An Overview of Image Security Techniques

Madhu B.
Dept. of CSE,Dr.AIT
Visvesvaraya
Technological Univesrity,
Belagavi, Bengaluru India

Ganga Holi
Dept. of ISE, GAT
Visvesvaraya
Technological Univesrity,
Belagavi, Bengaluru India

Srikanta Murthy K.
Dept. of CSE, NCET
Visvesvaraya
Technological Univesrity,
Belagavi, Bengaluru India

ABSTRACT

Today, the world is going to be digitalized in all the ways. Every business units, government and private sectors, research units are using the digital image as transferring mode for every critical data. These images over the internet which will not be secure. Therefore there is a need of image security. Currently, there exists various image security techniques like encryption, watermarking, steganography, etc. This paper discusses the basic image security techniques, the survey of the recent research in the field of image securities like ANN Based Approach, Genetic Algorithm Based Approach, DCT based approach, chaos-based approach, SVD based approach, Steganographic based approach, DWT based approach, visual cryptography based approach, watermarking based approach. The paper provides the future scope of image security.

Keywords

ANN, Chaos method, DCT, Digital signature, DWT, Genetic algorithm, Image Processing, Image security.

1. INTRODUCTION

The image is most widely used communication mode in the different areas like medical area, research area, business area, military area, etc. The important image transfer will takes place over an unsecured Internet network. Thus there is need of proper security for the image to avoid the unauthorized person's access the important information. The advantage of the image is that it covers more multimedia data, and it needs protection [1]. The cryptography is a kind of image security method; that offers the secure transmission and storage method for the image over the internet. Security is the major concern for any system to maintain the integrity, confidentiality and image authenticity. Although the cryptography is the effective method but it also faces the problem in providing the security if the data with grayscale is more [2].

In today's rapid growth of digital communication and electronic data exchange, many of us communicate in cyber space without thinking about the security of the same. The need for exchanging a lot of our private information and secrets in cyberspace. In today's highly computerized and interconnected world, the security of digital image/video has become increasingly more significant in applications such as pay-per-view TV, confidential video conferencing, medical imaging and in industrial or military imaging systems, online transactions, passwords, digital signatures legal’s, etc. These applications need to control access to images and provide the means to verify the integrity of images. In many cases,

such information leakage seriously invades personal privacy, example: the malicious spread of photos in personal online albums or patients' medical diagnosis images, and further more it may cause uncountable losses for a company or a nation, e.g. a secret product design for a company or a governmental classified scanned document. However, such convenience could also be used by malicious/unauthorized users to spread the image information rapidly that it may cause uncountable losses for the owner.

The encryption for an image is performed to achieve the secure image transmission over the internet. The encryption mechanism is widely used in many areas like image/video transmission, medical image transmission over the insecure network by which the protection against the unauthorized access can be provided. The encryption also has its applicability in military communication and tele-medication. Even the future point of view the encryption has more scope. In the case of image security, where the image has huge and a data properties like high redundancy, bulk capability, and high pixel correlation. The techniques used for encryption can be said as the protection tool for secret data. The encryption is the mechanism where the plain data can be converted to cipher or protected data, and it can read only by decrypting it. The reverse process of encryption is known as decryption that uses an encryption key to decrypt the original data. The data encryption has become the most for all the secret data especially using over the internet, extranets or intranets. The encryption is done by applying the mathematical function which generates a key later the key is used to get the encrypted/ciphered data. Again the mathematical key is used to get the original data. The security management is used to have the user’s authentication, accuracy in data security [4]. The image encryption methods can be classified as value transformation, visual transformation, position permutation algorithm. The common encryption mechanisms are Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES), Rivest, Shamir and Adelman (RSA) algorithm, and the Scalable encryption algorithm (SEA) and International Data Encryption Algorithm (IDEA). These mechanisms are widely used for images, videos, etc.

This paper discusses the survey over the image security techniques. The organized sections of the paper are: Section 2 describes the image processing and applications of image processing. Section 3 describes the security issues and existing image security methods. Section 4 discusses the existing research work in image security from ANN Based Approach, Genetic Algorithm Based Approach, DCT based approach, chaos-based approach, SVD based approach, Steganographic based approach, DWT based approach, visual cryptography based approach, watermarking based approach and Digital Signature based approach. Section 5 discusses the research gap,and illustrates the scope of future research and Section 6 gives the conclusion, Section 7 references.

2. IMAGE APPLICATIONS

The recent feasibility of much computer-based technologies has brought multimedia data transformation over the internet. The multimedia data can be included with image or video or audio or graphical objects that contain much important information's of organizations, governments, hospitals. Among the many multimedia, the data image is widely used for many aspects of military, hospital, etc.

2.1 Necessity for image security

Today, various people utilize the distinctive applications to image data transfer. By far most of the people use their images for various customers using the social application. The attack on these social applications can copy or hack the important data. For better usage of these applications, users are using it on their mobiles, tablets, etc. The protection against the hacking attacks on those web or available is plans, there exist distinctive data security framework for multimedia data. These present security frameworks are either using encryption or steganography, or the combination of both. There is diverse securable image encryption that can be especially for protection against the unauthorized access. A transferred over the internet having important data of military, security associations, social or adaptable applications. Hence the image security is necessary. The commonly used security mechanisms are DFT, DCT, DWT, etc.

The transfer of the image over the unsecured network will pose following attacks such as active and passive attacks.

Active attacks: This consists of few data stream modification or false data stream creation.

Passive attacks: This attack uses the data but not affect the system resources [5, 6].

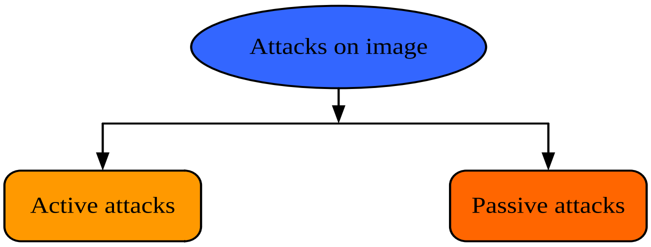

Figure.1 Attacks on image data

2.2 Performance Parameters of Encryption Technique

There exist some parameters that help in the evaluation of encryption technique performance [7].

2.2.1 *Encryption Ratio (ER)*

This measures the amount of data which need to be encrypted. ER needs to be less as to optimize the computational complexity.

2.2.2 *Speed (S)*

The speed of the encryption and decryption is much needed in real time applications.

2.2.3 *Visual Degradation (VD)*

Measures the image data perceptual distortion on the plain image. For some applications, VR needs to be achieved, so that no one can attack or access it but prefer to pay to access the unencrypted content. For the sensitive data, high VR is must disguise the visual content.

2.2.4 *Format Compliance (FC)*

In this a encrypted bit stream will be decoded without decryption.

2.2.5 *Cryptographic Security (CS):*

This defines encryption scheme necessity against brute force and plaintext-cipher text attack. It is really important for highly valuable multimedia application to satisfy cryptographic security.

2.2.6 *Compression Friendliness (CF):*

In encryption scheme is considered compression friendly if it has no or very little impact on data compression efficiency. Some encryption schemes impact data compressibility or introduce additional data that is necessary for decryption. It is desirable that size of encrypted data should not increase.

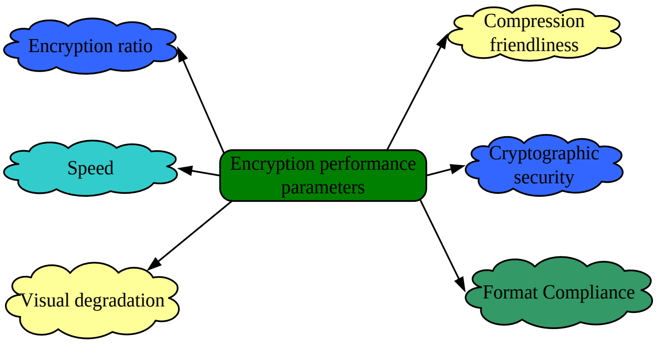

Figure 2.Encryption performance parameters

2.3 Different image encryption methods

The encryption methods are discussed as below [8].

2.3.1 *Cryptography:*

Image encryption (IE) algorithms attempt to convert original images to other images so that they are difficult to understand to keep the image confidentiality between users. The process of coding and transformation of plain text using a digital key into the unreadable format is called encryption; while the process of decoding and converting the unreadable text to readable information using a unique digital key is called decryption. Plain Text is an image that a sender wishes to transmit to a receiver, on which encryption process is applied. The cipher text is the result of encryption performed on plaintext using an algorithm, i.e. encrypted image.

2.3.2 *Secret Key Cryptography:*

This kind of cryptography adopts the single key for encryption in which the sender can encrypt the message with this key and in receiving end the receiver will decrypt the message using the same key.

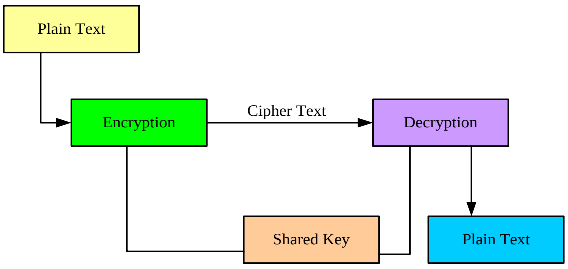

Figure.3.Secret key cryptography.

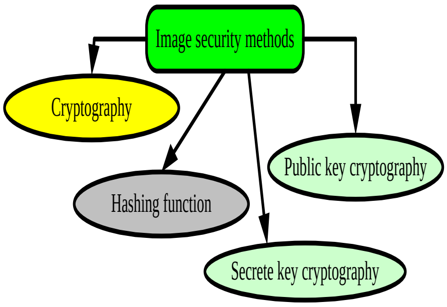

Figure.4 Image encryption methods

2.3.3 Public Key Cryptograph (PKC)

The kind of cryptographic mechanism that contrains two different types of key cryptosystems which are used to build a secure data communication among the sender and reciver over a unprotected network. In PKC a list of keys are used for encryption and hence it can also be considered as Asymmetric cryptosystem. In this there will be public and private key that can be used for public and private communication.

2.3.4 Hash Functions (HFs)

The HFs can be implemented to check the message integrity to make sure that the message is not modified, affected with the virus. The image is also an important part of our information Therefore it's very important to protect our image from unauthorized access.

2.4 Cryptography methods:

The cryptographic methods are classified as shown in figure.5. [9, 10].

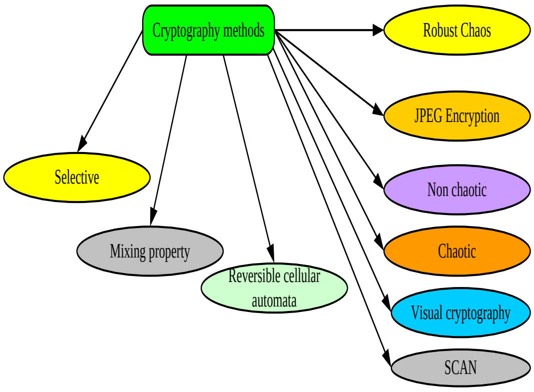

Figure.5 Cryptography methods

2.4.1 Optical Encryption

This kind of encryption group will use an optical instrument to attain the image encryption by randomizing the frequency components of image.

2.4.2 Selective Encryption

The kind of digital image encryption mechanism used to avoid the entire bits encryption. It chooses only selected bits for encryption.

2.4.3 Mixing property

It exhibits the diffusion property. If a set of possible plaintexts has an initial region in the phase space of the map (transformation), then it is the mixing property that implies scattering out of the influence of a single plaintext digit over many ciphers text digits.

2.4.4 Reversible Cellular Automata Based Encryption (RCAE):

This a type of cellular automata having specially constructed rules for reversible usage. The bit key size in this algorithm is 224 bit.

2.4.4 Robust chaos

This an efficient encryption mechanism has wide sigficance for the single key digits on cipher text digits. In this these keys will represent the encryption algorithm parameters hence these parameters are need to handled carefully along with the variables.

2.4.5 JPEG Encryption

This a encryption mechanism which was developed for JPEG 2000 format images. This method achieves multilevel encryption and a computational complexity can be reduced.

2.4.6 Non-chaotic Encryption (NCE)

A Sudoku matrix based encryptiom mechanism is called as NCE. In this Sudoku matrix can be represented as same column or row not two digits. The encryption mechanism is processd as Sudoku matrix generation for scrambling, replacement of image pixel iuntensity with Sudoku matrix and finally mapping process is applied for suffling of pixel positions.

2.4.7 Chaotic Encryption (CE)

This is a highly sensitive encryption mechanism in which high sensitivitive initial values, mixing poperties are exist. This mechanism also offers the periodicity in the encryption.

2.4.8 Visual Cryptography

This type of cryptographic mechanism uses ther human vision interpretation for image decryption and hence it doesniot need any cryptographic concepts and knowledge of complex computation. This privides the security in such away that no hacker can get any hint of encrypted image.

2.4.9 SCAN pattern (SCANP) based encryption

This kind of encryption was presented for the gray scale images that offers lossless compression. In this scan patter can be initialized by SCAN method which is a 2D spatial accessing method.

3. LITERATURE REVIEW

The Security is a major task for all the network environrnments.Image is one of the resource of sending information in all fields like medical image processing,networking,and in cloud environrnment also.

The following section lists some of the image security techniques.

Suthar et al. [11] introduced an image security method in frequency domain known as mixed hybrid scheme. The method is used to detect the image tamper and also maintains image quality. The experimental results of the scheme represent that method is robust against the different attacks.

The proposed algorithm performs encryption of host image by having a combination of 2D Discrete wavelet transform(DWT) , mid band -Discrete cosine transform and a secret key.

A method of image watermarking of the image is presented in Solorio et al. [12]. The stepwise implementation of the method is mentioned as:

- Localization of the tampered pixels blocks.
- Estimation of the five significant bits from the tampered image pixels.

The method is demonstrated that restoration is achieved by the presented method.

Private Key encryption based network security is discussed in Abusukhon and Talib [13]. The method is described for data encryption among the text file transformation among the server and client machines. The possible key for the permutation helps in analysis of the algorithm.

The immune system based segmentation algorithm for infrared images is discussed in Fu et al. [14]. A novel method is presented by the combination of segmentation and clonal selection algorithm to mitigate the segmentation thresholds.

A study on Residue Number System (RNS) and Data Encryption Standard (DES) based reversible watermarking method for image security is discussed in Singh et al. [15]. In authors work secret image was passed to the simple-DES based on key image and at last the encrypted image is obtained with the position matrix and watermark image. Later the watermarked image was subjected to RNS that gives the fully encrypted image. The decoding of the image is done by reversible watermarking.

Gupta et al. [16] illustrated an Embedded Zero tree Wavelet (EZW) compression and Chaos-based image security method. The EZW based method was used to achieve image security with compression while the Chaos method offers robustness in security along with mixing property. The EZW sequence is subjected to 2D data conversion and scrambling by Chaos method. The method out forms the more security.

An active and passive approach is presented in Yanyan et al. [17] to provide security protection for remote sensing images. A high quality of content protection mechanism was adapted to secure, store and transmission purpose. The encrypted image can be decrypted with the key.

The first stage of the proposed method is dividing the image into several subblocks,and search fingerprinting areas which effects the image with less quality.Then apply DCT transformation to every blocks followed by encryption of DCT coefficients using content encryption scheme**.**

A concept of data hiding mechanism is introduced in the Mohan et al. [18] to enhance the image security. The data hiding concept will offer the security and also recover the image with the efficient quality. In the concept of hiding will hide the some portion of the image and encrypt with the key. The hiding concept used in this is reversible that has got the higher capacity of data hiding.

The content owner side image is encrypted by chaotic transposition algorithm.As a second level security data hider then hides some data into the encrypted image based on histogram modification by data hiding key.At the receiver end he needs two keys for decrypting it.

A recursive cellular automata substitution and parallelization concept approached in Zefreh et al. [19]. The method is efficient in test analysis and computational aspects. The method was adopted for half portion of the image to encrypt the image while the half portion of the image mutually. The simulation results of the image concluded that performance in image security is improved.

This method is based on 2-D von Neumann Cellular Automata ,where the encryption is based on the replacement of the pixel values using a recursive CA substitution.

The related study for medical image security is carried out in Naveen et al. [20] by using the EZW and Chaos mechanism. The security for the digital medical data is much necessary as these data is transmitted among the hospitals and also for health insurance sectors. The enhancement in security by Chaos approach is more useful. By using the EZW approach, the 2D output sequence was converted to 2D and later chaos based scrambling mechanism is implemented in column and row manner. The method out forms with compression and extra security for the image.

Pandey and Srivastava [21] described a mechanism of image security in the virtual machine. The security was based on the encapsulated mobile agent (EMA). By using the BAN, logic representation is used to verify the methods efficiency.

An investigation of automata designs usage in health image security system was carried in Mitra [22]. A survey over the cellular automata based image encryption mechanism in health system was performed. Later the tent map and cellular automata combination were presented for image data encryption.

An image security and image authentication for the color image is presented in Shefali and Despande [23] known as the Self-embedding mechanism. The method was of Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) combination which simulates the extra security.

This method is used for color images.The technique first converts the host image into YIQ color space followed DCT and DWT transforms.

The Reversible was watermarking, and Arnold's Cat Map approach is presented in Umamageswari and Suresh [24] to provide the security for medical image transmission. In this region of interest and region of noninterest was defined with JPEG 2000 algorithm. The method provides the most secure mechanism in medical image security.

Another medical image security concept is discussed in Nabiyev et al. [25]. The survey the method medical image data during the data transmission and also rendered different watermarking techniques.

Existing methods and its research work:

This section significantly explains the important methods for image security and recent work on it.

3.1 ANN Based Approach

The simplified biological neuron system is known as an Artificial neural network, Which is connected with the wide range of neurones that processes the elements of brain nerves.ANNs are massively parallel adaptive networks mainly used to abstract and model some of the human nervous system functionality in an attempt capture some of its computational strengths partially. A neural network consists of components like activation state vector, activity aggregation rule, neurons, a pattern of connectivity, activation rule, signal function, learning rule and environment. ANNs are considered for the high computational rate environment.

Priego et al. [26] presented the security system and Hyper spectral Waterway is known as Hywacoss based on artificial neural network approach in the year 2011. The method was tested on real-time boats and ships image and provides the efficient validation.

Kishore et al. [27] have significantly explained the ANN and watermarking based image security in wavelet domain. The experiments are performed under Magnetic Resonance Imaging (MRI), Computer Tomography (CT) and Ultrasound imagery (US). The method is efficient for applicability in telemedicine.

3.2 Genetic Algorithm Based Approach:

Genetic algorithms (GA) are the significant unbiased optimization techniques used to sample the large solution space. The unbiased stochastic sampling, can be used in quick adaption in image processing applications. GAs used for image segmentation, classification, enhancement, feature extraction and image generation.

The recent research over the operation of the genetic algorithm is expressed in Pareek and Patidar [28] for the protection of grayscale medical image. The encryption from this method has drawn significant results for protection against differential attack, entropy attack, plaintext attack and brute-force attack.

A genetic algorithm based image steganography mechanism having the image quality tunability and high embedding ability is described in Kanan and Nazeri [29]. The method has got better embedding and PSNR results for the stego images.

3.3 DCT based approach

A discrete cosine transform (DCT) will have basic set of vectors known as sampled cosine function. The DCT method of converting a signal into elementary frequency components. DCT is applicable for image compression.

A DCT based wavelet realization induced adaptive impairing algorithm is presented in Li et al. [30]. In this, image model is described. The DCT-Haar algorithm is used to reduce the impulsive noise and performs the filling operation of missing data. Saad et al. [31] are introduced a DCT domain based image quality assessment. The features of the test image are extracted and image quality is improved. The method is tested over the LIVE IQA database.

3.4 Chaos-based approach:

The chaos based cryptographic algorithms have advised some new and efficient ways to develop secure data encryption techniques. The chaos encoding (CE) is a smart, sensible mechanism due to its ability of security, speed, complexity, cheap process overheads and process power etc.

The combined study of the Wang and Wang [32] states the image encryption based Chaos method with S-boxes construction. In this method, the plain image is divided into pixels of S-boxes. The method resists the differential attacks and plaintext attacks. The process was analyzed for 256 gray scale images.

In the work of Enayatifar et al. [33], the image encryption technology evaluations are description studied. Later a hybrid mechanism of DNA was presented with the logistic map and genetic algorithm. The experiments carried on the plain images shows that the proposed methods offers proper encryption and also restricts different attacks.

3.5 SVD based approach

This is a reliable and robust orthogonal matrix decomposition method. SVD is an attractive algebraic transform for image processing and has imaging properties. Even the SVD properties are completely used for image processing, still more research is needed. The properties of SVDs like solving of least squares problem, maximum energy packing, multivariate analysis and computing pseudo inverse of a matrix are helpful for an image.

An SVD domain based Gaussian noise level estimation for the images is discussed in Liu and Lin [34]. The work performed the noise level estimation for noise corrupted images. The mechanism can be implemented over the visual signals that overcome the issues of the noise estimation. From the experimental results, it was said that the method is reliable over the wide range of the visual signals.

Bhandari and Kumar [35] presented the Cuckoo search algorithm based satellite image contrast and brightness enhancement using DWT-SVD. In this, input image will be decomposed as four different standards by DWT while the CS algorithm is used to optimize every sub-bands of DWT. Flowingly the low threshold subband image singular matrix was obtained. The enhanced image of is reconstructed by IDWT. The proposed method got significant PSNR value.

3.6 Steganographic based approach:

This is used to hide the secret information in digital media so that only the sender and receiver can understand not from others. Recently, many data hiding mechanisms are developed for binary images which can be used to authenticate digitally stored handwritings, signatures, CAD graphs, and so on.

Fridrich and Kodovsky [36] described the digital images steganalysis by rich models. Steganalysis built around rich image models combined with ensemble classifiers is a promising direction towards automatic steganalysis for a wide spectrum of steganographic schemes.

In Feng et al. [37] Distortion reduction over the texture mechanism is presented to secure the steganographic image. From the image, mirroring-invariant local texture patterns, rotation and complement are extracted. From the comparative analysis over the constructed image and binary image, it has been said that binary based method is efficient.

3.7 Visual cryptography based approach:

This is a most secure kind of cryptography for a multimedia and are widely used for image files. But the embedding data into image changes its color frequencies in a predictable way.

An advanced visual cryptography is explained in Lee and Chiu [38] for General access structure. The conventional secret schemes of the images will generate the random pixels to hide the secret images. To solve this issue, an extended visual cryptography is presented.

Similar work is performed by Askari et al. [39], but for halftone images that too without expansion of pixels. The perfect security is maintained in this method.

3.8 Watermark approches:

This approach is used for broadcast monitoring Source tracking, copyright protection, etc. Currently the copyright protection of digital content is a major issue and Watermarking is the solution for it. Digital Watermarking is divided as visible and invisible watermarking.

The perceptible or visible watermarks can be viewed with normal eye including company logos, bills, TV channel logos etc. While the imperceptible or invisible watermarks requires mathematical calculations and are cannot be viewed with normal eye.

Curvelet Transformation can be classified as:

1. Using Wrapping method and
2. Using Fast Fourier Transformation algorithm.

The double transform based watermarking technique for the digital image scrambling is described in Wang and Li [40]. In this band pass of curvelet transform is introduced and hence a curvelet and visual system based mechanism are presented. The method has outcome with the significant against the noise adding, cropping, rotating & altering. Similarly significant against the noise adding, cropping, rotating & altering was presented for counter let domain in Sadeazami et al. [41], in which the author first investigated the counter let coefficients modeling with alpha stable distribution.

3.9 Discrete Wavelet Transform (DWT) based approach:

This is a kind of sub-band coding and found to yield a fast computation of Wavelet Transform. DCT is easy to implement and computation time optimimzation.

In Baviskar et al. [42] presented the Image fusion mechanism for security enhancement with the DWT subband exchange. The method offers reduced bandwidth utilization and less transmission time as it converts colored images to compressed textured gray-scale images. Also image fusion technique and compression scheme were explained in detail.

Mulla et al. [43] discussed the Shuffling approach for DWT-based image compression mechanism. In this colored image is converted to textured image that brings image compression. The performance evaluation of the proposed method is analyzed with plots of MSE, PSNR and security probability.

4 SUMMARY OF THE RECENT WORK

The summary of existing works from section III and IV are tabled in table 1.

Table.1 Summary of literature review

Authors	Work	Tool used	Remark
Suthar et al. [11]	Image security method of frequency domain	Watermarking	Robust against the different attacks
Solorio et al. [12]	Image watermarking based security	Watermarking	Restoration is achieved
Abusukhon and Talib [13]	Private Key encryption based network security	Private Key encryption	The possible key for the permutation helps in analysis of the algorithm
Fu et al. [14]	An immune system based segmentation algorithm for infrared images	Segmentation algorithm	Mitigates the segmentation thresholds
Singh et al. [15]	Residue Number System (RNS) and Data Encryption Standard (DES) based reversible watermarking method for image security	Residue Number System (RNS) and Data Encryption Standard (DES)	The watermarked image was subjected to RNS that gives the fully encrypted image. The decoding of the image is done by reversible watermarking
Gupta et al. [16]	EZW compression and Chaos-based image security method	EZW and Chaos	The EZW sequence is subjected to 2D data conversion and scrambling by Chaos method. The method out forms the more security
Yanyan et al. [17]	Active and passive approach remote sensing images security protection.	Active and passive approach	Succeeded in providing the security for remote sensing images

Table.1. Summary of literature review (Continued.)

Authors	Work	Tool used	Remark
Mohan et al. [18]	A concept of data hiding mechanism for image security enhancement.	Data hiding	Hide the some portion of the image and encrypt with the key. The hiding concept used in this is reversible that has got higher capacity of data hiding
Zefreh et al. [19]	A recursive cellular automata substitution and parallelization concept	Recursive cellular automata substitution and parallelization	Performance in image security is improved
Naveen et al. [20]	The related study for medical image security	EZW and Chaos mechanism	Out forms with compression and extra security for the image
Pandey and Srivastava [21]	A mechanism of image	Encapsulated mobile agent	The BAN logic representatio

	security in virtual machine	(EMA)	n is used to verify the methods efficiency
Mitra [22]	An investigation of automata designs usage in health image security system	Survey, tent map and cellular automata	Tent map and cellular automata combination were presented for image data encryption
Shefali and Despande [23]	An image security and image authentication for color image	Survey	Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT)
Umamageswari and Suresh [24]	The Reversible watermarking and Arnold's Cat Map approach for medical images	Reversible watermarking and Arnold's Cat map approach	The more secure mechanism in medical the image security
Nabiyev et al. [25]	Medical image security concept	Survey	Discussed many watermarking concepts.
Priego et al. [26]	Security system and Hyper spectral Waterway is known as Hywacoss based on artificial neural network approach for images	Hywacoss based on artificial neural network	Method was tested on real-time boats and ships image and provides the efficient validation
Kishore et al. [27]	The ANN and watermarking based image security in wavelet the domain	Watermarking and ANN	Efficient for applicability in tele-medicine
Pareek and Patidar [28]	The operation of genetic algorithm for protection of gray scale medical image	Genetic algorithm	Protection against differential attack, entropy attack, plaintext attack and brute-force attack

Table.1. Summary of literature review (Continued.)

Authors	Work	Tool used	Remark
Pareek and Patidar [28]	The operation of genetic algorithm for protection of gray scale medical image	Genetic algorithm	Protection against differential attack, entropy attack, plaintext attack and brute-force attack
Kanan and Nazeri [29]	A genetic algorithm based image stegnography mechanism having the image quality tunability and high embedding ability	Genetic algorithm based image stegnography mechanism	Better embedding and PSNR results for the stego images
Li et al. [30]	A DCT based wavelet realization induced adaptive impairing algorithm for image model	DCT-Haar algorithm	The DCT-Haar algorithm was used to reduce the impulsive noise and performs the filling operation of missing data
Saad et al. [31]	DCT domain based image quality assessment	DCT	The features of the test image are extracted and image quality was improved. The method was tested over the LIVE IQA database
Wang and Wang [32]	The image encryption based Chaos method with S-boxes construction	Chaos method	The process was analyzed for 256 grey scale images
Enayatifar et al. [33]	The image encryption technology evaluations are description studied	Logistic map and genetic algorithm	The experiments carried on the plain images shows that the proposed methods offers proper encryption and also restricts different attacks.
Liu and Lin [34]	A SVD domain based Gausian noise level estimation for the images	SVD domain	The method is reliable over the wide range of the visual signals

Bhandari and Kumar [35]	Cuckoo search (CS) algorithm based satellite image contrast and brightness enhancement by DWT-SVD	CS and SVD	The proposed method got significant PSNR value
Fridrich and Kodovsky [36]	The digital images steganalysis by rich models	Steganalysis	Promising direction towards automatic steganalysis for a wide spectrum of steganographic schemes.
Feng et al. [37]	Distortion reduction over the texture mechanism to secure the steganographic image	Texture mechanism	From the comparative analysis over the constructed image and binary image it has been said that binary based method is efficient

Table.1. Summary of literature review (Continued.)

Authors	Work	Tool used	Remark
Lee and Chiu [38]	An advanced visual cryptography	Visual cryptography	Better image hiding process
Askari et al. [39]	visual cryptography for Halftone images	Visual cryptography	Perfect security maintained
Wang and Li [40]	The double transform based watermarking technique for the digital image scrambling	Watermarking	Significant against the noise adding, cropping, rotating & altering in images.
Sadeazami et al. [41]	Significant against the noise adding, cropping, rotating & altering	Watermarking	Investigated the counter let coefficients modeling with alpha stable distribution
Baviskar et al. [42]	Image fusion mechanism for security enhancement with the DWT sub band exchange	DWT	Reduced bandwidth utilization and less transmission time
Mulla et al. [43]	Shuffling approach for DWT-based image compression mechanism	DWT	The performance evaluation of the proposed method is analyzed with plots of MSE, PSNR and security probability

5 RESEARCH GAP AND FUTURE WORK

From the survey of the recent researches it has been said that the security is the major concern in image transmission. The security issue is increasing rapidly with developed tools for hacking the image data. Many researches proposed solutions for the security issue but they were failed to get complete security over the insecure network.

6 FUTURE WORK

In future the study can be carried as followed:

- A test bed can be designed by considering the adversarial module (considering differential attack) and client module possession of confidential data over the network.
- A cryptographic framework can be designed for simple operation of image verification.
- A mathematical operation can be performed such as recurrence relation and polynomial mapping for building the robustness in security.
- An evolutionary algorithm can be used to bring the potentiality in cryptographic process.

7 CONCLUSION

This paper presents the survey over various techniques of image security and literatures of existing research work. Currently image is most widely used communication mode in different areas medical area, research area, business area, military area etc. The important image transfer will take place over the unsecure internet network. Hence Security is the major concern for any system to maintain the integrity, confidentiality and image authenticity. Although the cryptography is the effective method but it also face the problem in providing the security if the data in the image is more. This paper discussed the Necessity for image security, Encryption performance parameters, image encryption methods, Cryptography methods and important methods for image security and recent work on it. The study analysis of the existing research work helped in defining the research gap and providing the future research line for image security even better.

8 REFERENCES

[1] Perse, Elizabeth M., and John A. Courtright. "Normative images of communication media mass and interpersonal channels in the new media environment." Human communication research 19.4 (1993): 485-503.

[2] Calabrese, Thomas. Information security intelligence: Cryptographic principles and applications. Cengage Learning, 2004.

[3] Lam, Ieng-Fat, Kuan-Ta Chen, and Ling-Jyh Chen. "Involuntary information leakage in social network services." International Workshop on Security. Springer Berlin Heidelberg, 2008.

[4] Zhang, Bo. XOR based optical encryption with noise performance modeling and application to image transmission over wireless IP lan. Diss. 2004.

[5] Hill, Douglas W., and James T. Lynn. "Adaptive system and method for responding to computer network security attacks." U.S. Patent No. 6,088,804. 11 Jul. 2000.

[6] Kaufman, Charlie, Radia Perlman, and Mike Speciner. Network security: private communication in a public world. Prentice Hall Press, 2002.

[7] Spanos, George Anastasios, and Tracy Bradley Maples. "Performance study of a selective encryption scheme for the security of networked, real-time video." Computer Communications and Networks, 1995. Proceedings., Fourth International Conference on. IEEE, 1995.

[8] Alfalou, Ayman, and C. Brosseau. "Optical image compression and encryption methods." Advances in Optics and Photonics 1.3 (2009): 589-636.

[9] Kenneth H Rosen. Cryptography: theory and practice. CRC press, 2005.

[10] Denning, Dorothy E. "Cryptography and data security." (1982).

[11] Anil C. Suthar1, Chiragkumar B. Patel2, and Gopal R. Kulkarni3, “Simulation and implementation novel hybrid blind method of image security. InCommunication and Computing (ARTCom2012), Fourth International Conference on Advances in Recent Technologies, pp. 202-205, 2012

[12] S. B-Solorio, C.T. Li, & A.K. Nandi, “Watermarking method with exact self-propagating restoration capabilities”, In IEEE International Workshop on Information Forensics and Security (WIFS), pp. 217-222, 2012

[13] A. Abusukhon, and M. Talib, “A Novel network security algorithm based on Private Key Encryption. In Cyber Security”, Cyber Warfare and Digital Forensic (CyberSec), International Conference, pp. 33-37, 2012

[14] D. Fu, X. Yu, & T.Wang, “Segmentation algorithm study for infrared images with occluded target based on artificial immune system”, In Computational Intelligence and Security (CIS), Eighth International Conference on (pp. 350-353, 2012

[15] S.K. Singh, V.P. Gopi, and P. Palanisamy, “Image security using DES and RNS with reversible watermarking”, In Electronics and Communication Systems (ICECS), International Conference, pp. 1-5, 2014.

[16] T. Gupta, V. Sainath, C. Naveen, V. R. Satpute, and A. S. Gandhi, “Image security using chaos and EZW compression”, In Engineering and Systems (SCES), Students Conference, pp. 1-6, 2014.

[17] X. Yanyan, Z. Yuxia, and X. Zhengquan, “An Active-Passive Security Protection Method for Remote Sensing Image”, In Network Computing and Information Security (NCIS), International Conference on (Vol. 1, pp. 30-34), 2011

[18] A.K. Mohan, M.R. Saranya, & K. Anusudha, :An algorithm for enhanced image security with reversible data hiding. InContemporary Computing and Informatics (IC3I), 2014 International Conference, (pp. 1042-1045), 2014

[19] E.Z. Zefreh, S. Rajaee, S. and M. Farivary, “Image security system using recursive Cellular automata substitution and its parallelization”, In Computer Science and Software Engineering (CSSE), 2011 CSI International Symposium, (pp. 77-86), 2011

[20] C. Naveen, T. V. S. Gupta, V. R. Satpute, and A. S. Gandhi, "A simple and efficient approach for medical image security using chaos on EZW", In Advances in Pattern Recognition (ICAPR), 2015 Eighth International Conference, pp. 1-6, 2015.

[21] A. Pandey, and S. Srivastava, "An approach for virtual machine image security", In Signal Propagation and Computer Technology (ICSPCT), 2014 International Conference, pp. 616-623. IEEE, 2014.

[22] A. Mitra, "Investigating scopes for automata based designs targeting image security in health system," E-Health and Bioengineering Conference (EHB), pp. 1-4, 2015.

[23] S. Shefali and S. M. Deshapande, "Self embedding technique for digital color image authentication and security," 2007 International Conference on Industrial and Information Systems, Penadeniya, pp. 147-152, 2007

[24] A. Umamageswari, G.R.Suresh, “Security in Medical Image Communication with Arnold's Cat map method and Reversible Wa term arking”, International Conference on Circuits, Power and Computing Technologies, 2013

[25] V.V. Nabıyev, M. Ulutaş, and G. Ulutaş, “Secret Sharing Scheme to implement medical image security”, In 2010 IEEE 18th Signal Processing and Communications Applications Conference, pp. 820-823, 2010.

[26] B. Priego, D. Souto, F. L. Peña, and R. J. Duro, "An ANN based hyperspectral waterway control and security system", In 2011 IEEE International Conference on Computational Intelligence for Measurement Systems and Applications (CIMSA) Proceedings, pp. 1-6, 2011

[27] P.V.V. Kishore, K. S. Prajwal, M. K. Mohan, and S. Koteswarao, “Medical image watermarking with ANN in wavelet domain”, In Electronics, Computing and Communication Technologies (CONECCT), 2015 IEEE International Conference, pp. 1-6, 2015.

[28] N.K. Pareek, and V. Patidar, “Medical image protection using genetic algorithm operations”, Soft Computing, Vol. 20(2), pp.763-772, 2016.

[29] H.R. Kanan, and B. Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm", Expert Systems with Applications, Vol. 41, No. 14, pp. 6123-6130, 2014

[30] Y-R. Li, L. Shen, and B.W. Suter, “Adaptive inpainting algorithm based on DCT induced wavelet regularization”, IEEE Transactions on Image Processing, Vol. 22, No. 2, pp.752-763, 2013.

[31] M.A. Saad, A. C. Bovik, and C. Charrier, “Blind image quality assessment: A natural scene statistics approach in the DCT domain”, IEEE Transactions on Image Processing, Vol. 21, No. 8 pp.3339-3352, 2012.

[32] X. Wang, and Q. Wang, “A novel image encryption algorithm based on dynamic S-boxes constructed by chaos”, Nonlinear Dynamics, Vol. 75, No. 3, pp.567-576, 2014

[33] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, “Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence”, Optics and Lasers in Engineering, Vol. 56, pp. 83-93, 2014.

[34] W. Liu, Wei, and Weisi Lin. "Additive white Gaussian noise level estimation in SVD domain for images." IEEE Transactions on Image Processing 22, no. 3 (2013): 872-883.

[35] A.K. Bhandari, V. Soni, A. Kumar, and G. K. Singh, "Cuckoo search algorithm based satellite image contrast and brightness enhancement using DWT–SVD", ISA transactions, Vol. 53, No. 4, pp.1286-1296, 2014

[36] Fridrich, Jessica, and Jan Kodovsky. "Rich models for steganalysis of digital images." IEEE Transactions on Information Forensics and Security 7, no. 3 (2012): 868-882.

[37] B. Feng, W. Lu, and W. Sun, “Secure binary image steganography based on minimizing the distortion on the texture”, IEEE transactions on Information Forensics and Security, Vol. 10, No. 2, pp.243-255, 2015.

[38] N. Askari, H. M. Heys, and C. R. Moloney,"An extended visual cryptography scheme without pixel expansion for halftone images", In Electrical and Computer Engineering (CCECE), 2013 26th Annual IEEE Canadian Conference, pp. 1-6, 2013.

[39] N. Askari, H.M. Heys, and C.R. Moloney,”An Extended visual Cryptogrpahy Scheme without pixel expansion for halftone images” IEEE 2013

[40] Wang, and H. Li, “A Novel Scrambling Digital Image Watermark Algorithm Based on Double Transform Domains”, Mathematical Problems in Engineering, 2015.

[41] H. Sadreazami, M. O. Ahmad, and M. N. S. Swamy, “A study of multiplicative watermark detection in the contourlet domain using alpha-stable distributions”, IEEE Transactions on Image Processing, Vol. 23, No. 10, pp. 4348-4360, 2014

[42] J. Baviskar, A. Mulla, N. Kudu, A. Parthsarathy, and A. Baviskar, “Sub-band exchange DWT based image fusion algorithm for enhanced security”, In Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference, pp. 534-539, 2014.

[43] A. Mulla, J. Baviskar, S. Wagh, N. Kudu, and A. Baviskar, “Probabilistic triangular shuffling approach in DWT based image compression scheme”, In Communication, Information & Computing Technology (ICCICT), International Conference, pp. 1-6,2015.