjusts security with transforming time for ongoing applications is still a challenge for researcher in image encryption. On the other hand, some key elements, for example, the sort of information to be encoded, the rate of the information that must be ensured and the measures put set up to ensure the information from cryptanalytic attack, when considered in the configuration of a continuous image encryption procedure might be a reasonable answer for ongoing image encryption issues.

References

1. Shannon, C. E. (1948). The mathematical theory of communication. *The Bell System Technical Journal, 27*, 379–423.
2. Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal, 28*, 656–715.
3. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). *Applied cryptography*. Boca Raton: CRC.
4. Ding, W., Yan, W.-Q., & Qi, D.-X. (2000). *A novel digital hiding technology based on Tangram Encryption*. *IEEE Proceedings of on NEWCAS* 2005, *and Conways Game. Proceeding of* 2000 *International Conference on Image Processing* (Vol. 1, pp. 601–604), September 2000.
5. Zhao, X.-F. (2003). Digital image scrambling based on the Baker's transformation. *Journal of Northwest Normal University (Natural Science), 39*(2), 26–29.
6. Bao, G.-J., Ji S.-M., & Shen J.-B. (2002). Magic cube transformation and its application in digital image encryption. *Computer Applications*, *22*(11), 23–25.
7. Guibin Z, Changxiu C, Hu Zhongyu, et al. (2003). An image scrambling and encryption algorithm based on affine transformation. *Journal of Computer-Aided Design & Computer Graphics*, *15*(6), 711–715.
8. Jawad, L. M., & Sulong, G. B. (2013). A review of color image encryption techniques. *International Journal of Computer Science Issues, 10*(6), 266–275.
9. Sharma, M., & Kowar, M. K. (2010). Image encryption techniques using chaotic schemes: a review. *International Journal of Engineering Science and Technology, 2*, 2359–2363.
10. Li, C.-G., Han, Z.-Z., & Zhang, H.-R. (2002). Image encryption techniques: A survey. *Journal of Computer Research and Development, 39*(10), 1317–1324.
11. Rober, A., & Matthews, J. (1989). On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, *XIII*(1), 29–42.
12. Habutsu, T., Nishio, Y., Sasase, I., & Mori, S. (1990). A secret key cryptosystem using a chaotic map. *Transactions of the IEICE*, *E*73(7), 1041–1044.
13. Schwartz, C. (1991). A new graphical method for encryption of computer data. *Cryptologia, 15*(1), 43–46.
14. Bourbakis, N., & Alexopoulos, C. (1992). Picture data encryption using scan patterns. *Pattern Recognition, 25* (6), 567–581.
15. Kuo, C. J. (1993). Novel image encryption technique and its application in progressive transmission. *Journal of Electronic Imaging, 2*(4), 345–351.
16. Chang, K.C., & Liu, J.L. (1994). An image encryption scheme based on quad-tree compression scheme. In *Proceedings of the 1994 International Computer Symposium*, *Taiwan*, (pp. 230–237).
17. Alexopoulos, C., Bourbakis, N., & Ioannou, N. (1995). Image encryption method using a class of fractals. *Journal of Electronic Imaging, 43*, 251–259.
18. Yang, H.-G., & Kim, E.-S. (1996). Practical image encryption scheme by real-valued data. *Optical Engineering, 35*(9), 2473–2478.
19. Scharinger, J., & Pichler, F. (1996). Image encryption based on chaotic maps. *Proceedings of the 20th workshop of the Austrian Association for Pattern Recognition* (*OAGM/AAPR*) *on Pattern recognition 1996* (pp. 159–170).
20. Fridrich, J. (1997). Image encryption based on chaotic maps. *Proceedings of IEEE Conference on Systems*, *Man*, *and Cybernetics* (pp. 1105–1110).
21. Baptista, M. S. (1998). Cryptography with chaos. *Physics Letters A, 240*, 50–54.
22. Guo, J.-I., & Yen, J.-C. (1999). A new mirror-like image encryption algorithm and its VLSI architecture, Department of Electronics Engineering, National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China in 1999.
23. Yen, J.-C., & Guo, J.-I. (2000). New chaotic key-based design for image encryption and decryption. *IEEE International Symposium on ISCAS 2000*, *Geneva* (pp. IV-49–IV-52), May 2000.
24. Sobhy, M. I., & Shehata, A. R. (2001). Chaotic algorithms for data encryption. *IEEE Proceeding of ICASSP 2001*, (Vol. 2, pp. 997–1000), May 2001.
25. Masuda, N., & Aihara, K. (2002). Cryptosystems with discretized chaotic maps. *IEEE Transactions on Circuits*

and Systems I Fundamental Theory and Applications, *49* (*1*), 28–40.
26. Sinha, A., & Singh, K. (2003). A technique for image encryption using digital signature. *Optics Communications*, 1–6. Retrieved from www.elsevier.com/locate/optcom.
27. Sallen, M., Ibrahim, S., & Isnin, I. F. (2003). Enhanced chaotic image encryption algorithm based on Baker's map. *IEEE Proceedings of ISCAS 2003*, 2, II-508–II-511.
28. Shin, C.-M., Seo, D.-H., Chol, K.-B., Lee, H.-W., & Kim, S. J. (2003). Multilevel image encryption by binary phase XOR operations. *IEEE Proceedings in the year 2003*.
29. Belkhouche, F., & Qidwai, U. (2003). Binary image encoding using 1D chaotic maps. *IEEE Proceedings in the year 2003*.
30. Ying, W., DeLing, Z., Lei, J., et al. (2004). The spatial-domain encryption of digital images based on high-dimension chaotic system. *Proceedings of 2004 IEEE Conference on Cybernetics and Intelligent Systems*, *Singapore*, December 2004 (pp. 1172–1176).
31. Zhang, M.-R., Shao, G.-C., & Yi, K.-C. (2004). T-matrix and its applications in image processing. *IEEE Electronics Letters*, *40*(25), 1583–1584.
32. Deng, S., Zhang, L., & Xiao, D. (2005). Image encryption scheme based on chaotic neural system. In J. Wang, X. Liao, & Z. Yi (Eds.) *Advances in neural networks*, ISNN 2005, LNCS 3497 (pp. 868–872).
33. Gu, G., & Han, G. (2006). An enhanced chaos based image encryption algorithm. *IEEE Proceedings of the First International Conference on Innovative Computing*, *Information and Control* (*ICICIC'06*) *in 2006*.
34. Xiao, H.-P., & Zhang, G.-J. (2006). An image encryption scheme based on chaotic systems. *IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics*, *Dalian*, *13–16 August 2006*.
35. Nien, H. H., Huang, W. T., Hung, C. M., Chen, S. C., Wu, S. Y., Huang, C. K., et al. (2009). Hybrid image encryption using multi-chaos-system. In *7th International Conference on Information*, *Communications and Signal Processing* (*ICICS*), *December 2009* (pp. 1–5).
36. Rhouma, R., Arroyo, D., & Belghith, S. (2009). A new color image cryptosystem based on a piecewise linear chaotic map. In *6th International Multi-Conference on Systems*, *Signals and Devices*, *March 2009*, (pp. 1–6).
37. Ahmad, M., & Alam, M. (2009). A new algorithm of encryption and decryption of images using chaotic mapping. *International Journal on Computer Science and Engineering, 2*(1), 46–50.
38. Wei, W., Fen-lin, L., Xinl, G., & Yebin, Y. (2010). Color image encryption algorithm based on hyper chaos. In *2nd IEEE International Conference on Information Management and Engineering*, *2010* (pp. 271–274).
39. Kamali, M. R., Hossein, S., Shakerian, R., & Hedayati, M. (2010). A new modified version of advanced encryption standard based algorithm for image encryption. *International Conference on Electronics and Information Engineering* (*ICEIE*), *2010*, *1*(Iceie), 141–145.
40. Aihong, Z., Lian, L., & Shuai, Z. (2010). Research on method of color image protective transmission based on logistic map. In *International Conference on Computer Application and System Modeling* (*ICCASM*), *Oct. 2010*, Vol. 9, No. Iccasm, pp. 266–269.
41. Rodriguez-Sahagun, M. T., Mercado-Sanchez, J. B., Lopez-Mancilla, D., Jaimes-Reategui, R., & Garcia-Lopez, J. H. (2010). Image encryption based on logistic chaotic map for secure communications. *IEEE Electronics*, *Robotics and Automotive Mechanics Conference*, *Sep. 2010*, (pp. 319–324).
42. Mastan, J. M. K., Sathishkumar, G. A., & Bagan, K. B. (2011). A color image encryption technique based on a substitution–permutation network. *Advances in Computing and Communications, 4*, 524–533.
43. Pareek, K. K. S., Narendra K, & Patidar, V. (2011). A symmetric encryption scheme for colour BMP images. *International Journal of Computer Applications*, *Special Issue on Network Security and Cryptography*, 42–46.
44. Abugharsa, A. B., & Almangush, H. (2011). A new image encryption approach using block-based on shifted algorithm. *International Journal of Computer Science and Network Security (IJCSNS), 11*(12), 123–130.
45. Yadav, R. S., Beg, M. H. D. R., & Tripathi, M. M. (2013). Image encryption techniques: A critical comparison. *International Journal of Computer Science Engineering and Information Technology Research, 3*(1), 67–74.
46. Zhang, G., & Liu, Q. (2011). A novel image encryption method based on total shuffling scheme. *Optics Communication, 284*, 2775–2780.
47. Eslami, Z., & Bakhshandeh, A. (2013). An improvement over an image encryption method based on total shuffling. *Optics Communications, 286*, 51–55.
48. Ding, X., & Chen, G. (2014). Optical color image encryption using position multiplexing technique based on phase truncation operation. *Optics & Laser Technology, 57*, 110–118.
49. Zhang, Y., & Xiao, D. (2014). An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. *Communications in Nonlinear Science and Numerical Simulation, 19*, 74–82.
50. Sinha A., Singh, K. (2013). Image encryption using fractional Fourier transform and 3D Jigsaw transform. Retrieved from http://pdf-world.net/pdf-2013/Image-encryption-using-fractional-Fourier-transform-and-3D-Jigsaw-transform-pdf.pdf.
51. Zhou, N., Wang, Y., Gong, L., Chen, X., & Yang, Y. (2012). Novel color image encryption algorithm based on the reality preserving fractional Mellin transform. *Optics & Laser Technology, 44*(7), 2270–2281.
52. Abuturab, M. R. (2012). Securing color information using Arnold transform in gyrator transform domain. *Optics and Lasers in Engineering, 50*(5), 772–779.
53. He, Y., Cao, Y., & Lu, X. (2012). Color image encryption based on orthogonal composite grating and double random phase encoding technique. *Optik (International Journal for Light and Electron Optics), 123*(17), 1592–1596.
54. Chen, H., Du, X., Liu, Z., & Yang, C. (2013). Color image encryption based on the affine transform and gyrator transform. *Optics and Lasers in Engineering, 51* (6), 768–775.
55. Sui, Liansheng, & Gao, Bo. (2013). Single-channel color image encryption based on iterative fractional Fourier transform and chaos. *Optics & Laser Technology, 48*, 117–127.

56. Zhang, Y., Xiao, D., Wen, W., & Tian, Y. (2013). Edge-based lightweight image encryption using chaos-based reversible hidden transform and multiple-order discrete fractional cosine transform. *Optics & Laser Technology, 54*, 1–6.
57. Liu, S., & Sheridan, J. T. (2013). Optical encryption by combining image scrambling techniques in fractional Fourier domains. *Optics Communications, 287*, 73–80.
58. Liu, Z., Li, S., Liu, W., Wang, Y., & Liu, S. (2013). Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. *Optics and Lasers in Engineering, 51*, 8–14.
59. Li, H., Wang, Y., Yan, H., Li, L., Li, Q., & Zhao, X. (2013). Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform. *Optics and Lasers in Engineering, 51*, 1327–1331.
60. Sui, L., Xin, M., Tian, A., & Jin, H. (2013). Single-channel color image encryption using phase retrieve algorithm in fractional Fourier domain. *Optics and Lasers in Engineering, 51*, 1297–1309.
61. Kumar, M., Mishra, D. C., & Sharma, R. K. (2014). A first approach on an RGB image encryption. *Optics and Lasers in Engineering, 52*, 27–34.
62. Liu, Z., Zhang, Y., Li, S., Liu, W., Liu, W., Wang, Y., et al. (2013). Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains. *Optics & Laser Technology, 47*, 152–158.
63. Kong, Dezhao, & Shen, Xueju. (2014). Multiple-image encryption based on optical wavelet transform and multichannel fractional Fourier transform. *Optics & Laser Technology, 57*, 343–349.
64. Ran, Q., Zhao, T., Yuan, L., Wang, J., & Lei, X. (2014). Vector power multiple-parameter fractional Fourier transform of image encryption algorithm. *Optics and Lasers in Engineering, 62*, 80–86.
65. Qin, Y., Jiang, H., & Gong, Q. (2014). Interference-based multiple-image encryption by phase-only mask multiplexing with high quality retrieved images. *Optics and Lasers in Engineering, 62*, 95–102.
66. Chen, J-x, Zhu, Z-l, Fu, C., Zhang, L-b, & Yu, H. (2015). Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains. *Optics and Lasers in Engineering, 66*, 1–9.
67. Yu, Z., Zhe, Z., Haibing, Y., Wenjie, P., & Yunpeng, Z. (2010). A chaos-based image encryption algorithm using wavelet transform. In *2nd International Conference on Advanced Computer Control*, *March 2010*, *Vol. 2*, *No. 4*, (pp. 217–222).
68. El-Latif, A., Niu, X., & Amin, M. (2012). A new image cipher in time and frequency domains. *Optics Communications, 285*(21–22), 4241–4251.
69. Zhou, N., Zhang, A., Zhen, F., & Gong, L. (2014). Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. *Optics & Laser Technology, 62*, 152–160.
70. Zhang, X., Zhu, G., Ma, S. (2012). Remote-sensing image encryption in hybrid domains. *Optics Communications*, *285*, 1736–1743.
71. H. B. Kekre, Tanuja Sarode, Pallavi N. Halarnkar, Debkanya Mazumder, Image Encryption using Hybrid Transform Domain Scrambling of Coefficients, International Journal of Advance Research in Computer Science and Management Studies 2 (6) (2014).
72. Shubhangini, P., Nichat, S. S., & Sikchi, M. E. (2013). Image encryption using hybrid genetic algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*, 427–431.
73. Krishnamoorthi, R., Murali, P. (2012). A new hybrid-domain image encryption based on chaos with discrete cosine transform. *4th International Conference on Electronics Computer Technology*, *IEEE 2012*.
74. Ramahrishnan, S., Elakkiya, B., Geetha, R., Vasuki, P., Mahalingam, S. (2014). Image encryption using chaotic maps in hybrid domain. *International Journal of Communication and Computer Technologies*, *2*(5), 44–48.
75. Suresh, V., & Madhavan, C. E. V. (2012). Image encryption with space-filling curves. *Defence Science Journal, 62*(1), 46–50.
76. Rodrigues, J. M., Puech, W., & Bors, A. G. (2006). A selective encryption for heterogeneous color JPEG images based on VLC and AES stream cipher. *3rd European Conference on Colour in Graphics*, *Imaging and Vision (CGIV'06)*, *June 2006*, *Vol. 1*, (pp. 34–39).
77. van Droogenbroeck, M. & Benedett, R. (2002). Techniques for a selective encryption of uncompressed and compressed images. *Proceedings of Advanced Concepts for Intelligent Vision Systems* (*ACIVS*) *2002*, *Ghent*, *Belgium*, *September 9–11*.
78. Podesser, M., Schmidt, H.-P., & Uhl, A. (2002). Selective bitplane encryption for secure transmission of image data in mobile environments. *5th Nordic Signal Processing Symposium, on board Hurtigruten*, *Norway*, *October 4–7*.
79. Rao, Y. V. S., Mitra, A., & Prasanna, S. R. M. (2006). A partial image encryption method with pseudo random sequences (pp. 315–325) (Lecture Notes in Computer Science, Vol. 4332) [International Commission on Intervention and State Sovereignty (ICISS)]. Berlin: Springer.
80. Wong, A., & Bishop, W. (2007). Backwards compatible, multi-level region-of-interest (ROI) image encryption architecture with biometric authentication. *International Conference on Signal Processing and Multimedia Applications*, *July 2007*, (pp. 324–329).
81. Ju-Young, Oh, Dong-Il, Yang, & Chon, K. H. (2010). "A Selective Encryption Algorithm Based on AES for Medical Information". *Healthcare informatics research, 16*(1), 22–29.
82. Kumar, P. (2012). RC4 enrichment algorithm approach for selective image encryption. *International Journal of Computer Science & Communication Networks, 2*(2), 181–189.
83. Rad, R. M., Attar, A., & Atani, R. E. (2013). A comprehensive layer based encryption method for visual data. *International Journal of Signal Processing, Image Processing and Pattern Recognition, 6*(1), 37–48.
84. Panduranga, H. T., & Naveenkumar, S. K. (2013). Selective image encryption for medical and satellite images. *International Journal of Engineering and Technology (IJET), 5*(1), 115–121.

85. Ou, Y., Sur, C., & Rhee, K. H. (2007). Region-based selective encryption for medical imaging. *1st Annual International Workshop*, *2007*, *Vol. 4427*, *No. 4613* (pp. 62–73).
86. Yekkala, A. K., Udupa, N., Bussa, N., & Madhavan, C. E. V. (2007). Lightweight encryption for images. *IEEE International Conference on Consumer Electronics, 3*, 1–2.
87. Brahimi, Z., Bessalah, H., Tarabet, A., & Kholladi, M. K. (2008). A new selective encryption technique of JPEG2000 code stream for medical images transmission. *5th International Multi-Conference on Systems*, *Signals and Devices*, *July 2008* (pp. 1–4).
88. Krishnamoorthi, R., & Malarchelvi, P. D. S. K. (2008). Selective combinational encryption of gray scale images using orthogonal polynomials based transformation. *International Journal of Computer Science and Network Security, 8*(5), 195–204.
89. Kulkarni, N. S., Raman, B., & Gupta, I. (2008). Selective encryption of multimedia images. *32nd National Systems Conference*, *Dec. 2008* (pp. 467–470).
90. Younis, H. A., Abdalla, T. Y., & Abdalla, A. Y. (2009). Vector quantization techniques for partial encryption of wavelet-based compressed digital images. *Iraqi Journal of Electrical and Electronic Engineering, 5*(1), 74–89.
91. Flayh, N. A., Parveen, R., & Ahson, S. I. (2009). Wavelet based partial image encryption. *International Multimedia*, *Signal Processing and Communication Technologies* (*IMSPCT*), *Mar. 2009* (pp. 32–35).
92. Metzler, R. E. L., & Agaian, S. S. (2010). Selective region encryption using a fast shape adaptive transform. *IEEE International Conference on Systems*, *Man, and Cybernetic* (*ICSMC*), *2010* (pp. 1763–1770).
93. Sasidharan, S., & Philip, D. S. (2011). A fast partial encryption scheme with wavelet transform and RC4. *International Journal of Advances in Engineering & Technology (IJAET), 1*(4), 322–331.
94. Kuppusamy, K., & Thamodaran, K. (2012). Optimized partial image encryption scheme using PSO. In *International Conference on Pattern Recognition*, *Informatics and Medical Engineering*, *May 2012* (pp. 236–241).
95. Munir, R. (2012). Robustness analysis of selective image encryption algorithm based on arnold cat map permutation. In *Proceedings of 3rd Makassar International Conference on Electrical Engineering and Informatics*, *Nov. 2012*, (pp. 1–5).
96. Zhou, N., Liu, X., Zhang, Y., & Yang, Y. (2013). Image encryption scheme based on fractional Mellin transform and phase retrieval technique in fractional Fourier domain. *Optics & Laser Technology, 47*, 341–346.
97. Krikor, Lala, Baba, Sami, & Arif, Thawar. (2009). Zyad Shaaban image encryption using DCT and stream cipher. *European Journal of Scientific Research, 32*, 48–58.
98. Divya, V. V., Sudha S. K., & Resmy, V. R. (2012). Simple and secure image encryption. *International Journal of Computer Science*, *9*(*6*), 286.
99. Taneja, N., Raman, B., & Gupta, I. (2011). Combinational domain encryption for still visual data. *Multimedia Tools and Applications, 59*(3), 775–793.
100. Parameshachari P. B. D., Soyjaudah, K. M. S., & Devi K. A. S. (2013). Secure transmission of an image using partial encryption based algorithm. *International Journal of Computer Applications*, *63*(16), 33–36.
101. Martin, K., Lukac, R., & Plataniotis, K. N. (2005). Efficient encryption of wavelet-based coded color images. *Pattern Recognition, 38*(7), 1111–1115.