Asian Journal of Applied Science and Technology (AJAST)
(Peer Reviewed Quarterly International Journal) Volume 3, Issue 3, Pages 101-108, July-September 2019

Analysis of Various Image Encryption Techniques for Enhancing Image Security

Praseeja V S[1] & VR. Nagarajan[2]

[1]*Research scholar, Department of Computer Science, Sree Narayana Guru College, Coimbatore - 641 105.*
[2]*Assistant Professor, Department of Computer Application and Information Technology, Sree Narayana Guru College, Coimbatore - 641 105.*

Article Received: 29 January 2019 Article Accepted: 15 May 2019 Article Published: 27 July 2019

ABSTRACT

Secure sharing of images in between the varied users needed the development of image cryptography. An economical image cryptography technique is often requisite, such as the users aside from the sharing participant cannot acknowledge the image. At the current time, the protection of transmission information has become a necessary method which might be achieved by cryptography. Basically, such a big amount of totally different techniques are accustomed to shield personal image information from those that lawlessly attempt to have access. Thus, here the technique is often needed to stay information secured and capable. Cryptography provides indispensable techniques for defensive transmission information. Information security plays a crucial role once counsel 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 don't know about transfer of information. In steganography the confidential information is concealed in some other way that the confidential information is undistinguishable. In this work a survey is done based on the image encryption techniques.

Keywords: Cryptography, Steganography, Image Security, Protection.

1. INTRODUCTION

Owing to the regular run of digital images within the world over the printed media, it's become necessary to secure them from unwanted access. Secret writing could be a widespread technique to sustain multimedia system image security in transmission over the net. It's employed in a range of fields together with web communication, medical imaging and military communication, etc. Inspite of inherent options of images like huge information redundancy and mass data capability, the secret writing of images differs from that of texts [8]. Therefore, techniques that are applicable for text information might not be presumably sensible for multimedia system (images, video, etc) information.

With the ever-increasing growth of multimedia system applications, security is a vital issue in communication and storage of images, and secret writing could be a common technique to uphold image security. Image secret writing techniques attempt to convert original image to a different image that's arduous to understand; to stay the image confidential between users, in a different word, it's essential that no-one may get to grasp the content for coding. The method of encrypting plain text messages into ciphertext messages is termed encryption and the reverse method of remodeling cipher text back to plain text is termed as decoding. Image and video secret writing have applications in numerous fields together with web communication, multimedia systems, medical imaging, Tele-medicine, and military communication. Color images are being transmitted and hold on in great amount over the net and wireless networks that cash in of fast development in the multimedia system and network technologies.

In recent years, many color image secret writing approaches are planned. Until now, numerous encoding algorithms are planned and widely used, like AES, RSA or plan most of that are employed in text or binary information [4]. It's tough to use them directly in multimedia system information and inefficient for color image secret writing as a result of high correlation among pixels. For multimedia system information are usually of high redundancy of enormous volumes and need period interactions. The model for image encryption is given in fig.1.

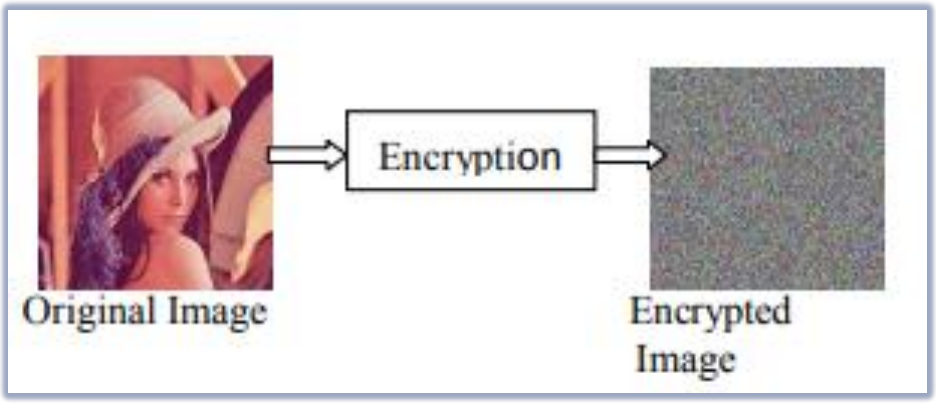

Figure No: 1 Image Encryption

The image encoding is to transmit the image firmly over the network so no unauthorized user will ready to rewrite the image. Image encoding, video encoding, chaos-based encoding have applications in several fields together with web communication, transmission, medical imaging, Tele-medicine and military Communication, etc. The evolution of encoding is moving towards a way forward for endless prospects. The image information has special properties like bulk capability, high redundancy and high correlation among the pixels. Encoding techniques are terribly helpful tools to shield secret information. Encoding is going to be outlined because of the conversion of the plain message into a type known as a ciphertext that can't be browsed by any folks while not decrypting the encrypted text. Decoding is that the reverse method of encoding that is the process of changing the encrypted text into its original plain text, so it is browsing.

Enlarged use in communication of images and data over the web has additionally enhanced the risk of knowledge outpouring. Therefore, need for secure information transmission has up. Cryptography is one mechanism that gives confidentiality of the information and so ensures data security. During this mechanism, the image/data to be sent is remodeled into another type referred to as ciphertext creating it tough for the illegal person to browse. The reverse method of transformation referred to as decoding is administrated at the receiver aspect to recover the plain text. The cryptography mechanisms are generally classified into 2 categories:

- Symmetric key Cryptography: An equivalent key is going to be used for encoding and decoding of images/data.
- Asymmetric key Cryptography: During this mechanism, two kinds of keys are used: Public key (known to all) and Private key (known to the meant user). The sender encrypts the information victimization public key of the destination and also the receiver decrypts it via its non-public key. This mechanism provides far better security as compared to parallel key cryptography however at the value of time quality.

Encryption of information has become a very important to defending data resources, particularly on the web, intranets, and extranets. Encoding is that the method of applying special mathematical algorithms and keys to rework digital information into cipher code before they're transmitted and decoding involves the applying of mathematical algorithms and keys to urge back the first data from cipher code. The most goal of security

management is to supply authentication of users, integrity, accuracy, and safety of information resources. The image encoding algorithmic rules is classified into 4 major groups: (i) cryptographic techniques (ii) steganographic techniques (iii) transformation based algorithm and (iv) chaotic techniques.

2. RELATED WORK

Xingyuan Wangn et al. [1] devised a chaotic technique that uses R, G, B system to vary and cipher the image. The essential plan is to use a chaotic rule that works on the color system. Authors mentioned that ancient cryptographic techniques like DES and RSA are not any longer appropriate for image encoding because the algorithms neglected the correlation between the R, G, B element of images. The combined permutation and combined diffusion stages effectively cut back the correlations between R, G, B elements and enhance the performance of encrypting. The projected rule is going to be ready to work against the resistant of the chosen plain- text/ciphertext attack. Finally, the projected work was performed effectively on the color image that was the disadvantage of the previous technique as they performed simulation on greyscale pictures.

A Mitra et al. [2] delineate a theme for the image encoding by utilizing a mix of distinctive permutation techniques. Essentially the first thought of author is that an image is often seen as a course of action of bits, pixels, and blocks. The correlation linking these bits, pixels, and blocks presents a transparent knowledge of an image. Therefore this recognizable knowledge is often lessened by decreasing the link among the bits, pixels, and blocks by exploiting some permutation technique. A random permutation theme is performed. They need incontestable outcomes with the mix of [block, bit, pixel] permutation one by one. The decoded image is often non-inheritable because of the original image by having a converse permutation solely, instead, they get the jumbled image. At last, they need to be finished up their system, the simplest case state of affairs and aforementioned that any work is going to be attainable with variable length.

Wei-bin et al. [3] projected a secure system for image encoding exploitation Henon chaotic map. To shuffle the link between the first and encrypted image, they applied shuffling on the position of image pixels whereas ever-changing the grey values of pixels. Former the Arnold map is employed to shuffle the positions of the image pixels. Later, they shuffle image picture element by pixel and encoding has been done supported Henon's chaotic system. They additionally mentioned that there's terribly less encoding time for the image encryption as compared to the alternative.

Nidhi Sethi et al. [4] projected a completely unique encoding strategy that has two phases. Within the former part, the input image is remolded by applying a replacement alteration methodology whereas in the later phase Chirikov normal map and increased logistical map are used for shuffling the pixels worth of a picture and diffusion severally. The aim of the increased logistical map is to provide an impulsive series of image pixels. Varied images are accustomed specific to the potency of the projected rule. The demonstration shows that the projected strategy is a method to cover the correlation between the first image and the cipher image. The result's additionally compared with 2 totally different methodologies, haar moving ridge, and quick haar wavelet. Finally, they complete it with the protection of projected work towards attacks.

3. SURVEY OF IMAGE ENCRYPTION TECHNIQUES

3.1 Cryptographic Techniques

A. Data Encryption Standard (DES): It's a bilaterally symmetric block cipher. It's 64-bit block size that uses a 56-bit key. Plaintext of 64-bit block size is employed for input in addition as output mistreatment 64-bit block for ciphertext. DES solely functions on the blocks that are of the same size. Substitution in addition as permutation each operation is performed throughout execution. Same operation is recurrent for sixteen times to provide the ciphertext. Security of information depends upon the operation performed range of times throughout ciphertext generation. DES was replaced by Triple DES (3DES) as a result of its stronger methodology. It primarily encrypts the information 3 times in addition as uses completely different keys with the key size of most 168 bits. It's relatively slow in reference to the latest block cipher [7].

B. AES encryption: It's primarily known as advanced encryption standard. It's a bilaterally symmetric key encryption technique which can replace the unremarkably used data encryption standard (DES). It uses 128-bit blocks. The key lengths supported by cipher are primarily 128, 192, and 256 bits. Because the key sizes will increase, the complexness of the cipher formula additionally will increase.

C. Blowfish: It's additionally a secret writing formula of a bilaterally symmetric kind. It uses a block size of 64-bit and key length varies from thirty-two bits to 448 bits. It additionally uses sixteen round operations and S-box that is vital dependent. It produces a pseudo-random operation table for key programming with the assistance of secret writing. This table generated supported the key provided by the user. This approach is best throughout differential and linear science. It's not applicable once there's a requirement of the memory area.

D. Triple DES: It's an adaptation of data encryption standard. It consists of 56 key bits and eight parity bits with the assistance of 64-bit key. Block size utilized by Triple DES is eight bytes. It performed the secret writing of information in eight bytes chunks. The most reason behind Triple DES formula is to boost the safety level mistreatment 3 completely different keys. It's safer as compared to others however it is terribly slow.

E. RSA algorithm: It was developed by Rivest-Shamir-Adleman. It's the foremost often used public-key formula or asymmetric algorithm. It's used for various functions i.e. secret writing of information in addition as in digital signatures. Resolving of numbers is taken into account as admire security provided by RSA however it's still a question of discussion. Computation performed in RSA with integers modulo n = p * letter wherever p, the letter is 2 huge secret primes numbers. During this approach, secret writing is performed by exponentiated of message m with a little public exponent e. On the opposite hand, decoding is performed with the ciphertext c = ME (mod n) that computes the increasing reversed = e-1 (mod (p-1)*(q-1)). Subsequently cd is obtained by cd = me * d = m (mod n). The non-public key includes the n, p, q, e, d and on the opposite hand public key contains solely n and e to boost the safety level key size ought to be larger than 1024 bits.

F. Diffie-Hellman: It's the primary secret writing formula that uses discrete logarithms in a very restricted field. It permits 2 completely different users to share a secret key over a timid medium no matter the sooner secrets. It's unremarkable formula for the exchange of keys. In numerous cryptography protocols, 2 or a lot of parties attempt to

begin communication. On the opposite hand, it's assumed that at the start they are doing not have any mutual secrecy. The Diffie-Hellman protocol uses the key exchange for the development of the common secret key over insecure communication media. However, hardware model cannot be created.

G. Digital Signature Algorithm: It's a mathematical system that is employed to validate the genuineness and consistency of a message, computer code or digital document. It's not as economical as RSA for signature authentication.

H. ElGamal: It's a public key cipher i.e. asymmetric key secret writing formula is employed for public-key cryptography that relies on the Diffie-Hellman key agreement. ElGamal is the precursor of DSA.

3.2 Steganographic Techniques

The Greek word steganos that means covered writing is behind the idea of steganography. Here it's difficult to even find that a message is being sent. This kind of ciphering is known as steganography. Steganography is that the technique of inserting hidden messages similar to that unauthorized person, except the sender and anticipated receivers will find the presence of the messages. The prime objective of steganography is to hide the key message or data similar to that spyware which is powerless to find it [6]. If spies inaugurate any uncertain information in this case then aim is the consequence. There are varied sorts of information in steganography i.e. text and message, audio and video, etc.

There are numerous sorts of Steganography i.e. Image Steganography, Audio Steganography, Video Steganography, Text files Steganography.

A. Image Steganography: In image steganography, information is hidden within a picture in such some way that the original image remains similar. The common image steganography algorithmic rule is LSB primarily based embedding algorithm.

B. Audio Steganography: Within the audio steganography secret information or data is hidden in an audio, therefore it's referred to as audio steganography. There are many ways to cover secret data in audio i.e. LSB, part writing, etc.

C. Video Steganography: In video steganography technique secret information or data is hidden in a video, therefore it's referred to as video steganography. The video consists of each i.e. image further as audio. Therefore the video steganography will be used for each image further as audio.

D. Text Files Steganography: In-Text files primarily based steganography technique secret information or data is hidden in a text, therefore it's referred to as text files steganography. It primarily needs less area or memory as a result of it solely stores secret information or data within the kind of text. It's quicker than different steganography technique. However, this system is never used as a result of text less contains a great deal of redundant information.

E. Least Significant Bit (LSB): It's primarily the foremost common technique used for concealing the key information or data in any digital media i.e. image, video, audio or could also be text. During this technique, LSB or last little bit of image is replaced by the bit of secret message. Therefore information will be hidden with the

utilization of eight-bit or twenty-four-bit image. Usually, an image having twenty-four-bit size is used for great deal of knowledge. LSB is often used however still it's vulnerable as a result of it will be detected throughout the transmission of knowledge. There are numerous techniques are evolved i.e. increased LSB, Edge LSB and Random LSB.

3.3 Transform Based Encryption Techniques

A. Hartley Transform and gyrator trans-form: During this approach primarily color image is isolated into Red, Green and Blue channels at the moment Hartley transformation is performed severally. Once this all the 3 reworked channels are increased. To get the primary cryptography and cryptography key part and amplitude truncation takes place. With the conjuction of the random part mask, the encoded image is modulated. Then this modulated image is gyrated reworked and at the moment part and amplitude truncated to induce the second encrypted image and second cryptography key.

B. Cascaded Fractional Fourier transform: The original images are primarily separated into 2 part masks throughout the cryptography method. Few masks are modulated into the interim mask then these are encrypted into ciphertext image and on the opposite hand remaining masks are used as cryptography keys. Throughout the truncation part, the asymmetric system will be accustomed into ciphertext. Solely a licensed user will retrieve the information with the assistance of the various part masks. Thus this method has high resistance for varied styles of attacks together with a chosen plaintext attack [8].

C. JTC (joint transform correlator) architecture: It uses part and amplitude truncation technique for a brand new optical cryptosystem. However part and amplitude truncation end up in the asymmetric and it creates the hybrid attack i.e. integration of precise attack on asymmetric cryptosystem and chosen-plaintext attack on joint transform correlator, terribly troublesome. With the assistance of correlation pure mathematics, authentication and verification administered.

3.4 Chaotic Based Encryption Technique

A. Chaotic image coding: The permutation and diffusion structure is utilized by the many spherical based chaotic image encryption techniques. Unambiguously, for the event of the many permutation sequences for several plain images first plaintext feedback technique is embedded within the permutation method at the moment secret key generated dynamically by using plaintext or ciphertext feedback for diffusion. This approach possesses massive key area and it will repel the differential attack [5].

B. 2D-SLMM (two-dimensional sine logistical modulation map): It was derived from the sine and logistic maps. Once it was compared with the chaotic maps that are already existed, then it provides higher randomness, broader chaotic vary, hyper chaotic property and lower implementation price in comparisons to others. A CMT (chaotic magic transformation) technique was planned to alter the element position of the image with efficiency. At the moment each 2nd SLMM and CMT were combined to develop a completely unique image coding formula. It does not solely protect the images with lower time complexness additionally as higher security levels however also revel numerous varieties of attacks. The various encryption techniques are illustrated in table 1.

Encryption Techniques	Time Computation	Key Sensitivity	Pixel Sensitivity	Correlation Analysis
Cryptography	Moderate	Good	Good	Good
Steganography	Good	Excellent	Poor	Moderate
Transform Based	Moderate	Good	Moderate	Good
Chaotic Method	Moderate	Excellent	Excellent	Excellent

Table No: 1 Analysis of Encryption Techniques

All the techniques mentioned in the survey are in the spatial domain. Each technique has some advantages and drawbacks however cryptographic techniques proved to be safer and therefore in future, these is also combined with some frequency-domain technique to additional get higher-end up in terms of increased hardiness against attacks and reduced time quality.

4. CONCLUSION

It's the age of the advancement in technology. All sorts of valuable knowledge primarily communicated with the assistance of the public network. During this work, the Cryptography and Steganography technique are mentioned and sorts the problems in each. The additional cojointly varied cryptography techniques and their performance are mentioned. Every secret writing theme is isolated in its own approach. It's different for various applications. Differing types of activity are thought-about to shield the info from unauthorized users. In this work, numerous image secret writing algorithms are analyzed. Some algorithms are functioning on grayscale image whereas different algorithms are working on R, G, B color system that is that the latest trend and it's the need for image secret writing. These secret writing algorithms are studied and analyzed well underneath the various parameters to push the performance of the encryption strategies conjointly to make sure the protection proceedings. To sum up, all the techniques are helpful for secret writing. Every technique is exclusive in its own approach, which could be appropriate for various applications. The additional work is done that resist other attacks by analyzing the capabilities of algorithms.

REFERENCES

[1] Xingyuan Wangn; LinTeng,XueQin, A novel colour image encryption algorithm based on chaos, Signal Processing 92 (2012) 1101–1108, 2011 Elsevier.

[2] A Mitra; Y. V. Subba Rao; S. R. M. Prasanna,A New Image Encryption Approach using Combinational Permutation Techniques, International Journal of Electrical and Computer Engineering 1:2 2006

[3] Chen Wei-bin; Zhang Xin, Image Encryption Algorithm Based on Henon Chaotic System, 2009 IEEE.

[4] Nidhi Sethi; Sandip Vijay, Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique,Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013).

[5] R. Y. H. Zhao "An Efficient Chaos-based Image Encryption Scheme Using Affine Modular Maps" I. J. Computer Network and Information Security, 2012, 7, 41-50.

[6] Bashardoost, M., Rahim, M. S. M., Altameem, A., & Rehman, A. (2014). A Novel Approach to Enhance the Security of the LSB Image Steganography. Research Journal of Applied Sciences, Engineering and Technology, 7(19), 3957-3963.

[7] S. E. Zoghdy, Y. A. Nada and A. A. Abdo, "How Good Is The DES Algorithm in Image Ciphering?" in International Journal of Advanced Networking and Applications, vol. 2, no. 5, (2011), pp. 796-803.

[8] 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.