A Survey on Image Encryption Techniques

Sunil Kumar*,Manish Kumar*,RajatBudhiraja*, M.K.Das* and Sanjeev Singh*

Abstract

Information security plays an important role when confidential information is transferred between two or more parties. There are two approaches i.e. Cryptography and Steganography which are used to tackle security issues. In cryptography technique, information is stored and transmitted in a particular form in such a way that only intended user can read and process it but does not hide the existence of information. On the other hand Steganography basically conceals the existence of the information in such a way that other person except sender and receiver donot know about transfer of information. In steganography the confidential information is concealed in some other way that the confidential information is undistinguishable. In this paper a survey is done based on the existing techniques.

Keywords: Cryptography, Steganography, Encryption

Introduction

Information Security talks about the procedures and approaches which are in-tended and applied to secure sensitive, private and confidential information or data from illegal access, usage, misappropriation, revelation, obliteration, alteration. Confidentiality, integrity, and availability are the main components of information security. Cryptography and steganography are the two techniques which provide these services. The word Cryptography was origin from the Greek word secret writing. Cryptography is basically the procedure of adding some input data with a password stipulate by the user to produce an encrypted output. The input data given by user is called plaintext and encrypted data is called Cipher text. Basically data is encrypted in such a manner that only authorized user can get back the original plain text in a specific time. Ciphers are generated by combining plaintext with keys. Decryption is the process of renovating cipher text message back to plaintext (Leo Yu Zhanget al. 2014; Xingyuan Wang etal. 2015). Encryption techniques are widely used which basically makes the information secure. Importance of encryption has been growing as the increase in utilization of internet worldwide. In the Babylonian Era about 3000 B.C, encryption was used. In recent times the main reason for evolving the encryption techniques was military and political settings. But as the increase in data communication every day and widespread use of internet, demand and its implementation increased. When a new encryption algorithm evolved, then it is decrypted as well. After that again a new encryption algorithm created, this process repeats. Classical encryption: In Egypt about 3000 B.C, pictograms were used on a stele. Pictograms were

*Institute of Informatics and Communication, Cluster Innovation Centre, University of Delhi

impossible to decrypt but in the 19th century with the discovery and study on the Rosetta stone, made the decryption easy. In the scytale cipher a cylinder of particular dimension was used. In this technique basically a parchment strip was wrapped up around the diameter of cylinder. It was decrypted with the help of wrapping the parchment strip.

This method was basically related to the rearranging the sequences. After this method, a new encryption method i.e. Caesar cipher, was evolved in first century B.C. As it was most frequently used by the Julius Caesar, so it was named as Caesar cipher. In this method an each of letters in alphabet replaced by the letter located a set number of places further in alphabetical language. As in this process shifting of characters was involved, so sometimes it was referred as shifting cipher technique. An example is shown below:

Plaintext	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Encryption	SMKRATNGQJUDZLPVYOCWIBXFEH

As encryption technologies became progressively advanced based on the information attained and e orts made to decrypt traditional encryptions as well as the creation of new encryptions techniques, Cryptography became more common during the middle Ages. Due to increase in the diplomatic activities need of conveying personal information increased. It leads to the frequent use of encryption technique. As in case of Caesar cipher encryption, only one character is assigned for one alphabet. This weakness was lead to found Mary Queen guilty for conspiring to shoot Queen Elizabeth I. In the nomenclature cipher, codes were used to replace the phrased in addition to the alphabets. Nomenclature cipher is also known as cipher Mary. Basically the codes used in this Mary cipher were mentioned in the code book. It is used as key for the sender as well as receiver. It made the encryption technique for secure. As in case of nomenclature cipher code book was used to each cipher. It results in difficulties for receiving and providing a key. A new polyalphabetic substitution technique was evolved in the 15th century. In this technique two or more sets of encryption alphabets was used. It is known as Vigenere cipher. As shown in below if the key UNIVERSITYOFDE is used to encrypt DRSANJEEVSINGH, the letters in plaintext are referred to the characters listed across the top of the table where as key is referred to on the left side. So encrypted message is resulted by the intersection of the both letters i.e. one letter of the plaintext and corresponding letter of the key.

Goals There are the followings goals of cryptography i.e. Access Control, Confidentiality, Data integrity, Authentication, Non-repudiation, Availability.
Access Control basically control as well as provide limited the access to the system and application as well as virtual resources. In case of computation, users are granted privileges to the resources and systems i.e. a key card which provides access control and also grant the access to a particular area. But it is not much secure because the credentials can be stolen or may be transferred. In another secure method which uses authentication at two factors. First factor is that the person who want access, he or she must show credentials and another factor is the validation of identity or it can be any Personal Identification Number or may be biometric reading or access code.
Confidentiality necessitates that a cryptanalyst will be unable to recover plain text from obstructed cipher text (ZhongyunHua et al., 2015). There are certain measures which are necessary to disclose the sensitive information from unauthorized per-son. Online banking is

the good example to ensure confidentiality for an account number. Encryption of data is the good example to provide the confidentiality.

Data integrity deals with the illegal tampering of data. To tackle such type of problem, it is necessary to detect the manipulation of data i.e. deletion of data, substitution of data and insertion of data from unauthorized users.

Integrity basically involves the accuracy, consistency as well as reliability of data in complete life cycle. Steps should be taken in such a way which ensured that data cannot be altered by unauthorized people. Authentication provides the assurance to the receiver that data is authentic (Xiao Wei Li et al. , 2014).Communicating parties should identify each other. There are mainly three factors which ensure authentication. First one is password or personal identification number i.e. fingerprint, retina scan or may be another biometric measurement. Another factor consists of card or key which is used access control. Access control basically includes the authentication, authorization and audit of the entities which are trying to access.

Non-repudiation is basically a service which inhibits an entity from repudiating previous

Plaintext	DRSANJEEVSINGH
Key	UNIVERSITYOFDE
Encrypted Message	XEAVRAWMOQWSJL

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

pledges or activities(Ch.-H. Lin et al., 2013). Availability necessitates that computer system possessions should be accessible to authorized parties when needed.

1. Techniques

Cryptography plays vigorous role in preserving the message harmless when it is transmitted across anxious networks i.e. Internet in such a way that introducer could not read it. Cryptography protects both data and information from any internal as well as external attacks. Cryptography is widely categorized mainly into two types i.e. symmetric key encryption technique and asymmetric key encryption technique. Symmetric Key Cryptography: Symmetric key encryption techniquealso known as the secret-key, one key, private key, shared key and one-key encryption. In symmetric key cryptography only an exclusive single key is used at both sides for encryption or decryption the confidential information. The actual message is also called plain text. This plain text is encrypted with the help of sender as well as receiver using same key on the receiving end to get the original message. The authentic user could only retrieve the key for encryption as well as decryption. Instead of providing security communication, this technique basically having problem with the circulation of key because if any illegal person got the key, in that case whole data will be accessed without any trouble. There are numerous asymmetric key algorithms i.e. AES, RC2, RC4, RC6, Blowfish,Serpent,

Triple, etc.

2.1. Symmetric Encryption Techniques

Data Encryption Standard (DES): It is a symmetric block cipher. It has 64-bit block size that uses a 56-bit key. Plaintext of 64 bit block size is used for input as well as output using 64-bit block for cipher text. DES only functions on the blocks which are of same size. Substitution as well as permutation both operations are performed during execution. Same function is repeated for sixteen times to produce the cipher text. Security of data depends upon the operation performed number of times during cipher text generation.DES was replaced by Triple DES (3DES) because it has stronger method. It basically encrypts the data three times as well as uses different keys with key size of maximum 168 bits.it is comparatively slow in reference of new block cipher.

AES encryption: It is basically called as Advanced Encryption Standard. It is a symmetric key encryption technique which will replace the commonly used Data Encryption Standard (DES).It uses 128-bit blocks.The key lengths supported by cipher are basically 128, 192, and 256 bits. As the key sizes increases, the complexity of the cipher algorithm also increases.

Blow fish: it is also an encryption algorithm of symmetric type. It uses a block size of 64-bit and key length varies from 32 bits to 448 bits. It also uses sixteen round function and S-box which is key dependent. It produces a pseudo-random lookup tables for key scheduling with the help of encryption. This table generated based on the key provided by the user. This approach is better during differential and linear cryptanalysis. It is not applicable when there is a demand of memory space.

CAST: It is known as Carlisle Adams and Stafford Tavares. It is also a 64 bit block cipher.

CAST-128 is also like DES based Substitution-Permutation Network (SPN) cryptosystem.CAST-128 uses a key length of size between 40 to 128 bits.

IDEA: It is basically International Data Encryption Algorithm. It is also a symmetric encryption algorithm which was developed to substitute the DES standard. It uses a key of size 128 bits. It can tackle both differential and linear analysis.

RC2: It is a cipher which has variable-key-length.

RC4: It is also a variable-key-size stream cipher. It uses the key size up to 2048 bits (256 bytes). It is very fast in comparison to other others. Because the speed of RC4 is very fast so it is used in numerous applications. It is fundamentally a pseudo random generator and result is XORed with the stream of data. So it is significant that same key is not used for the encryption of different data streams.

RC6: it is also a symmetric key block cipher. It was designed to fulfill the requisite of AES.

SEED: It is a block cipher. It uses the 128 bits for key as well as for block. It basically uses S-boxes and XOR operation is performed and mixed with the modular addition.

Serpent: It is a very fast as well as secure block cipher. It is suitable for various combinations of keys.

TEA: It is a Tiny Encryption Algorithm. It is also very fast and more secure cipher. But it is having problem with the key scheduling because it is unable to provide more secure environment. It basically provides 16 to 32 rounds for encrypting the data but more number of rounds makes it very slow.

Triple DES: It is a adaptation of Data Encryption Standard. It consists of 56 key bits and 8 parity bits with the help of 64 bit key. Block size used by Triple DES is 8 bytes. It performed the encryption of data in 8 bytes chunks. The main reason behind Triple DES algorithm is to enhance the security level using three different keys. It is more secure in comparison to others but it is very slow.

2.2. Symmetric Encryption Techniques

Asymmetric Key Cryptography: Asymmetric Key Cryptography is also known as public key cryptography. In asymmetric key cryptographydifferent keys are used for both encryption as well as decryption. Basically these keys are mathematically related to each other. In asymmetric key cryptographic technique, if illegal person knows the single key in that case he

or she cannot get the original message because both keys will be needed to get the plaintext. The key used in encryption is known as public key and on the other hand key used for decryption is known as private key because it is kept secret. Both keys are generated in such a manner that no one can not generate the private key with the help of the public key. There are numerous asymmetric key algorithms i.e. Elliptic Curve DSA (ECDSA), Public-Key Cryptography Standards (PKCS), RSA, Key Exchange Algorithm (KEA), DiffieHellman, and Digital Signature Algorithm (DSA) etc.

RSA Asymmetric algorithm: it was developed by Rivest-Shamir-Adleman. It is the most frequently used public key algorithm or asymmetric algorithm. It is uses for different purposes i.e. encryption of data as well as in digital signatures.

Factoring of numbers is considered as equivalent to security provided by RSA but it is still question of debate. Computation performed in RSA with integers modulo n = p * q where p, q are two large secret primes numbers. In this approach encryption is performed by exponentiated of message m with a small public exponent e. On the other hand decryption is performed with the ciphertext c = me (mod n) which computes the multiplicative reverse d = e-1 (mod (p-1)*(q-1)). After that cd is obtained by cd = m e * d = m (mod n). The private key includes the n, p, q, e, d and on the other hand public key contains only n and e. To enhance the security level key size should be greater than 1024 bits.

Diffie-Hellman: It is the first asymmetric encryption algorithm which uses discrete logarithms in a limited field. It allows two different users to share a secret key over a unconfident medium irrespective of the earlier secrets. It is commonly algorithm for the exchange of keys. In various cryptography protocols, two or more parties try to start communication. On the other hand it is assumed that at the beginning they do not have any mutual secrecy. So they cannot use secret it. Diffie-Hellman protocol uses the key exchange by consenting for the construction of the common secret key over an insecure communication media. In case of mathematical group Diffie-Hellman protocol is considered as more secured. But we cannot make hardware model.

Digital Signature Algorithm: It is a mathematical system which is used to validate the authenticity and consistency of a message, software or digital document. It is not as efficient as RSA for signature authentication.

ElGamal: It is a public key cipher i.e. an asymmetric key encryption algorithm is used for public-key cryptography which is based on the Diffie-Hellman key agreement. ElGamal is the precursor of DSA.

ECDSA: It is Elliptic Curve DSA. It is basically a variant of the Digital Signature Algorithm (DSA) which works on elliptic curve groups. The size of Public key inn case of ECDSA is twice the size of security level used in Elliptical curve cryptography.

XTR: It is also the asymmetric encryption technique. It is basically an innovative way which uses the traces to represent as well as calculate the powers of various elements of a subgroup in a finite field. Security of XTR based on the exertion of the discrete logarithm. Fast key generation, small key size and speed are the few advantages in XTR.

2.3. Steganography Techniques

The Greek word steganos meaning covered writing is basically the concept be-hind the theory of steganography. Here it is di cult to even detect that a message is being sent. This type of ciphering called steganography. Steganography is the method of inserting concealed messages just like that unauthorized person, except the sender and anticipated receivers can detect the presence of the messages. Theprime objective of steganography is to conceal the secret message or information just like that spysare not able to detect it (Leo Yu Zhang et al.,2014). If spys inaugurate any doubtful data in that case aim is consequented. There are numerous types of data in steganography i.e. text and message, audio and video etc.

There are three components in the basic model of steganography (Yang Liu et al., 2013): The Carrier image: it is also known as the cover object which will convey the message that is to be

concealed. The Message: it could be various types i.e. image, video, file, audio etc.
The Key: it is basically used to get the original message bydecoding/deciphering/discovering the hidden message. There are various types of Steganography i.e. Image Steganography, Audio Steganography, Video Steganography, Text,files Steganography (SukalyanSoma et al., 2013):

a. Image Steganography: In image steganography, data is concealed inside an image in such a way that original image remains the same. The common image steganography algorithm is LSB based embedding algorithm.
b. Audio Steganography: In the audio steganography secret data orinformation is hided in an audio, so it is known as audio steganography. There are several ways to hide secret information in audio i.e. LSB, Phase coding etc.
c. Video Steganography: In video steganography method secret data or information is hided in a video, so it is known as video steganography. As we know that video consists of both i.e. image as well as audio. So we can say that video steganography can be used for both image as well as audio.
d. Text les Steganography: In Text les based steganography method secret data or information is hided in a text, so it is known as text les steganography. It basically requires less space or memory because it only stores secret data or information in the form of text. It is faster than other steganography technique. But this technique is rarely used because text les contains large amount of redundant data (SukalyanSoma et al., 2013).
e. Least Significant Bit (LSB): It is basically the most common technique used for concealing the secret data or information in any digital media i.e. image, video, audio or may be text. In this technique LSB or last bit of image is replaced by the bit of secret message (GuominZhoua et al.,2014). So data can be hide with the use of 8 bit or 24 bit image. Generally an image having 24 bit size used for hiding large amount of data. As LSB is commonly used but still it is vulnerable because it can be detected during the transmission of data. There are various techniques are evolved i.e. Enhanced LSB, Edge LSB and Random LSB (GuominZhoua et al.,2014).
f. Bitmap Steganography: It is basically of two types i.e. Lossy compression and Lossless Compression.

Lossy compression technique is not reliable because it does not provide the guarantee to preserve data. Lossless compression technique gives the guarantee even after all the operation performed by the user. But lossy compression technique widely used inspite of degrading the quality of image during restoration(Qiang Zhang andXiaopeng Wei, 2013).

As BMP les provides lossless compression so it is commonly used. These BMP images basically created using pixels and these pixels are compared with RGB i.e. Red, Blue, Green. These colors are the primary colors and any color can be formed using these colors. One byte is created from 8 bits and first bit is called MSB (most significant bit) and least significant bit is called LSB.

Rao et al. basically proposed a method; using combination of both Steganography and cryptography to conceal the undisclosed data in an image. Firstly secret information is embedded in an image by using the Least Significant Bit (LSB) technique. Then this embedded image was encrypted. Finally this encrypted image is decrypted and data is retrieved with the secret key (Guoyan Liu et al. 2014).

Nivedhitha et al. introduce a technique to embed the secret image into cover image with the help of LSB technique and then encrypted the information using DES algorithm and used the key image.

Wai et al. basically presented three steganography techniques. RC4 encryption technique is used and then encrypted information is embedded in BMP image le with the help of three steganography methods (Miao Zhang and Xiaojun Tong, 2014).

2.4. Transform Based Encryption Techniques

Muhammad, discussed a new color image encryption technique i.e. asymmetric single-channel based, with the help of using Hartley transform and gyrator trans-form. In this approach basically color image is isolated into Red, Green and Blue channels after that Hartley transformation is performed each of them independently. After this all the three transformed channels are multiplied. To obtain the first encryption and decryption key phase and amplitude truncation takes place. With the conjugation of random phase mask, encoded image is modulated. Then this modulated image is gyrated transformed and after that phase and amplitude truncated to get the second encrypted image and second decryption key (AtiehBakhshandeh and ZibaEslami, 2013)

Tao et.al, discussed the cascaded fractional Fourier transform for a multiple-image cryptosystem. First of all original images basically separated into two phase masks during the encryption process. Few masks are modulated into the interim mask then these are encrypted into ciphertext image and on the other hand remaining masks are used as encryption keys. During the truncation phase, asymmetric system can be used to produce ciphertext. Only an authorized user can retrieved the data with the help of the different phase masks. So this technique has high resistance for various types of attacks including chosen plaintext attack (SimYingOng et al., 2015).

Hang et.al, discussed affine transform in the gyrator transform to propose a new color image encryption. With the help of affine transform, RGB components of the color images were converted into real as well as imaginary parts. After that complex function was encoded as well as transformed in gyrator transformdomain. To enhance the security level, gyrator transform was transformed twice. Parameters used in a ne and gyrator transform basically used as keys (HongjunLiua et al , 2013).

Lei et.al, discussed iterative random phase encoding and amplitude-phase hybrid encoding in FrFT (fractional Fourier transform) domain for the double image encryption. As in case of iterative random phase encoding scheme, to encode two original images to a single complex-valued image a binary random marix is defined after that it is converted into stationary white noise image with the help of fractional Fourier transform. With the help of correct keys as well as initial conditions of chaotic system, the original image can be easily retrieved. Noise interference, high security levels and robustness against dataloss are basically achieved by it (Qu Wang, Qing Guo and Liang Lei, 2013).

Lei et.al, discussed multistage random phase encoding in GT (gyrator trans-form) and amplitudephase mixed encoding for a new double image encryption technique. To mixed encode two primitive images to a single complex-valued image a random binary distribution matrix is defined in the amplitude and phase mixed encoding operation, after that with the help of the multistage phase encoding with gyrator transform is used to encrypt the stationary white noise distribution. Correct keys with applying initial condition of chaotic system, basically used to retrieved the ciphered image. This technique basically results in the robustness in noise disturbance as well against data loss and higher security level (Liansheng Sui, KuaikuaiDuan and Junli Liang, 2015)).

Liang et.al, a novel discrete fractional transform basically defined by the various parameters i.e. vector, periodicity, fractional order. It is basically called as discrete multiple-parameter fractional angular transform. The proposed double-image encryption scheme is based on the transform and two coupled logistic map. First of all two plaintext images sequentially connected as well scrambled by the chaotic permutation process to obtain enlarge image. In the permutation process basically sequences of chaotic pairs generated with the two-coupled logistic map. After that this scrambled image basically decomposed into the two new components. After this operation, a logistic map is generated based on the chaotic random phase mask and one of these two components basically converted into the modulated phase mask. With the help of modulated phase mask, another component is encoded into the interim

matrix. Finally ciphertext with stationary white noise distribution is obtained by the two-dimensional discrete multiple-parameter fractional angular transform. This fractional angular transform basically perform the operation based on the interim matrix. Hence in this approach no phase keys are used for the encryption and decryption process, it results in better key management (Liansheng Sui et al., 2015).

PAN et.al, discussed a new double image encryption and discrete fractional random transform by combining compressive sensing with discrete fractional random transform. With the help of a two-dimensional sine Logistic modulation map,two random circular matrices and the measurement matrix utilized in compressive sensing are constructed. These two images can be encrypted with the compressed sensing as well as connected into one image. After the encryption operation, the original image can be retrieved with the help of discrete Fourier transform and Arnold transforms (Nanrun Zhou et al. , 2015).

Naveen et.al, discussed a JTC (joint transform correlator) architecture which uses phase and amplitude truncation technique for a new optical cryptosystem. But phase and amplitude truncation results in the asymmetric and it make the hybrid attack i.e. amalgamation of precise attack on asymmetric cryptosystem and chosen-plaintext attack on joint transform correlator, very di cult. With the help of correlation geometry, authentication and verification carried out (A. Akhavan, A. Samsudin and A. Akhshani, 2015).

Zhao et.al, with the help of chaos-based local pixel scrambling technique and gyrator transform, a new double-image encryption algorithm is proposed. These two images are basically complex function. To scramble the pixels at local area, Arnold transform is used. Standard map and logistic maps are used to generate the position of scramble area and android transform frequency respectively. After that complex function is converted with the help of gyrator transform. Gyrator transform and pixel scrambling used as the key for encryption (Nanrun Zhou et al. , 2015).

Wang et.al, logistic maps and discrete fractional random transform based encryption scheme proposed for double image encryption. Pixel position of an enlarged image i.e. composite two plaintext, are relocated after that with the help of chaotic confusion diffusion process intensity values are changed. After that Two scrambled plaintext can be recovered from the enlarged image. These are basically encoded into the amplitude and phase part of the complex function. With the help of discrete fractional random transform i.e. logistic map are used to encrypt with white noise distribution (Ensherah A. Naeema et al., 2014).

2.5. Chaotic Based Encryption Technique

Leo Yu Zhang et.al, discussed about the chaotic image encryption. The per-mutation and diffusion structure is employed by the several round based chaotic image encryption techniques. It becomes unconfidently when the value of iteration round is one and in this case it can be easily recovered. As he further discussed that to repel the known attacks a feedback mechanism based on some temp value i.e. for gray image a single round permutation-diffusion chaotic cipher. Unambiguously, for the development of the several permutation sequences for several plain images firstly plaintext feedback technique is embedded in the permutation process after that secret key generated dynamically by employing plaintext or ciphertext feedback for diffusion. This approach possesses large key space and it can repel the differential attack (Leo Yu Zhang et al.,2014).

Xing Yuan Wang et.al, discussed allied chaos and assorted bit permutation for the encryption of color image. Assorted bit permutation technique is applied todiminish the computing cost as well as improvement in the permutation efficiency by consideration of the difference i.e. information amount among bit planes. After that to obtain the ciphered color image XOR operation is performed for R, G, B components of color images, thus obtains cipher color images. This process basically generates the pseudo random sequences throughout the

complete encryption process (Xingyuan Wang,and Hui-li Zhang , 2015).

Yang Liu et.al, discussed a new image encryption algorithm which is based on the complex number in chaotic maps. In this approach a number of maps were constructed and then it was proved chaotic in the complex number field after that its characteristics were analyzed. To design a pseudorandom key stream sequence, two maps were choosing among various chaotic maps. In this technique, two entropy coding methods and plain image data were scrambled as well as di used with the help of pseudorandom key stream sequences. It basically results in reduction of the correlation among signals (Yang Liu, Xiaojun Tong and ShichengHu ,2013).

Jun-xin Chen et.al, discussed the demand of real time secure image encryption i.e. chaos based image encryption. Mostly are related to the architecture based upon permutation diffusion. Basically these are independent control parameters. But it contains two weaknesses i.e. according to first one, to encrypt one plain pixel atleast two variables based on chaotic state are required in permutation as well as diffusion process. It produces high computation complexity. According to the second approach generated key stream basically depends upon the secret key, it makes the system vulnerable against plaintext attacks.Chen further discussed how to tackle with this weakness with the help of a fast chaos based image encryption technique using a dynamic state variable mechanism to enhance security as well as efficiency .

ZhongyunHua et.al, discussed the approach i.e. 2D-SLMM (two-dimensional Sine Logistic modulation map) that was derived from the sine and logistic maps. When it was compared with the chaotic maps that are already existed, then it pro-vides better ergodicity, broader chaotic range, hyper chaotic property and lower implementation cost in comparisons to others. A CMT (chaotic magic transformation) technique was proposed to change the pixel position of image efficiently. After that both 2D SLMM and CMT was combined to develop a novel image encryption algorithm. It not only protects the images with lower time complexity as well as higher security levels but also revel various types of attacks .

Xiao Wei Li et.al, discussed an approach with the help of CAT (cellular automata transform) and computer generated integral imaging to introduce a unique three dimensional (3D) image encryption approach. In this approach basically light rays coming from the 3D image digitally recorded the two dimensional (2D) elemental image arrays (EIA). After that 3D image is mapped based on ray tracing through with the help of virtual pinhole array. After that with the help of 2D CATscrambling transform for the 2D EIA, encrypted image is generated. Computational integral imaging reconstruction (CIIR) technique is used to reconstruct the image and at the output plane depth dependent plane images are reconstructed .

Lin et.al discussed a new encryption approach which is based on the changing random greeds that is suitable with color images, batch binary and gray level. In this approach m images are encoded into m+1 total random grid. On the other hand human visual system is used to decrypt it. This method provides an advantage because it neither uses pixel expansion nor basis matrix for encoding .

GuoshengGu et.al discussed a chaotic 3D cat map method to encrypt an image. In this method several operations performed simultaneously i.e. permutation of pixel location and values of pixels were substituted at every iterative step of chaotic map. It reduces the forward and reverse making operation into a diagonal of pixel images. To eliminate unwanted finite precision a perturbation is introduced. So it provides simplicity and efficiency. It basically creates a large key space as well as revel the attacks based on cipher .

Manish Kumar et.al, discussed a technique for encryption and decryption for an RGB image with the help of random matrix in two stages which are affined with the discrete wavelet transformation. In this approach RMAC parameters are mandatory for encoding and decoding of images. A new formula also used for all the conceivable range to select keys for encryption as well as decryption an RGB image. This technique can also be used for the transfer of data

related to images securely and efficiently .

Yicong Zhou et.al, discussed a technique for a chaotic system with the help of the combination of the two one dimension (1D) chaotic map techniques that are already existed. It is simple and more effective system. With the help of this approach several 1D chaotic maps with wider ranges are produced and then their behavior was compared with their chaotic or seeds map. It provides the better result. According to the novel approach for image encryption, with the same set of security keys, it basically generates entirely diverse encrypted image every time when new algorithm is applied to the original image .

Ahmed et.al, discussed Quantum chaotic system based a novel color image encryption scheme. First of all, Y (Luminance) component of low frequency sub band are scrambled in integer wavelet transform which is based upon the total automorphism. Horizontally as well as vertically adjacent pixels are mixed with the help of adopted quantum chaotic map and two different types of modules are generated. After that an intermediate chaotic key stream image is generated to accomplish the substitution with the help of quantum chaotic system .

Zhang et.al, discussed the various encryption image techniques for differentformats of image i.e. JPEG (Joint Photographic Experts Group), GIF (Graphics Interchange Format), PNG (Portable Network Graphics), and TIFF (Tagged Image File Format). According to Devaney's theory, a cross chaotic map technique was proposed and blocks are divided dynamically of the 3D baker. Cross chaotic map are also used in the encryption for the diffusion and permutation. In this method images le structure and syntax are not destructed .

Radu et.al discussed a novel approach i.e. hyperchaotic map which was generated from parametric equations of serpentine curve. With the help of classic bi-modular architecture a new encryption scheme used in Hyperchaotic map, in this scheme basically pixels of plain image are shuffled by a random permutation generated with a new algorithm as well as a confusion state i.e. XOR is used to modify the pixels .

Zhang et.al discussed the spatiotemporal non adjacent coupled map lattice to develop a new image encryption algorithm. It is having supplementary cryptography features in dynamics as compare to the logistic or coupled map. In this technique for image encryption a bit pixel permutation approach enables the bit plane of pixels without any additional storage space. It results in more security and high efficiency of the proposed algorithm .

Francois et.al, discussed a new encryption approach for image with the combination of chaotic function and XOR operator. This approach not only provide large key space to revel the brute force attacks but also encrypted images securely with any entropy structure which ensure i.e. indistinguishability, diffusion and con-fusion properties in the cipher images. This approach is efficient and secure as randomness, correlation and sensitivity are analyzed .

Chen et.al, discussed an approach for to encrypt the optical image which is based on the vector composition and multi-beam interference. During the encryption process image is encoded into n-1 phase and generated masks are regarded as the keys for the encryption system and on the other hand cipher text based on the multibeams interference and vector composition. During the decryption procedure phase only masked with n beams of parallel incident and original image is obtained after Fourier transform. For further enhancing the security levels keys can be used separately .

Soma et.al, discussed chaos based Gray scale image encryption scheme is used for a non-adaptive partial encryption. Speed and time is the main factor for this approach. In this approach grayscale image is decomposed into corresponding eight bit planes after that encrypted data is coupled with the help of pseudorandom binary generator (PRBNG). The first four bits are encrypted with the help of the encrypted keys which are obtained during recurrence relation based on PRBNG. After that four insignificant bits are combined with the significant bit planes to obtain the finally ciphered image .

Rasul et.al, discussed a new technique which is based on hybrid model of DNA (Deoxyribonucleic acid), chaotic map and CA (Cellular automata). To encrypt the pixels of plain image CA rules and DNA sequence XOR operator are used simultaneously. Two

dimensional chaotic maps are used to find the rule number in CA as well as DNA. This techniques revels various attacks .

Wang et.al, discussed Dynamic random growth and hybrid chaotic maps based hybrid approach for a new block image encryption. Drawback of cat map that it can be easily cracked because of periodicity and attacker can easily choose plaintext. But if cat map is used in another way then cyclical phenomenon can be easily eliminated and repel the attack based on chosen plaintext. During the diffusion process, based on the image block an intermediate parameter can be easily calculated. To generate the random data, intermediate parameter is basically used as initial parameter. In this process, plaintext is responsible for the generation of key stream which repel the chosen plaintext .

Wang et.al, discussed a hybrid approach for image encryption which is based on chaotic system and deoxyribonucleic acid (DNA). First of all bitwise XOR operation is performed based on the pixels of the plain by pseudorandom sequence generated by chaos system i.e. coupled map lattice (CML). After that with the help of DNA encoding procedure image is encoded to obtain a DNA matrix. After that DNA matrix based initial conditions are generated for CML. And then rows as well as columns of DNA matrix are basically permuted. It creates the confusion. Then finally based on the DNA decoding procedure confused matrix is decoded .

Qiang et.al, discussed also the hybrid approach based on DNA subsequence and chaotic system. It basically uses the concept of subsequence operations of DNA rather than complex biological operations (i.e. deletion, elongation and truncation). After that addition operation based on DNA using Chen's hyper chaotic map is performed in the cipher image .

Guomin et.al, discussed a skew tent map based symmetrical approach to encrypt the image. It uses the line map based approach because it is applicable for any size of image for the encryption. R, G, B components are encrypted at bit level and operation are performed at the same time to disturb the correlations. It does not need any sub block complex processing so it can be implemented parallel. It is more secure .

Wang et.al, discussed improved gravity model and chaotic system based image encryption technique. First of all two chaotic sequences are generated based on logistic map to shuffle the original image. After that using improved Gravity model this shuffled image is di used. Finally to enhance the encrypted image with the help of changing one pixel on the plain image, chaotic system again di used.

Xing et.al, discussed a new approach which is based on RCA (reversible cellularautomata) combining chaos. In this basically periodic boundary reversible cellular automata and an intertwining logistic map are used. In this 4 bits represent the each pixel of image. After that pseudorandom key stream is generated with the help of intertwining logistic map to permute these units in the confusion state so that introducer cannot detect it. To iterate many rounds for achieving the diffusion in bit level, two dimensional reversible cellular automata i.e. discrete dynamically system is applied. Hence we only consider higher 4 bits because these higher bits transfer all information mostly.

Yushu et.al discussed a novel cryptosystem by combination of time varying de-lay and coupled map lattices. This approach basically overcome the drawbacks in the previous methods based on the permutation diffusion architecture because the addition of pixel values of the original image basically used for the determination of the parameters of permutations and on the other hand cipher image used previously can be utilized in case of diffusion for the next time. So it is more efficient, reliable, practicable and secured communication.

Zhang et. al, presented a novel crypto system i.e. delay in the variation of time and coupled map system as well as a new image encryption algorithm having permutation diffusion architecture which overcome drawbacks in the existing methods, because the combinations of pixel value of original image is basically used for determination of the permutation parameters and on the other hand previous cipher image information is employed in the next diffusion. It

results in proficient, feasible, and consistent, with high potential to be adopted for secure communications and network security.

Zhu et. al, discussed the hyper-chaos because it has more complex dynamic characteristics. So it results in more secure image encryption scheme. So based on it, a new image encryption scheme proposed by integrating with compression. In this scheme basically first of all 2D hyper-chaos discrete nonlinear dynamic system used for shuffling the plain image after that Chinese reminder theorem basically used for diffusion and compression the shuffled the plain image concurrently. It also can be used for changing the plain image information significantly as well as plain image can be compressed with compressed ratio k, which is considered as most critical in case of the transmission of multimedia.

Qiang et.al, presented a hyper-chaotic system for a new image fusion encryption algorithm. It is based on the DNA sequence operation and image fusion. Firstly key image and original images are encoded to obtain the two DNA sequence matrices. After this chaotic sequences which was generated by hyper chaotic, basically used to maps and scramble the locations of the elements by DNA sequence matrix i.e. generated by the original image. After that by using DNA sequence, XOR operation is scrambled with DNA matrix and random DNA matrix. Finally encrypted image is obtained by decoding the sequence matrix. It resists thestatistical as well as exhaustive attack .

Mohamed discussed an image encryption algorithm which is based on one dimensional cellular automata. As for the same image encryption and decryption operations can be performed using multiple process parallel, so it is fully parallelizable. With the help of RCA based construction of an extended pseudorandom permutation parallelization is made possible because it takes a nonce as a supplementary parameter. To certify the perfect cryptographic security properties, PRP exploits the behavior of chaotic and the higher sensitivity initially for the RCA .

Campo et.al, as to ensure the confidentiality when the information is transferred over insecure networks, color image encryption plays an important role. Basically a new color image encryption algorithm was developed which is based on the plain image characteristics (to revel attacks based on plaintext) and optimized distribution of 1D logistic map which is based on Murillo-Escobar's algorithm. It results in RGB image encryption is very fast as well as more secure in case of different known attacks. It can also be applied in real time applications i.e. it needs high security levels .

Zhang et.al, discussed a novel image encryption algorithm which is based upon the spatiotemporal chaos for the mixed linearnonlinear coupled map lattices. If a comparison is made between logistic map and spatiotemporal chaotic system, it provides more outstanding features dynamically. In this approach bit level permutation basically enables the lower and higher bit planes of pixels permute mutually without any extra storage space. It provides the high efficiency and superior security .

Yuling et.al, discussed chaos based lightweight image encryption approach. This encryption technique is performed in transformed domain. With the help of IWT (Integer Wavelet Transform) original image is decomposed into the detail components and its approximation. After that diffusion of the approximation coefficient is performed with the help of the secret keys i.e. usually generated by spatiotemporal chaotic system as well as followed by the inverse IWT to construct the di used image. After that in order to reduce the correlation among contiguous pixels, plain permutation is performed for diffusion mage with the help of the logistic mapping. It is more robust and secure mechanism .

RasulEnayatifar et.al, discussed first of all a specified number of chaotic images created using chaotic map. WDICA approach was applied to improve security levels. The main functions of WDICA are correlation coefficient and entropy. The main goal is this approach is to minimize correlation coefficients and maximize the entropy. With the help of WDICA, optimization of all iteration values are performed, this is the main advantage of it. Hence it results in excellent

encryption technique .

Atieh et.al, discussed a novel approach for image encryption which is based upon the chaotic maps, permutation diffusion architecture and cellular automata. To confuse the plain image a piecewise linear chaotic map is utilized in permutation phase. To obtain a secure and efficient cryptosystem, a reversible memory cellular automata as well as Logistic map are employed. The main advantage of the proposed method i.e.affluence of implementation, secured diffusion mechanism and computation efficiency. It can also detect the authenticity of the image i.e. tampered or not during transmission. It is very much important during transfer of sensitive information .

Osama et.al, discussed the transparent encryption technique for current spatial data protection methods, after that a proficient model was proposed for encryption and decryption i.e. digital image les stored in hard disk. Transformation method basically intended to shuffling the block of images as well as for the decrement of correlation, it basically reduces the perceivable information for the other parts of encryption. Hence an adequate level of security with a reasonable computational complexity can be achieved .

Ghebleh et.al, discussed a new image encryption approach i.e. chaos based for encryption applications in medical. In this approach multiple rounds are performed for the encryption and in each round two phases are performed i.e. a masking phase a shuffling phases. These phases are block based. To mask and shuffle an input image chaotic cat maps are used. A pseudorandom matrix having the same size as input image is used during masking phase. It basically improves the speed of the operation. According to the outputs of some chaotic maps, blocks of this pseudorandom matrix are permuted in each round of the shuffling phase. Mixing basically take places between blocks of images in order to avoid the attacks i.e. differential attacks.

Chen et.al, discussed a new image encryption scheme based on Gray code permutation. This technique basically takes full advantage of (n, p, k)-Gray-code achievements. It provides the higher efficiency. To compose the cryptosystem comprehensively, a plaintext based image diffusion scheme is used. It results in higher efficiency as well as higher security.

Xiaoling et.al, discussed chaotic based image encryption technique for an efficient self-adaptive model. A proficient and fast encryption algorithm is proposed with the help of the double simple two-dimensional chaotic systems and classical structure of permutation-diffusion. It different among all the existed systems, here generated key stream are dependent on the plaintext in both the operations. For different plain images, different key streams are generated i.e. only one bit is changed in the plain image. Operation speed of it is high because it avoids the mathematical methods i.e. high dimensional partial differential equations. It revel the chosen and known plaintext attacks and also provides good efficiency andsecurity as well
.

Ghebleh et.al, discussed chaotic maps based a robust shufflingmasking image encryption technique. A 3-dimensional chaotic cat map coupled with a zigzag scanning technique for shuffling the phase permutation square blocks of bytes. Scrambling of the byte blocks of the shuffled image is done with combined outputs of three one dimensional chaotic skew tent maps after the completion of masking phase. It is performed in such a way that each and every block is influenced by the all previous masked blocks. It basically generates the ciphered image which exhibits the followings i.e. at histograms, random behavior, no adjacent correlation of pixels and entropy basically close to the original value. It results in higher sensitivity to the secret key, larger key space and robustness against the differential attacks. It is more secure and more reliable .

Chun et.al, proposed a new approach for image encryption which is based on chaotic map with mechanism of permutation diffusion. Diffusion based on the encryption took place between plain images and its pixel i.e. generated by the bitwise XOR operation. Finally to di

use the shuffled image, the constructed spatiotemporal chaotic sequence is employed. Encryption technique is high key sensitive and also having the large key space. It revel the statistical attack, differential attack, known-plaintext attack, chosen-plaintext attack, entropy attack and brute-force attack.

Yang et.al, discussed an image encryption technique which is having a pixel level diffusion and bit level permutation technique. In case of bit level permutation each pixel is divided into 8 bits and the resultant bit is arranged based on Arnold map in rows as well as column direction. It results in a significant diffusion for bit level permutation. To change the histogram distribution and gray value of the permutated image affine cipher is applied in pixel level diffusion process.

Zhang et.al, discussed that it is worldwide accepted that higher bit planes carry more information rather than lower bit planes in case of cryptosystems which are bit level image. Enhanced encryption basically took place in higher bit planes in comparison to lower bit planes. All the achievement in bit level basically is existed for standard images not for any special images i.e. medical images. Because in these case ciphered images can leak the information of lower bits. In this technique first of all incapability of existing scenarios are given and after that swapping and inter pixel computing permutation approach is used. It results in higher security levels .

Reddy et.al, discussed the why the need of encryption and decryption to secure images from various types of attacks. With the combination of chaotic images, a new diffusion method was proposed for RGB image encryption and decryption. This algorithm was formulated for the complete range to select keys for encryption as well as decryption of RGB image. Two standard examples were considered toanalyze the approach. Following analysis were performed i.e. PSNR, MSE, key sensitivity, NPCR, UACI, key space. It results in higher security level .

Chen et.al, firstly discussed gyrator transformed and pixel scrambling techniques for double image encryption. But it lacks in phase based image during noise perturbation attack. It results in serious deterioration in retrieved phase based image. So details analysis basically performed for cross-talk disturbance in original scheme and possible improvement was proposed. It results in enhance security of the original cryptosystem .

Liu et.al, proposed a asymmetric color image encryption technique which is based on a chaos based. Based on key changing mechanism different receivers got different keys. To produce two initial values of the Henon map and to generate two pseudo random sequences basically hash value of plain image is applied. First of all six pseudo random arrays are generated to shift component of red, blue and green circularly with the help of rows and column after that diffusion of three color components took place by XOR operation. During the decryption process i.e. control parameters of Henon map, the iteration times, two initial values of Henon map and the iteration number m-n+1 basically served as keys. It results in feasibility and effectiveness for asymmetric cryptosystem in case of color image encryption.

Liang et.al, discussed an asymmetric technique based multiple image encryption technique. First of all each and every plain image basically scrambled which is based upon the sequence of chaotic pair generation with the help of a system having symmetric coupled identical logistic blocks. After that phase only function of the scrambled image is retrieved with the help of phase retrieval process in case of the fractional Fourier transform domain. After that phase function which are modulated are encrypted into the cipher text with stationary white noise distribution by using chaotic and fractional Fourier transform diffusion. To retrieve the phase-only functions of plain images three random phase functions are used. In the process of encryption, three decryption keys are generated. This process makes the system more secure. To check the quality of decrypted image, peak signal to noise ratio is evaluated which results in enhancement of the encryption capacity.

Tanaka et.al, discussed the encryption method based on format complaint with the data embedding feature for JPEG compressed image. First of all encoding of DC coefficient take place with the help of the textural information carried by AC coefficients. After that scanning of ac coefficient takes place in eight different orders which results in small bit stream size. After that extraction of block from AC coefficient is performed as well as manipulated to increase the scope of permutation. After that to embed the external information, virtual queue are decomposed.

Tao et.al, discussed hyper-chaotic system and DNA system process based on new image fusion encryption algorithm. But this approach can be wrecked with the help of 4mn/3 +1 choosing plain image where mn is the size of the plain-image. In this research paper security of the encryption technique basically re-evaluated and it is also find that this encryption technique can be wrecked even less than [log2 (4mn)/2] +1 .

Niud et.al, discussed a color image encryption technique which is based on chaos with the help of bijection method. In this process basically complete image is basically di used with the help of XOR operation for different random rounds. After that each and every component of color is discrete into the blocks having same size. With the help of Chen system an 88 S-box is generated. After the substitution of each block with S-box, the ciphered image can be obtained .

Liu et.al, discussed color pathological image encryption algorithm which is basically enhanced chaos based with the help of SHA-2 i.e. for the generation of one-time keys. The hash value of the random number and plain basically used to create one-time initial conditions for Chebyshev maps. It helps in sending different ciphered images for the different recipients. It also changes the key stream in each and every confusion process by keeping same initial values. In this approach hash value of the prior block is XORed with the each block. Basically permuted image is divided into block of 256 bit. This approach is very robust against the common attacks .

Abdul et.al, discussed the hybrid model for image encryption, it contains basically DNA (deoxyribonucleic acid) masking, GA (Genetic algorithm) and logistic map. The number of initial DNA masks is created with the help of DNA and logistic map functions after that Genetic algorithm is used to choose the best mask for the encryption. It basically improved the DNA masks quality which is harmonious with the plain images. It results in excellent encryption as well as revel the classic attacks .

Zhang et.al, discussed the jpeg image based encryption and decryption. Analysis and comparison is taken place for encryption and decryption. As well as JPEG image chaotic encryption security techniques is discussed for the two different schemes. Encryption and decryption is not only fast but also match with JPEG format for the 88 data block. JPEG image is used in most of the common applications because it fulfills the criteria for the storage as well as transmission. It also provides the feasible and operative solution in case of JPEG images .

Wang et.al, proposed spatiotemporal chaotic system based image encryption algorithm. To increase the security level key stream buffer and a circular S-box are used. This encryption algorithm basically consists of basically diffusion as well as substitution process. In case of the substitution process, S-box basically contains the head pointer with the circular sequence. According to the pixel valueand head pointer, each image pixel is replaced with S-box. The value of head pointer varies with respect to the substituted pixel. On the other hand, in case of diffusion process, random numbers which are generated by the chaotic system are cached by key stream buffer. With the help of key stream buffer a random number is chosen and to encrypt the each image pixel, it is enciphered by incorporation of the previous cipher pixel. It is more secure and more efficient for real image encryption .

Lang, discussed a new color based image encryption technique with the help of the following

operations in CB (Color Blend) and CP (Chaos Permutation) by using RPMPFRFT (reality-preserving multiple-parameter fractional Fourier transform) domain. Original image first of all exchanged and mixed from RGB (Red, Green and Blue) color space to new (RGB) by rotating the color cube with a random angle matrix. After this reality-preserving multiple-parameter fractional Fourier transform is basically used for modifying the pixel values. All the three components of scrambled RGB color space are converted with the help of three different pairs. To enhance the security, former steps output basically scrambled. This technique is more secure as well as feasible .

Wei et.al, discussed a novel encryption confusion scheme which is based on the paired inter permuting planes. To replace the classical confusion operations an exchange and random access strategy is employed. Efficiency was analyzed based on the histogram distribution, entropy analysis, ability to revel differential attacks and ability to revel differential attacks.

Kadir et.al, a hybrid image encryption scheme was proposed based on the hyper chaotic system and CFI (Choquet fuzzy integral). The encryption algorithm is based on the pseudo-random number generator based CFI. First of all PWLCM (piecewise linear chaotic map) based 128 bit keys generated. To generate the initial parameters of the Choquet fuzzy integral, Lorenz system is iterated for limited times. For confusion and diffusion of three components of pixels, CFI based output is used. It results in good encryption and larger key space as well revels the common attacks .

Dong, with the help of one time based coupled chaotic system, a novel algorithm was developed. Key and plaintext sensitivity is contained by the key stream. In each and every encryption process, SHA-3(The Secure Hash Algorithm-3) is used to combine with the initial keys i.e. to make the key stream change, to generate the new keys. First of all six initial values of the chaotic systems are generated by applying SHA-3 hash value of the plain image. After that six state variables are permuted and combined, out of six only three variables are randomly selected to encrypt the red, green and blue components. This approach is reliable as well as provides the secure communication .

Zhang, if any image encryption schemes which have cipher code stream whichis controlled by the secret key, but plaintext is same. Then it results in vulnerable system. As in case of an image encryption scheme using Choquet fuzzy integral and hyper chaotic Lorenz system, pseudorandom cipher code generation method is cryptanalyzed .

Kuma et.al, discussion of previous encryption scheme i.e. Diffusionsubstitution based gray image encryption scheme, which is not secure and secret can be deducted with the help of chosen plaintext .

Rong et.al, discussed a novel image encryption method which combines compressive sensing (CS) with quadrature phase-shifting digital holography. First of all image is encrypted with axis quadrature phase holograms using two random phase masks. With the help of single pixel compressive holographic imaging, the two encrypted images are highly compressed in a one dimensional. With the help of optimization problem solution, encrypted images easily reconstructed. The original image only reconstructed with the help of the two holograms and correct keys .

Jeng et.al, discussed, in all image encryption techniques which are based on chaos, basically depends upon the diffusion and permutation. In this paper Jeng basically point out the problem i.e. low security sensitivity as well as plain image changes, in chaos and hyper-chaos based image encryption. Hence security only relies on diffusion operation. It also entails the level of security is degraded potentially. So a hyper chaos based image encryption scheme basically proposed which fixes all the weakness .

Zhang, DNA sequence operation and hyper-chaotic system based security features were discussed for image encryption. Encryption scheme used in DNA encoding and decoding methods are basically equivalent to each other and it makes confusion only state. With the help of chosen plaintext attack, this was easily broken down .

Wang et.al, chaos based image encryption algorithm have increased but there are some drawbacks in chaotic based cryptosystem which are threat from the security point of view. For the Chebyshev chaotic map based image encryption, cryptanalysis was made and it results in the following vulnerability i.e. plaintext based attack can easily break the system, existence of equivalent keys as well as weak keys for The encryption based scheme, low sensitivity when there is change in plain image.to overcomes this issue a remedial technique can be used .

Akhshani et.al, most of the chaos based encryption techniques are improved version of existing cryptographic algorithms. But still security problems also exist in the improved techniques. A chaos based image encryption algorithm is analyzed for the proposed improvements. It results in the weakness of the system against the chosen plaintext .

Zhang et.al, discussed that to construct cryptographic primitives CRT (ChineseReminder Theorem) is widely used. Based on the Chinese reminder theorem, security of a class of image encryption basically discussed which also referred as CECRT. Secret key of CECRT can be easily recovered efficiently with the help of the properties of the Chinese Reminder Theorem .

Tang et.al, DNA encoding and chaos map based RGB image encryption algorithm was proposed recently. But with the help of four pairs of chosen plain-images and the corresponding cipher-images, this encryption image can be easily broken. In this approach it was found that this encryption algorithm can be easily broken down with the use of known plain image. It also supported by experimental results as well as theoretical analysis .

Liu et.al, discussed the security scheme i.e. based on hybrid chaotic system and cyclic elliptic curve and it is find that with the help of known plaintext attack only one pair of ciphered image can be break down on the other hand with the help of choosing one plain image and all zero pixel values as well as corresponding ciphered image attacked by chosen plaintext .

Tong, discussed a chaos map based image encryption technique which is based on chaotic characteristics and conjugacy. A Cat map named block Cat map is also considered for permutation development based on multiple-dimensional chaotic maps to create the large key space. The encrypted algorithm is basically based on the permutation substitution. Different chaotic maps are used to control each key. There are different types of analysis i.e. cipher sensibility analysis, weak-keys analysis, statistical analysis, entropy analysis, differential analysis, cipher random analysis to test the security of the new image encryption scheme. This image encryption technique basically provides the solution for higher security and higher speed as well as lower precision for one dimensional chaotic function .

Liansheng et.al, proposed a double image encryption technique based upon the high dimension chaotic system and amplitude phase retrieval system in gyrator transform. In this approach basically three chaotic random sequences are generated with the help of chen system. First of all scrambling of widen image which having two plaintext images take place. After that it is separated into two new provisional images. After this with the help of third sequence i.e. modulated by a random phase key generated on logistic map, one interim image is converted to the private phase key. With the help of this private key, second interim image basically converted to the cipher text with white noise distribution. In amplitude-phase retrieval process which is based on this private phase key, another interim image is converted into the cipher text with white noise distribution .

Abbas et.al, a new image encryption technique was proposed based on the 2-D chaotic Baker map in different transform and a cyclic shift domain. The following techniques are exploited in this scheme i.e. IWT (Integer Wavelet Transform), DWT (Discrete Wavelet Transform), DCT (Discrete Cosine Transform). A comparison of all these results that DWT is superior .

Lima et.al, discussed a new approach for image encryption. In this a cosine number transfer method is used. It is basically a mathematical technique which requires the arithmetic operation. It avoids the errors and it allows the recovery of image if only encryption or decryption is identical. It is flexible and easily applied to the applications of medical images.

It revel the many attacks of cryptography .

Comparison of Image Encryption Schemes

A comparison among various encryption techniques as well as their performance with respect to various parameters is presented in table 1. Speed basically depends upon the particular encryption algorithm. It is measured in terms of variable, moderate, low and fast. Security of cryptographic algorithm is measured into three levels i.e. Low, Moderate and High. If the cryptographic scheme is not secure against special attacks and cryptanalysis attacks then security is measured as low. If cryptographic scheme is secure against some of the cryptanalysis attacks then it is measured as moderate. If it is robust against all cryptanalysis and special attacks then security of this scheme is measured as high.

Table 1: Performance Comparison of Image Encryption Schemes

Type of Data	Domain	Proposal	Encryption Algorithm	Speed	Cryptographic security	Advantages	Limitations	Lesson Learnt from each approach	Milestone work in each approach	Possible development trend
Image	Spatial Domain Scheme	Lin et.al	Chaining Random Grid	Fast	High	Bandwidth and storage saving.	It suffer from high computational cost and image size expansion	No pixel expansion is involved	overhead of a skillfully designed codebook is removed	It can be applied to heavyweight computation
		Zhang et.al	Single round permutation diffusion chaotic cipher	Fast	High	One can develop different permutation sequences for different plain-images	This secure chaotic cipher is valid only for gray images.	chaotic image encryption algorithm found insecure when the iteration round is equal to one	large key space, high security and good encryption decryption speed	Real-time image can be encrypted
		Hua et.al	Heterogeneous bit-permutation and correlated chaos	Fast	High	It differentiate the information contents of bits in a pixel	It requires at least one invocation of one-way permutation for every bit of length	heterogeneous bit-permutation decreases computation cost and improves permutation efficiency	the introduction of correlated chaos not only makes the initialization for permutation chaotic maps, but enhances the link between the chaos	With the help ofXOR operation, heterogeneous bit permutation technique provides the different way of diffusion for images.
		Liu et.al	Complex number chaotic maps based	Low	High	It reduces the encryption time, correlation of cipher image.	It has slow speed because a lot of iterations are required and many values have to be discarded.	Chaotic map from the real number field to the complex number field generate pseudorandom sequences	Encryption algorithm supports high security and efficiency	Confusion and diffusion can be applied to spread the influence of each bit of the plain-image all over the cipher-image.

		Chen et.al	A dynamic state variables selection	Fast	High	A tiny change in the plain image will bring about totally different key stream sequences even though the same secret key is used.	At least two chaotic state variables are required for encrypting one plain pixel, in permutation and diffusion stages respectively.	permutation and diffusion are two independent procedures with fixed control parameters	superior security and high efficiency achieved	pixel-swapping based confusion strategy and snake-like mode diffusion can be produced in state variables distribution
		Ling	A chaotic 3D cat map	Fast	High	The main advantage of this methodis security, simplicity and efficiency.	Only one traverse of the image pixels is needed.	Confusion and diffusion areachieved by a composed encryption design of combined permutation and substitution operation.	It is immune to various types of cryptographic attacks.	One can easily to extend the algorithm for color images by employing encryption to the Red, Green, Blue channels separately
		Zhou et.al	1D chaotic maps (seed maps)	Fast	High	This algorithm give excellent performance in image encryption as well as with respect to various attacks.	It is based on existing chaotic map.	It has excellent diffusion and confusion properties and can resist the chosen-plaintext attack.	Proposed chaotic system is able to produce a large number of new chaotic maps.	the encryption speed of proposed algorithm can be improved by performing the 1D substitution processes in parallel.
		Zhang et.al	Cross chaotic map	Low	Moderate	Cross chaotic map has better performance inLyapunov exponent and complexity analysis.	Diffusion and permutation with 3D baker are carried out based on features of image formats. There is not any single method.	Diffusion and permutation are the main tools for encryption in any scheme.	proposed method is highly secure, and the speed of algorithm is faster than classical solutions	Confusion can also be applied for this scheme to confuse the attacker.
		Boriga et.al	Hyper chaotic map based on parametric equations	Fast	High	the proposed image encryption scheme provides an efficient and secure way for image encryption	hyper chaotic map derivate from the parametric equations of serpentine curve	The pixels from the plain image are shuffled with a random permutation.	pixels are modified with a XOR-scheme based on the proposed map.	Diffusion can also be applied to make it more complicated.
		Qian et.al	Spatiotemporal non-adjacent coupled map lattices	Fast	Moderate	a bit-level pixel permutation strategy which enables bit planes of pixels permute mutually without any extra storage space.	reduces the intrinsic features of an image.	the key space and sensitivity is good enough to resist to brute-force attacks.	Superior security and high efficiency.	initial conditions and parameters of the maps can be generated using 3D catmap.

		Francois et.al	Coupling of chaotic function and XOR operator	Fast	High	The advantage of the encryption scheme is its automatic adaption to the entropy of the plain-image assuring secure cipher-image.	Only integers are used in the proposed algorithm.	This method has drasticall y disrupted the internal binary structure of the images and progressi vely induced randomne ss characteri stics.	cryptosyst em is efficient and secure enough to be used for the image encryption and transmissi on.	Randomness can also be increased using Lorentz map.
		Chen et.al	Multi-beams interference principle and vector composition	Fast	High	the encryption system divides information of the original image into 7 parts randomly, hence the attacker cannot distinguish the original image.	the quality of the decrypted image become bad when incorrect pixel number of Phase only mask is small.	to obtain the phase only masking back casting approach is necessary	no decrypted image can be obtained until all the keys are rightly used.	the keys can be stored separately to improve the security of encryption system
		Som et.al	A Non-adaptive Partial Encryption of Grayscale Images Based on Chaos	Fast	High	The proposed algorithm effectively determines significant bit planes on the basis of contribution made by them to form a pixel.	It is applicable for gray image only.	The significan t bit planes are encrypted by the key steam generated on the basis of a chaos based Pseudora ndom binary number generator.	Encryption algorithm is effective, simple to implement , it's secret key space is reasonably large and can effectively resists exhaustive attack, statistical attack.	Designing an adaptive algorithm to detect the significant bit planes and thereafter encrypting them by chaos based PN sequence would be of future concern.
		Enayatifar et.al	A hybrid model of the Tinkerbell chaotic map, deoxyribonucleic acid (DNA) and cellular automata (CA)	Fast	High	It is suitable high-security encryption.	Proposed scheme is applicable only for gray images.	The DNA-based approach includes two phases .the first phase applied to encode plain image pixels to a DNA sequence next phase, affect encoded plain-	proposed scheme not only demonstrat es outstandin g encryption , but also resists various typical attacks.	Proposed scheme can be modified for the color images.

								image pixels.		
		Wang et.al	Hybrid chaotic maps and dynamic random growth technique	Fast	High	Proposed scheme eliminate the cyclical phenomenon and resist chosen plaintext attack	An intermediate parameter is calculated according to the image block. Hence attacker can easily modify the image block.	the generated key streams are dependent on the plaintext image.	the proposed encryption algorithm is secure enough to be used in image transmission systems.	Confusion and Lorentz map can be applied to enhance the security.
		Wang et.al	Based on DNA (Deoxyribonucleic acid) sequence operations and chaotic system	Fast	High	The scheme is able to resist differential attack, brute-force attack, statistical attack and plaintext attack.	This scheme is valid only for gray images.	Permutation of rows and columns of the DNA matrix is necessary to enhance the security.	It has extraordinarily high security due to hybrid approach.	Proposed scheme can be modified for the color images, further Salt & pepper, Gaussian, Poisson and speckle attack can be applied to check the security.
		Zhang et.al	Based on DNA subsequence operation and chaotic system	Fast	High	Proposed algorithm is very suitable for digital image encryption.	This algorithm only applicable for gray scale image.	Pixels can be scrambled using different technique	Algorithm not only has good encryption effect, but also has the ability of resisting exhaustive Attack and statistical attack.	Lorentz map can also be used to increase the randomness.
		Zhou et.al	A novel symmetrical image encryption algorithm based on skew tent map.	Fast	High	It is valid for both gray-scale image and color image.it is suitable for encryption of any size of image.	There is no complex sub-block processing operation	R, G, B components of the true color image are encrypted at bit level and operated at the same time.	It is highly secure and suitable for practical image encryption	Confusion ,permutation and diffusion can be applied to spread the influence of each bit of the plain-image all over the cipher-image
		Wang et.al	Based on chaotic system and improved Gravity Model	Fast	High	Gravity Model can be use not only in image encryption, but also in information hiding.	The proposed scheme is valid only for gray images.	The scheme is sensitivity to the keys, which can improve the complexity and difficulty of decryption.	Proposed algorithm has good effect and it can resist common attacks	The proposed algorithm can be extended to the algorithm for color images
		Wang et.al	Reversible cellular automata (RCA) combining chaos	Fast	High	The proposed scheme has perfect information protection ability, and satisfied the confusion and	Diffusion is applied only for the higher 4 bits in a pixel.	The higher 4 bits carry almost the information of an image.	Algorithm is more secure and hence more suitable for image encryption	It is enhanced in parallelism cryptosystem.

						diffusion request in cryptosystem			for application s.	
		Zhang et.al	A linear hyperbolic chaotic system of partial differential equations	Fast	High	It has larger parameter space, stronger sensitivity to initial condition and control parameters.	It has not been employed in cryptography so far.	It has higher potential to adopt for network security and secure communi cations.	The proposed scheme is efficient, practicable and reliable.	Lorentz and chen's chaotic can also be applied to generate the initial parameters.
		Zhu et.al	Hyper chaos sequence based shuffling and Chinese reminder theorem	Fast	High	It can be used to change the plain image information drastically.	Hyper-chaos has more complex dynamical characteristic s than chaos.	Diffusion and compressi on can be applied simultane ously.	It compress the plain image with a given compressi on ratio.	It can be extended to the 3D hyper chaos.
		Zhang et.al	Image fusion and DNA sequence operation and hyper chaotic system	Fast	High	Algorithm is very suitable for digital image encryption.	proposed algorithm can only resist most known attacks	larger secret key space and high sensitive to the secret key is the main concern for encryptio n algorithm	Proposed algorithm not only has good encryption effect, but also has the ability of resisting exhaustive attack and statistical attack	Matrices can be generated using random generator.
		Mohamed	Reversible one-dimensional cellular automata	Fast	High	Parallel mode of operation for encryption and decryption, specific image's area can be deciphered without knowledge of the full Ciphered-image.	it provides the ability to perform only a selective area decryption	high security and execution performa nces can be achieved using the approach	very useful for real time application s	better performances can be achieved if hardware implementati on is used.
		Escobar	Based on total plain image characteristics and 1D logistic map with optimized distribution based on Murillo-Escobar's algorithm	Fast	High	Simple structure and easy to implement, ideal for fast encryption of high capacity data	shorter periodicity, and small key space	DNA encoding and chaotic sequences are dependen t only from the secret key	fast and secure against several known attacks	it can be implemented in real-time applications where a high security is required.
		Qian et.al	Based on the spatiotemporal chaos of the mixed linear–nonlinear coupled map lattices	Fast	High	key space and sensitivity is better enough to make brute-force attacks infeasible.	It is valid for gray image.	bit level pixel permutati on enables the lower and higher bit planes of pixels	superior security and high efficiency	We can explore related applications in other information security fields
		Luo et.al	Chaos based encryption	Low	High	Effective coding compression to satisfy desirable storage.	time required for encryption and decryption is a little higher	secure image encryptio n scheme both in transform	An efficient, secure and robust encryption mechanis	Can be used for practical application in real-time transmission system

								domain and spatial domain	m	
		Enayatifar et.al	Weighted discrete imperialist competitive algorithm (WDICA)	Fast	High	The advantage of this method is its ability to optimize the outcome of all iterations using WDICA	This algorithm only applicable for gray scale image.	WDICA is applied to the cipher images.	WDICA not only demonstrates excellent encryption but also resists various typical attacks	it can be implemented in real-time applications where a high security is required.
		Akhavan et.al	chaos-based image encryption	Fast	High	A JTC based encryption scheme asymmetric enhances the security.	Due to amplitude- and phase-truncation, the encryption scheme becomes asymmetric.	cryptanalysis of the scheme reveals that it is resistant to hybrid attack	A novel and highly secure encryption scheme based on JTC architecture combined with amplitude- and phase-truncation approach.	The scheme can be implemented digitally or optically employing a conventional JTC
		Zhang et.al	Chinese Reminder Theorem	Fast	High	The image encryption algorithm presented and analyzed and proved to be weak against chosen plain-text attack.	Many of the proposed improvement methods suffer from serious security problems	The shuffling step is very weak and the shuffling map could be recovered with limited amount of chosen plain-images for all the cases.	the security of the recently proposed improvement method for a chaos based image encryption algorithm is analyzed	The size of the key space is less than the claimed value and it can be improved.
		Eslami et.al	Chaotic maps, cellular automata and permutation–diffusion	Low	Moderate	highly secure diffusion mechanism	This algorithm only applicable for gray scale image.	It can detect whether the image is tampered during the transmission or not.	computational efficiency and ease of implementation.	it can be implemented in real-time applications and also for color images.
		Kanso et.al	Chaos-based image encryption	Fast	High	high sensitive dependence of the encryption and decryption schemes to a slight modification in the secret key, the plain image and the encrypted image	Only specific to medical	The mixing of the blocks provides a strong chaining of the image blocks, to defeat differential attacks	the key space is large enough to defeat brute force attacks.	It can be implemented in real-time secure image communication.
		Chen et.al	Gray code based permutation	Fast	High	It takes full advantage of	This algorithm	pixel-related	high security	The proposed algorithm can

						(n, p, k)-Gray-code achievements	only applicable for gray scale image.	image diffusion mechanism resist known-plaintext or chosen-plaintext attack		be extended to the algorithm for color images
		Huang et.al	chaotic image encryption algorithm	Fast	High	It can solve the fixed Keystream problem.	It was tested for gray image only.	It can resist against chosen-plaintext and known-plaintext attacks	high security and efficiency.	3D logistic map can also be applied.
		Ghebleh et.al	A robust shuffling–masking image encryption	Fast	High	masking of every block is influenced by all previously masked blocks.	masking phase uses three interconnected 1D skew tent maps to mask the output of the shuffling phase	secure and reliable scheme for use in secure communication applications.	a large key space, strong sensitivity to the secret key, and is robust against differential attacks.	Masking can be done through several ways to enhance the security for real time applications
		Song et.al	Nonlinear chaotic algorithm (NCA) chaotic map	Fast	High	The performance of the proposed scheme is verified with the statistical analysis including histogram analysis, information entropy analysis, correlation analysis and differential analysis.	It was tested for gray image only.	the scheme is secure enough to resist the brute-force attack, entropy attack, differential attack, chosen-plaintext attack, known-plaintext attack and statistical attack.	proposed encryption scheme is of high key sensitivity and large key space	This scheme can also be extended to multimedia data.
		Zhu et.al	Arnold map	Fast	High	bit-level permutation and diffusion	It was tested for gray image only.	Arnold map, Permutation and diffusion Are enough to resist from several attacks.	the proposed scheme is competitive with that ordinary Permutation–diffusion type image cipher.	It can be applied for practical image encryption and color images.
		Chen et.al	Nonlinear inter-pixel computing and swapping based on chaos	Fast	High	higher bit-planes carry more information than lower bit-planes	When ciphering these images, such cryptosystem may leak the important information of lower bit-planes	satisfactory security performance can be achieved within the first encryption round.	high level of security for practical secret applications.	It can be applied to real time applications.
		Kumar et.al	Chaotic map based	Fast	High	The key space can be	complex non-linearity	plain image can	Proposed algorithm	It can be implemented

						increased by selecting high dimensional chaotic system.		be recovered with negligible data loss, having very low MSE values	offers high security and is suitable for practical image encryption.	in real-time secure image Communicati-on
		Liu et.al	Chaos-based asymmetric color image encryption	Fast	High	distribute different keys to different receiver through keys changing mechanism	Only hash value used to generate the initial conditions.	By modifying one-bit in the plain image in each encryption can resist against known-plaintext and chosen plaintext attacks	Feasibility and effectiveness of the asymmetric cryptosystem for color image encryption	It can be applied further in symmetric color image encryption.
		Sui et.al	Logistic map based	Fast	High	each plain image is scrambled based on a sequence of chaotic pairs generated with a system of two symmetrically coupled identical logistic maps.	phase-only function of each scrambled image is retrieved with an iterative phase retrieval process in the fractional Fourier transform domain.	three decryption keys are generated in the encryption process, which make the proposed encryption scheme has high security against various attacks, such as chosen plaintext attack.	three random phase functions are used as encryption keys to retrieve the phase-only functions of plain images	encryption capacity of the proposed scheme can be further enhanced by
		Ong et.al	Format-compliant encryption method with the data embedding feature for JPEG compressed image	Fast	High	the proposed method is able to generate an encrypted image of the same size as the original image	AC coefficients are scanned in eight different orders only.	The performance of the proposed method is verified through experiments using various standard test images and the UCID dataset.	The proposed method has superiority in terms of robustness against sketch attacks.	AC and DC coefficients can be further decomposed into more than 8 orders to enhance the security.
		Xie et.al	Fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system	Fast	High	The effectiveness of the proposed chosen-plaintext attack is supported by theoretical analysis, and verified by experimental	The scheme can be broken with 4mn/3 +1 chosen plain-images.	image encryption algorithm under study is not recommended in applications requiring	the encryption scheme can be effectively broken with less than $[\log_2 (4mn)/2]$ +1 chosen plain-	A high level of security can be achieved by applying different methods.

						results.		a high level of security.	images.	
		Liua et.al	Chaos-based color image block encryption scheme using S-box	Fast	High	The ciphered image can be obtained after substituting each block with the paired S-box.	Each component of the color image is divided into blocks with the same size.	For each block, a one-to-one correspon ding 8× 8 S-box is generated to substitute it.	scheme is suitable for image encryption	Lorentz map can be combined with the chaotic map to generate the initial condition so that attacker can be confused.
		Liu et al.	Chaos based SHA-2	Fast	High	The permuted image is divided into 256-bit long blocks	Random numbers are applied to generate only one-time initial conditions.	The avalanche effect is applied to diffuse the blocks.	Proposed algorithm is robust against common attacks	Confusion, permutation and diffusion can be applied to improve the proposed scheme.
		Enayatifar et.al	Based on a hybrid model of deoxyribonucleic acid (DNA) masking, a genetic algorithm (GA) and a logistic map	Fast	Moderate	A hybrid model of a genetic algorithm and chaotic function is the best DNA mask for image encryption	Limited DNA masks are generated by using a logistic map and DNA sequence.	DNA and logistic map functions are used to create the number of initial DNA masks.	Proposed scheme not only demonstrat es excellent encryption but also resists various typical attacks.	Diffusion can also be applied to further enhance the security.
		Zhang et.al	Discrete chaotic sequence	Fast	High	The proposed scheme not only decreases the operations of the image encryption and decryption, but also makes the size of the encrypted image.	It is valid only for jpeg images.	JPEG image encryptio n can meet the security requireme nt of the storage and transmissi on of JPEG images.	Proposed scheme provides an effective and feasible way of encrypting JPEG images.	The proposed scheme can be further improved for the different types of image format.
		Zhang et.al	Based on spatiotemporal chaotic system	Fast	High	S-box is considered as a circular sequence with a head Pointer	It is valid for the gray images.	circular S-box and the key stream buffer are introduce d to increase the security	encryption algorithm is highly secure and more efficient for most of the real image encryption practices.	The proposed scheme can further be applied to the color images.
		Lang	Color Blend (CB) and Chaos Permutation (CP) based	Fast	High	The original color image is first exchanged and mixed randomly from the standard red–green–blue (RGB) color space to R′G′B′ color space by rotating the	the encrypted image is real-valued	output is real which can save storage space of image	Proposed algorithm is feasible, secure, sensitive to keys and robust to noise attack and data loss	The proposed color image encryption can also be applied to encrypt three gray images by transforming the gray images into three RGB color components.

						color cube with a random angle matrix.				
		Zhang et.al	exchange and random access strategy	Fast	Moderate	The proposed scheme involves the random confusion of the coordinates of the two predefined permuting planes.	every pixel is randomly mapped	"random access" strategy introduce ultra-security when the new confusion methods are applied to RGB color channels.	The proposed scheme has better histogram distributio n, correlation coefficient s, and ability to resist differential attacks	Randomness can be further generated. Using random or seed generator.
		Zhang et.al	confusion-diffusion based	Fast	High	The RGB components of the color image are converted into the real part and the imaginary part of a complex function by employing the affine transform	Real part and the imaginary part of a complex function are converted into the gyrator domain.	affine transform and the gyrator transform are regarded as the key in the encryptio n algorithm	The gyrator transform is performed twice to enhance the security of this encryption algorithm	Security and robustness of the proposed color encryption scheme can be improved further using diffusion and confusion.
		Liu et.al	Choquet fuzzy integral (CFI) and hyper chaotic system	Fast	High	The key stream has both the key sensitivity and the plaintext sensitivity.	Plain image is employed to generate only six initial values of the chaotic systems.	The scheme can achieve good encryptio n result through only one round encryptio n process, the key space is large enough to resist against common attack.	The scheme is reliable to be applied in image encryption and secure communic ation.	More initial values can be generated using random generator and Lorentz map.
		Jeng et.al	Chaos based Permutation and Diffusion	Fast	High	The proposed image encryption method combined two-step-only quadrature phase-shifting digital holography with compressive sensing (CS) has been proposed	This method largely decreases holograms data volume	Proposed method can be efficientl y applied to binary image and grayscale image to perform image encryptio n and compressi on .	it is also suitable for some special optical imaging cases such as different wavelengt hs imaging and weak light imaging	it is expected to be widely used for 3D object encryption, video secure transmission, real-time video encryption technology and future all-optical networks, such as real-time images security transmission and naked-eye 3D Television.

		Zhang	Based on DNA sequence operation and hyper-chaotic system	Fast	High	The proposed scheme is enough to improve the sensitivity.	Security of the proposed scheme relies only on two operations, permutation and diffusion.	Confusion and diffusion are not secure enough until or unless any hybrid approach applied.	proposed scheme can resist the known-plaintext and the chosen-plaintext attacks.	3D cat map can be applied to enhance the security.
		Wang et.al	Chebyshev chaotic map	Fast	High	The proposed scheme is flexible and can be applied to any size of image.	DNA encoding and decoding schemes provide nearly no additional privacy.	all kinds of DNA encoding and decoding schemes used in this encryption scheme are equivalent to each other	The proposed scheme successfully broke the scheme with the chosen plaintext attack method.	The proposed scheme can be further improved to enhance the security in actual communication.
	Frequency Domain Scheme	Wei Li et.a	Computer-generated integral imaging and cellular automata transform (CAT)	Fast	Moderate	A set of plane images of 3D image is reconstructed along the Output planes.	Recording setup is necessary.	a set of plane images of 3D image is reconstructed along the output planes	Quality of the reconstructed Image improved by reducing energy loss compared with the traditional complicated transform process	Reconstructed 3D image quality of the proposed scheme can be greatly improved using pixel algorithm.
		Sharma	Two stage random matrix affine cipher associated with discrete wavelet transformation	Fast	High	Efficient and secure encryption scheme.	encryption process is elementary but decryption process is more unmanageable	This approach can be used for transmission of RGB image data efficiently and securely through unsecured channels.	attacker cannot decrypt the image correctly until he don't have correct keys and the correct arrangement of RMAC parameters,	Fractional Fourier transform can be combined with discrete wavelet transformation.
		Chen et.al	Affine transform and gyrator transform	Fast	High	Before encrypting the color image, the piecewise linear chaotic map (PWLCM) is used to generate the 128-bit secret keys.	The outputs of the Choquet fuzzy integral (CFI) are used to confuse and diffuse the three color components of the image.	The proposed scheme is reliable to be adopted for network security and secure communications.	The proposed scheme not only can achieve good encryption result and large key space	Confusion and diffusion can be applied to enhance the security.
		Latif et.al	Total auto-morphism in	Fast	High	good encryption	Only Y (Luminance)	quantum chaotic	proposed method	Confusion and diffusion

			integer wavelet transform			performance	component of low frequency subband are scrambled.	system is better way for encryption	maintains good encryption performance.	can be applied to make it more complicated
		Li et.al	Cascaded Fractional Fourier transform	Fast	High	Using phase truncation in the fractional Fourier domain, one can use an asymmetric cryptosystem to produce a real-valued noise-like ciphertext	Any user can reconstruct all of the original images using a different group of phase masks	masks is subsequently modulated into an interim mask, which is encrypted into the ciphertext image	The proposed system has high resistance to various potential attacks, including the chosen plaintext attack	Phase masking can be improved using different ways.
		Abuturab et.al	Hartley transform and gyrator transform	Fast	High	Encryption and decryption takes place in two phase	the proposed algorithm can only resist any type of histogram based attacks.	Gyrator transform is extremely sensitive to key	Security system is compact and feasible.	It can be extended to resist various type of attacks.
		Khashan et.al	transformation algorithm	Low	Moderate	reduce the perceivable information for other unencrypted parts	Only block based encryption was performed.	improvement in processing speed	sufficient level of security achieved within a reasonable computational Complexity.	Diffusion, confusion method can also be applied.
		Chen et.al	Pixel scrambling technique and gyrator transform	Fast	Moderate	scheme well address the cross-talk disturbance.	there is serious cross-talk disturbance in the phase-based image when the encrypted data undergoes noise perturbation or occlusion attack	The disturbance will cause serious deterioration in the retrieved phase based image and bring about visibility ambiguities to the receiver,	enhance the security of the original cryptosystem	Cross talk disturbance can be further improved using diffusion and confusion.
		Liu et.al	Based on amplitude-phase hybrid encoding and iterative random phase encoding in fractional Fourier transform (FrFT)	Fast	High	The multiple rounds for encryption can be performed in the scheme or some plaintext information can be added during the encryption process.	known-plaintext attack can break the chaotic system with only a pair of plain image/cipher image.	Cyclic elliptic curve and generalized logistic map can be replaced with the simple and excellent system like piecewise linear chaotic map.	rough comparison between chaos theory and optical technique applied to image encryption is done in terms of robustness and statistical analysis.	The scheme should possess the architecture of confusion–diffusion to improve sensitivity.
		Wang et.al	Based on amplitude–phase mixed encoding and multistage random phase encoding in	Fast	High	The image encryption algorithm is based on permutation–substitution,	small key space	In order to produce a large key space, a	image encryption method solves the problem of low	In order to produce a large key space, a Cat map named block Cat

			gyrator transform (GT) domains			and each key is controlled by different chaotic maps		Cat map named block Cat map is also designed for permutation process based on multiple-dimensional chaotic maps	precision of one dimensional chaotic function and has higher speed and higher security	map is also designed for permutation process based on multiple-dimensional chaotic maps. It can improve the security.
		Sui et.al	Discrete multiple-parameter fractional angular transform and logistic map	Fast	High	Amplitude-phase hybrid encoding blends the information originating from the original images randomly into the amplitude and phase components of a complex valued image.	the complex image is further encoded into a white Gaussian noise distribution by an iterative phase encoding system with FrFTs.	The primitive images can be retrieved exactly by applying correct keys with initial conditions of chaotic system.	the encryption method has impressively high security level and certain robustness against data loss and noise interference.	The introduction of phase amplitude hybrid encoding can thoroughly alleviate the difference of two original images in keys space and sensitivity to the transform orders of FrFT.
		Sui et.al	Yang-Gu mixture amplitude-phase retrieval algorithm and high dimension chaotic system in gyrator transform domain	Fast	High	the proposed method is highly sensitive to the decryption keys	information originating from the secret images are blended uniformly together in the amplitude and phase distributions of a synthetic complex valued image.	The primitive images can be recovered exactly by applying correct keys with initial conditions of chaotic system, the GT orders and the pixel scrambling operation	the proposed scheme has considerably high security level and certain robustness against data loss and noise disturbance.	In the future, we can further investigate the resistance of this novel approach against other types of attacks.
		Li et.al	Chaos Based local pixel scrambling technique, Arnold and gyrator transform	Fast	High	The proposed encryption scheme has an obvious advantage that no phase keys are used in the encryption and decryption process, which is convenient to key management.	No phase keys are used.	the proposed encryption scheme has high resistance against to the potential attacks such as chosen plaintext attack.	A set of numerical simulations have illustrated the feasibility and effectiveness of the encryption scheme such as high robustness against other attacks such as	the security of the cryptosystem can be enhanced by using extra parameters such as initial values of chaos functions, fractional orders and vector parameters of transform.

									brute-force attack, noise attack and occlusion attack.	
		Zhou et.al	A two-dimensional sine Logistic modulation Map, Arnold transform and the discrete fractional random transform	Fast	High	Compared with existing chaotic maps, it has the wider chaotic range, better ergodicity, hyper chaotic property and relatively low implementation cost.	It is not suitable for large images.	It can quickly shuffle neighboring pixels within an image.	better ergodicity and hyper chaotic	Diffusion can spread the influence of each bit of the plain-image all over the cipher-image.
		Sui et.al	Discrete fractional random transform and logistic maps	Fast	High	the ciphertext image is real-valued function and more convenient for storing and transmitting	plaintext images fails to be decrypted unless all of the correct keys such as three initial values of Chen system, the rotation angle of GT and the private phase key are known.	Extensive cryptanalysis and simulation results have demonstrated the security, validity and feasibility of the propose encryption scheme.	the proposed encryption scheme has high resistance against to various possible attacks such as chosen-plaintext attack.	the security of the proposed encryption scheme is enhanced greatly because of high sensitivity of initial values of Chen system and rotation angle of gyrator transform.
		Naeem et.al	The Integer Wavelet Transform (IWT), the Discrete Wavelet Transform (DWT), and the Discrete Cosine Transform (DCT)	Fast	High	effective compression and fast encryption	It cannot tolerate a certain range of noise intensity and occlusion attacks	scheme is sensitive to the keys and secure with a strong ability to resist statistical analyses.	The scheme can not only reduce the data of the encrypted image, but also tolerate a certain range of noise intensity and occlusion attacks.	The scheme can also scramble and change the image pixels greatly due to the Arnold transform and the discrete fractional random transform.
		Lima et.al	Cosine number transform	Fast	High	A chaotic confusion–diffusion process is used to disorder the plaintext images, which strengthens the nonlinearity in spatial domain and DFrRT domain.	The plaintext images fails to be recovered unless all of the correct keys including four initial values of logistic maps and a phase distribution are known.	The phase distribution is produced in the encryption process and directly related to two plaintext images.	the proposed scheme has the characteristic of asymmetric encryption technique and high resistance against to the conventional attacks such as chosen plaintext attack.	3 D chaotic map can also be applied to scrambling and shuffling the images.

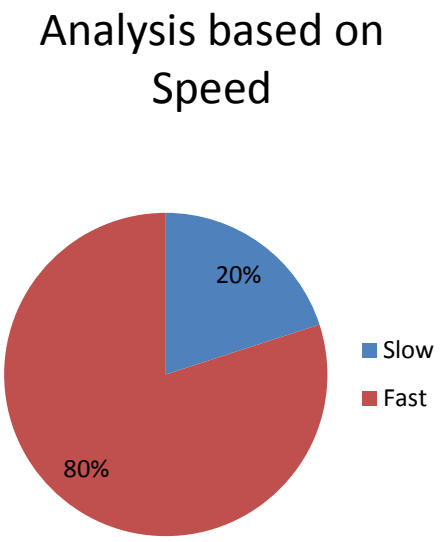

Figure 1

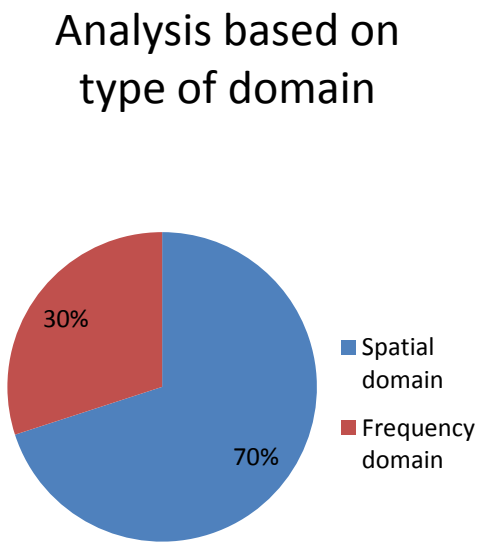

Figure 2

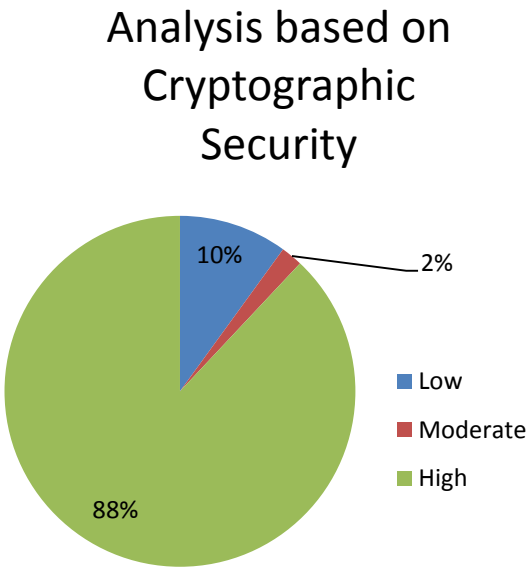

Figure 3

2. Conclusion

It is the era of the advancement in technology. All types of valuable data basically communicated with the help of public network. In this paper we have discussed the Cryptography and Steganography techniques, types as well issues in both. We further also discussed the various cryptography techniques and their performance. Each and every encryption scheme is isolated in its own way. It is different for different applications. Different types of measurement are considered to protect the data from unauthorized users.

References

Leo Yu Zhang, Xiaobo Hu, Yuansheng Liu, Kwok-Wo Wonga, JieGan(2014),A chaotic image encryption scheme owning temp-value feedback, Communications in Nonlinear Science and Numerical Simulation 19 (10) 36533659.

Xingyuan Wang, Hui-li Zhang(2015), A color image encryption with heterogeneous bit-permutation and correlated chaos, Optics Communications 342 5160.

Yang Liu, Xiaojun Tong, Shicheng Hu(2013), A family of new complex num-ber chaotic maps based image encryption algorithm, Signal Processing: Image Communication 28 15481559.

Junxin Chen, Zhi-liang Zhu, Chong Fu, Hai Yu, Li-bo Zhang(2015), A fast chaos-based image encryption scheme with a dynamic state variables selection mecha-nism, Commun Nonlinear Science and Numerical Simulation 20 846860.

ZhongyunHua, Yicong Zhou, Chi-Man Pun, C.L. Philip Chen(2015), 2D Sine Logistic modulation map for image encryption, Information Sciences 297 8094.

Xiao Wei Li, Sung Jin Chob, Seok Tae Kim(2014), A 3D image encryption technique using computer-generated integral imaging and cellular automata transform, Optik 125 29832990.

Ch.-H. Lin, T.-H.Chenb, Ch.-S.Wub(2013), A batch image encryption scheme based on chaining random grids, ScientiaIranica D 20 (3), 670681.

GuoshengGu, Jie Ling(2014), A fast image encryption method by using chaotic 3D cat maps, Optik 125 47004705.

Manish Kumar, D.C. Mishra, R.K. Sharma(2014), A first approach on an RGB image encryption, Optics and Lasers in Engineering 52 2734.

Yicong Zhou, Long Bao, C.L. Philip Chen(2014), A new 1D chaotic system for image encryption, Signal Processing 97 172182.

Ahmed A. Abd El-Latif ,Li Li, Ning Wang, Qi Han, XiamuNiu(2013), A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces, Signal Processing 93 29863000.

Miao Zhang, Xiaojun Tong(2014), A new chaotic map based image encryption schemes for several image formats, The Journal of Systems and Software 98 140154.

RaduBoriga, Ana Cristina Dsclescu, IustinPriescu(2014), A new hyperchaotic map and its application in an image encryption scheme, Signal Processing: Image Communication 29 887901.

Zhang Ying-Qiana, Wang Xing-Yuana(2015), A new image encryption algorithm based on non-adjacent coupled map lattices, Applied Soft Computing 26 1020.

M. Francois, T. Grosges, D. Barchiesi, R. Erra(2012), A new image encryption scheme based on a chaotic function, Signal Processing: Image Communication 27 249259.

Linfei Chen, Jingyu Liu, Jisen Wen, XiongGao, Haidan Mao, Xiaoyan Shi, QinglingQu(2015), A new optical image encryption method based on multi-beams interference and vector composition, Optics and Laser Technology 69 8086.

Sukalyan Soma, SayaniSenb(2013), A Non-adaptive Partial Encryption of Grayscale Images Based on Chaos, Procedia Technology 10 663 671.

RasulEnayatifar, HosseinJavedaniSadaei, Abdul Hanan Abdullah, Mal-rey Lee, Ismail FauziIsnin(2015), A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata, Optics and Lasers in Engi-neering 71 3341.

Xingyuan Wang, Lintao Liu, Yingqian Zhang(2015), A novel chaotic block image encryption algorithm based on dynamic random growth technique, Optics and Lasers in Engineering 66 1018.

Xing-Yuan Wang, Ying-Qian Zhang, Xue-Mei Bao(2015), A novel chaotic image encryption scheme using DNA sequence operations, Optics and Lasers in Engineer-ing 73 5361.

Qiang Zhang, Xiaopeng Wei(2013), A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system, Optik 124 6276 6281.

GuominZhoua, DaxingZhangb, YanjianLiub, Ying Yuana, QiangLiua(2014)., A novel image encryption algorithm based on chaos and Line map, Neuro com-puting

Xing-yuan Wang, Na Wei, Dou-dou Zhang,(2015) A novel image encryption algorithm based on chaotic system and improved Gravity Model, Optics Commu-nications 338 209217.

Xingyuan Wang, Dapeng Luan(2013), A novel image encryption algorithm using chaos and reversible cellular automata, Communication Nonlinear Science Numerical Simulation 18 30753085.

Yushu Zhang, Di Xiao, YongluShu, Jing Li(2013), A novel image encryption scheme based on a linear hyperbolic chaotic system of partial di erential equations, Signal Processing: Image Communication 28 292300.

Hegui Zhu, Cheng Zhao, Xiangde Zhang(2013), A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem, Signal Processing: Image Communication 28 670680.

Qiang Zhang, Ling Guo, XiaopengWei(2013), A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system, Optik 124 3596 3600.

FaraounKamelMohamed(2014), A parallel block-based encryption schema for digital images using reversible cellular automata, Engineering Science and Tech-nology, an International Journal 17 85-94.

M.A. Murillo-Escobar,C. Cruz-Hernndez, F. Abundiz-Prez, R.M. Lpez-Gutirrez, O.R. Acosta Del Campo(2015), A RGB image encryption algorithm based on total plain image characteristics and chaos, Signal Processing 109 119131.

Zhang Ying-Qian, Wang Xing-Yuan(2014), A symmetric image encryption al-gorithm based on mixed linearnonlinear coupled map lattice, Information Sciences 273 329351.

YulingLuo, Minghui Dub, Junxiu Liu(2015), A symmetrical image encryption scheme in

wavelet and time domain, Commun Nonlinear SciNumerSimulat 20 447460.

RasulEnayatifar, Abdul Hanan Abdullah, MalreyLee(2013), A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption, Optics and Lasers in Engineering 51 10661077.

Muhammad Ra q Abuturab(2015), An asymmetric single-channel color image encryption based on Hartley transform and gyrator transform Optics and Lasers in Engineering 69 4957.

AtiehBakhshandeh, ZibaEslami(2013), An authenticated image encryption scheme based on chaotic maps and memory cellular automata, Optics and Lasers in Engineering 51 665673.

Osama Ahmed Khashan, Abdullah MohdZin(2013), An Efficient Adaptive of Transparent Spatial Digital Image Encryption, Procedia Technology 11 288 297.

A. Kanso , M. Ghebleh(2015), An efficient and robust image encryption scheme for medical applications, Commun Nonlinear SciNumerSimulat 24 98116.

Jun-xin Chen, Zhi-liang Zhu, Chong Fu, Hai Yu, Li-bo Zhang(2015), An efficient image encryption scheme using gray code based permutation approach, Optics and Lasers in Engineering 67 191204.

Xiaoling Huang, GuodongYe(2014), An efficient self-adaptive model for chaotic image encryption algorithm, Commun Nonlinear SciNumerSimulat 19 40944104.

M. Ghebleh, A. Kanso, H. Noura(2014), An image encryption scheme based on irregularly decimated chaotic maps, Signal Processing: Image Communication 29 618627.

Chun-Yan Songa, Yu-Long Qiaob, Xing-Zhou Zhangb(2013), An image encryption scheme based on new spatiotemporal chaos, Optik 124 3329 3334.

HeguiZhua, Cheng Zhaob, XiangdeZhanga, Lianping Yang(2014), An image encryption scheme using generalized Arnold map and affine cipher, Optik 125 66726677.

Jun-xin Chen, Zhi-liang Zhu, Chong Fu, Li-bo Zhang, Yushu Zhang(2015), An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach, Commun Nonlinear SciNumerSimulat 23 294310.

Manish Kumar, PradeepPowduri, Avinash Reddy(2015), An RGB image en-cryption using di usion process associated with chaotic map, journal of informa-tion security and applications 21 20-30.

Jun-xin Chen, Zhi-liang Zhu, Chong Fu, Li-bo Zhang, Hai Yu(2015), Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains, Optics and Lasers in Engineering 66 19.

HongjunLiu,AbdurahmanKadir(2015), Asymmetric color image encryption scheme using 2D discrete-time map, Signal Processing 113 104112.

Liansheng Sui, KuaikuaiDuan, Junli Liang, Zhiqiang Zhang, HainingMeng(2014), Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain, Optics and Lasers in Engineering 62 139152.

Yanbin Li, Feng Zhang, Yuanchao Li, Ran Tao(2015), Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform, Optics and Lasers in Engineering 72 1825.

SimYingOng, KokSheik Wong, Xiaojun Qi, Kiyoshi Tanaka(2015), Beyond format-compliant encryption for JPEG image, Signal Processing: Image Communication 31 4760.

Tao Xie, Yuansheng Liu, JieTang(2014), Breaking a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system, Optik 125 71667169.

HongjunLiua, AbdurahmanKadirb, YujunNiud(2014), Chaos-based color image block encryption scheme using S-box, International Journal of Electronics and Communication (AE) 68 676686.

Guoyan Liu, Jie Li, Hongjun Liu(2014), Chaos-based color pathological image encryption scheme using one-time keys, Computers in Biology and Medicine 45 111117.

RasulEnayatifar, Abdul Hanan Abdullah, Ismail FauziIsnin(2014), Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence, Optics and Lasers in Engineering 56 8393.

Dinghui Zhang, FengdengZhang(2014), Chaotic encryption and decryption of JPEG image, Optik 125 717 720.

Xuanping Zhang, Zhongmeng Zhao, Jiayin Wang(2014), Chaotic image encryption based on circular substitution box and key stream buffer, Signal Processing: Image Communication 29 902913.

Jun Lang(2015), Color image encryption based on color blend and chaos per-mutation in the reality-preserving multiple-parameter fractional Fourier transform domain, Optics Communications 338 181192.

Wei Zhang, Hai Yu, Zhi-liang Zhu(2015), Color image encryption based on paired interpermuting planes, Optics Communications 338 199208.

Hang Chen, Xiaoping Du, Zhengjun Liu, Chengwei Yang(2013), Color image encryption based on the affine transform and gyrator transform, Optics and Lasers in Engineering 51 768775.

HongjunLiua, XingyuanWanga, AbdurahmanKadir(2013), Color image encryption using Choquet fuzzy integral and hyper chaotic system, Optik 124 3527 3533.

Chang'eDong(2014), Color image encryption using one-time keys and coupled chaotic systems, Signal Processing: Image Communication 29 628640.

Zhang(2014), Comments on Color image encryption using Choquet fuzzy integral and hyper chaotic system Optik 125 55605565.

AlirezaJolfaei, Xin-Wen Wu, VallipuramMuthukkumarasamy(2014), Comments on the security of Di usionsubstitution based gray image encryption scheme, Digital Signal Processing 32 3436.

Jun Li, Hongbing Li, Jiaosheng Li,Yangyang Pan, Rong Li(2015), Compressive optical image encryption with two-step-only quadrature phase-shifting digital holography, Optics Communications 344 166171.

Fuh-GwoJeng, Wei-Lun Huang, Tzung-Her Chen(2015), Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes, Signal Processing: Image Communication

34 4551.

Yong Zhang(2015), Cryptanalysis of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system, Optik 126 223229.

Xingyuan Wang, Dapeng Luan, XuemeiBao(2014), Cryptanalysis of an im-age encryption algorithm using Chebyshev generator, Digital Signal Processing 25 244247.

IshaMehra, Sudheesh K. Rajput, Naveen K. Nishchal(2014), Cryptanalysis of an image encryption scheme based on joint transform correlator with amplitude- and phasetruncation approach, Optics and Lasers in Engineering 52 167173.

A. Akhavan, A. Samsudin, A. Akhshani(2015), Cryptanalysis of an improvement over an image encryption method based on total shuffling, Optics Communications 350 7782.

Chengqing Li, Yuansheng Liu, Leo Yu Zhang, Kwok-Wo Wong(2014), Cryptan-alyzing a class of image encryption schemes based on Chinese remainder theorem, Signal Processing: Image Communication 29 914920.

Yuansheng Liu, Jie Tang, Tao Xie(2014), Cryptanalyzing a RGB image en-cryption algorithm based on DNA encoding and chaos map, Optics and Laser Technology 60 111115.

Hong Liu, YanbingLiu(2014), Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve, Optics and Laser Tech-nology 56 1519.

Xiao-Jun Tong(2013), Design of an image encryption scheme based on a multiple chaotic map, Commun Nonlinear SciNumerSimulat 18 17251733.

QuWanga, Qing Guob, Liang Lei(2013), Double image encryption based on phase-amplitude hybrid encoding and iterative phase encoding in fractional Fourier transform domains, Optik 124 5496 5502.

Qu Wang, Qing Guo, Liang Lei(2013), Double image encryption based on phaseamplitude mixed encoding and multistage phase encoding in gyrator trans-form domains, Optics and Laser Technology 48 267279.

Liansheng Sui, KuaikuaiDuan, Junli Liang(2015), Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps, Optics Communications 343 140149.

Liansheng Sui, Benqing Liu, Qiang Wang, Ye Li, Junli Liang(2015), Double-image encryption based on Yang-Gu mixture amplitude-phase retrieval algorithm and high dimension chaotic system in gyrator domain, Optics Communications 354,184196.

Huijuan Li, Yurong Wang, Haitao Yan, Liben Li, Qiuze Li, Xiaoyan Zhao(2013), Double-image encryption by using chaos-based local pixel scrambling techniqueand gyrator transform, Optics and Lasers in Engineering 51 13271331.

Nanrun Zhou, Jianping Yang, Changfa Tan, Shumin Pan, Zhihong Zhou(2015), Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform,20.

Liansheng Sui, Haiwei Lu, Zhanmin Wang, Qindong Sun(2014), Double-image encryption using discrete fractional random transform and logistic maps, Optics and Lasers in Engineering 56 112.

Ensherah A. Naeema, Mustafa M. AbdElnabya, Naglaa F. Solimanb,i, Alaa M. Abbasc(2014),

E cient implementation of chaotic image encryption in transform domains, The Journal of Systems and Software 97 118127.

J.B. Lima, F. Madeiro, F.J.R. Sales(2015), Encryption of medical images based on the cosine number transform, Signal Processing: Image Communication V35 18.

Yang Liu, Xiaojun Tong, Shicheng Hu(2013),A family of new complex number chaotic maps based image encryption algorithm,Signal Processing: Image Communication Vol28 pp. 1548–1559.