RESEARCH ARTICLE OPEN ACCESS

An Analysis Over Secured Image Encryption Approaches

Mr. Baldeep Singh [1], Ms. Tanika Thakur [2]
Assistant Professor [2]
Department of Electronics and Communication Engineering
SVIET, Ramnagar, Patiala
Punjab -India

ABSTRACT
In today's era, several multimedia technologies has been developing significantly. Audio, Video and images are being transferred over the network openly and insecurely. Thus, security is primary feature that requires consideration to avoid from unauthorized entities. There are number of encryption techniques which have been developing to provide security over insecure channel. This paper considered several encryption methods used for security of images on the internet. Behavior of individual methods is discussed with the work performed previously in the domain of image encryption. Moreover, different encryption methods are also analyzed in this paper.

Keywords:- Image Encryption, Encryption methods, RSA, Diffie-Hellman Algorithm, Digital Signature Algorithm, Elliptic Curve Cryptography

I. INTRODUCTION

Nowadays most of the communication takes place online by using the internet services. The data travels through various gateways to reach the destination. Thus data security is quite essential ingredient in the communication so that the confidential data can be saved from unauthorized users or hackers. If any security paradigm is not applied to the confidential data then the hackers can easily make modifications in data and can lead to the false information. The security of information has become a key research area due to the enhancement in online data transfer rate. Data security can be done by following various ways such as cryptography, encryption, watermarking and steganography etc. Cryptography is a referred as a science to write a plane text into a coded language [1]. Similarly the encryption is done by converting the plane text into cipher text and also generates a key which is used to encrypt it. Consequently, the same key is used further to decrypt the cipher text to plane text. The watermarking is totally different domain from cryptography and encryption. It is a technique of generating a copyright of particular information. In this the watermark is embedded on the confidential information, the information can be of various formats such as text, audio, video, images etc.

The image encryption explodes the idea of transmitting the image over the internet in a secure manner so that no unapproved or unauthorized client can decode the image. An image involved several properties such as mass limit, high association, high association and high severance among the pixels which forces exceptional prerequisites on any encryption method. The most common method used for image encryption is scrambling. This method ensures that the information ought not to be identified [2]. Several methodologies are involved which utilizes this strategy such as Steganography, Packing, Advanced watermarking and Cryptography. The emphasis of this paper is to identify numerous encryption methods used for advanced digital images.

II. ENCRYPTION METHODS

The encryption technique used for encryption of message can be further classified into different groups as shown below [11] [12]:

- **Optical Encryption:** the encryption technique utilizes the optical devices in view of acquiring the image encoding while making the components of image random.
- **Selective Encryption:** the whole bits in data stream are not connected in the encryption method. In this only specific bits are used to encode the data stream.
- **Mixing property:** It represents the diffusion property. The data which needs to be encoded has initial region in the phase space of map. Then, mixing property method has implemented in order to acquire single plain text over multiple encoded text digits.
- **Reversible Cellular Automata Based Encryption (RCAE):** in this technique, cellular automat has designed specifically to get reversible usage. The size of key used for such purpose is 224 bit.
- **Robust chaos [2]:** the encryption method is considered as an optimal technique shows great significance particularly for single key digits over encoded data digits. The encryption keys used in this method depicts the encoding paradigm factors which lead to the handling of the variables carefully.
- **JPEG Encryption:** this method was originated for the encryption of images in JPEG 2000 format. The multilevel encoding is involved in this process that reduced the computational complexity.

- **Non-chaotic Encryption (NCE):** the encryption method involved Sudoku based matrix represented in the form of rows as well as columns. For the encoding or scrambling of plain text, Sudoku matrix is involved. Moreover, the intensity of image pixel can also be changed with the help of this matrix. At last, the mapping technique was implemented to shuffle the position of pixels.
- **Chaotic Encryption (CE) [2]:** also referred as highly sensitive encryption method as it involves sensitive initial values coupled together with mixing property. Furthermore, periodic form of encryption is also provided by this encryption technique.
- **Visual Cryptography:** can be employed for encryption as well as decryption process. In this technique, human vision is involved to encrypt the data at the transmission side, therefore no decryption algorithm is use to decrypt the image at the receiver side. The primary feature of this encryption technique is high security as no unauthorized user can access the information sealed under an image.
- **SCAN pattern (SCANP) based encryption:** designed specifically for gray scale images that provides lossless encryption of data. This encryption method used 2D spatial accessing technique for encryption.
- **DES (Data Encryption Standard):** referred as Block Encryption algorithm. DES is the first most developed invented encryption standard by National Institute of Standard and Technology. It is a symmetric type of cryptography mechanism. Therefore it uses the similar key for encryption and decryption on both sides i.e. sender and receiver end. In this the key size is limited to 64 bits. Out of 64 bits, 56 bits are reserved for independent key to represent the actual cryptography transformation and rest of the 8 bits is reserved for error detection. DES performs encryption in various rounds and permutation and substitution is the major functions performed under each and every round. Several parameters are involved for the expansion of key with cipher text. In this the decryption process is as same as the encryption process but only the difference is that in decryption round keys are implemented in reverse order. The output is comprised of 64 bit cipher text.
- **3DES (Triple DES):** Triple DES is an enhanced version of data encryption standard. In this the block size is bigger in comparison to the DES. It reserves the 64 bits for block size and 192 bits for key size. It applies for 3 times in order to enhance the security level. The disadvantage is that it is slower is processing.
- **AES (Advanced Encryption Standard):** categorized under symmetric cryptography. Another term used for AES is Rijindael's algorithm. It is developed to overcome the loop holes of the DES as it did not found suitable to the advanced computer systems. The main motive of the NIST to introduce the AES was to replace the DES so that it can be utilized by non-military agencies. The different data blocks on which encryption can be performed is 128 bits using 128, 198 and 256 bits of symmetric keys due to its variable length of 128 to 256 bits. The advantage of AES encryption over other encryption technique is that it is quite fat and flexible. It is mostly suitable for small devices. It is tested for various security applications.
- **Blowfish:** It is an encryption algorithm which works upon public domain developed by Bruce Schneider in the year of 1993. The encryption process using this technique becomes fast. It is a type of symmetric cryptography technique. It comprised of 64 bits block size and variable length block size for key which lies between 32 bits and 448 bits. It is one of the superior cryptographic mechanisms as it is quite secure. But the limited size for block size is the major drawback of blowfish due to which it is substituted by AES and two fish mechanism. But after having various limitations like small block size etc, this algorithm is successful algorithm against any kind of security breach. The application of this encryption technique helps to avoid any attack.
- **RC4:** based upon the stream cipher symmetric key used for encryption. In this encryption mechanism the XOR operation is performed on information and same algorithm is used for encryption and decryption mechanism. The key stream did not depend upon plain text. It also uses the variable sized key length which ranges from 1 to 256. It creates a state table which is further used for generating the random bits from pseudo cod and vice versa. This conversion leads to the cipher text in the output.
- **Diffie –Hellman Algorithm:** It is specifically used for sharing the keys which are used for cryptography. It is oldest method which is applied for securing the key sharing. In diffie Hellman algorithm it is not necessary for the sender to have any knowledge regarding receiver of the message.

III. LITERATURE REVIEW

This section of the paper discussed previous work performed by several researchers in the field of image encryption to enhance the security.

Madhu B, "An Overview of Image Security Techniques" [1] has described about the basic mechanism for image security. Various researches that had been conducted in the past few years were discussed in this paper such as Artificial Neural Network based technique.GA based algorithm, DCT based technique, chaos-based method, SVD based method, Steganography based algorithm, DWT dependant technique, visual Cryptography method, watermarking method. In this paper the scope of image security was also described. As the present world is getting more digitalized therefore all the sectors whether business, private or research are using the digital image communication system. As the images

transmitted over the open networks therefore these are not secured, therefore image security plays an important role. At present different type of image security techniques are used such as encryption, watermarking, steganography, etc. This paper had explained basic techniques used for image security.

Fahad bin Muhaya , "Chaos based Secure Storage and Transmission of Digital Medical Images" [2] had proposed the encryption paradigm based on chaotic logistic map. As there is quick and progressive improvement in the field of medical images transmission, so security of images becomes crucial part of consideration. Due to the large amount of implementation of medical images in the field of healthcare communities, it is necessary to prevent the information from the illegal access. The chaotic based image encoding scheme had been presented in this paper. The chaotic logistic map was implemented in order to scramble the values of pixels in the image used in medical field. To obtain the high level safety features the basic form of data encryption standard (DES) was implemented in this paper. The experiment was conducted to validate the efficiency and reliability of proposed mechanism for medical images security over the network.

Manel Dridi, "Cryptography of medical images based on a combination between chaotic and neural network"[3], the author conducted this study specifically for developing an encryption and decryption approach by using medical images. The technique was named as chaotic-neural-network. The objective behind this study was to assure the security of the medical images by applying the less complex encryption mechanism and then to compare the present techniques with existing methods. In this the robustness was improved by applying the XOR operation on original image and generated key. Then the weight value of the neurons was generated by creating the binary sequence with the help of chaotic system. The simulation of the proposed work was done by considering the images of 8 and 12 bits per pixels. The results proved the efficiency and reliability of the proposed work over the existing mechanisms.

Hongjun Liu, "Image encryption using DNA complementary rule and chaotic maps",[4] proposed an image encryption mechanism. First way was to mystify the pixels of the image by converting the nucleotide to its base pair randomly. And the other way was to create the new encryption key on the basis of the plain images and common keys by altering the condition of the chaotic systems automatically for individual process of encryption. The grayscale image was used as an input image and then permuted the rows and columns on the basis of the arrays that were generated by the PWLCM i.e. Piece Wise Linear Chaotic Map. The proposed work decomposed the pixel of images into four different nucleotides by using DNA coding scheme. Then the decomposed nucleotides were converted to its base pair randomly by utilizing the complementary rules. The time sequence was generated by using chebyshev maps. The experimental results were generated in order to prove that the proposed system had enough key space to secure the data from any kind of attacks.

Mamta Jain, "Secure Medical Image Steganography with RSA Cryptography using Decision Tree" [5], provided a security mechanism to secure the patient's information behind the images by applying the RSA cryptography which followed the concept of decision tree. The decision tree was used because of its robust and flexible nature. It provided the decision regarding the concealing position of the secret message in medical images. The RSA algorithm was used for encoding the patient's information and then the encoded information is divided into various blocks. Then this encrypted data is embedded on the medical images by using steganography. On the receiver side, this information was decrypted using RSA algorithm. The simulation analysis concluded the performance of the proposed method.

Mamta Juneja et al., "A Review of Cryptography Techniques and Implementation of AES for Images" [6], reviewed several cryptographic techniques such as Advanced Encryption Standards, Data Encryption Standards, 3-DES, RC4 and Blowfish. Then the contrast study among these techniques had been developed on the basis of the various patterns such as key size, used block size and required number of rounds for applying the techniques. On the basis of the comparison it was observed that the AES encryption outperforms the rest of the encryption techniques.

Nidhal Khdhair, "New Image Encryption Algorithm Based on Diffie –Hellman and Singular Value Decomposition" [7], the author introduced a novel and new method to encrypt the images in three steps only. The process was initiated by applying the Fibonacci transform to scramble the pixels of the image. Then in second step the deffie-Hellman key exchange mechanism was employed to generate the private key for encryption which was further used for encrypting the matrix generated by the singular value decomposition. In third step the SVD was implemented for generating the matrix and then encrypts this matrix. After evaluation it was observed that the original image can be retrieved without losing any information by employing the proposed work.

Dr. Parmanand Astya, "Image encryption and decryption using Elliptic curve cryptography" [8], today the security major concern for the purpose of research. To maintaining the security is a tedious task to perform while data transferring. In order to do so, many encryption and decryption techniques have been developed. RSA and deffie-Hellman are the most prominent security mechanisms, utilized by various authors for their research. But the size of the encryption is key is the major loop hole of RSA and Deffie-Hellman mechanism. ECC is another option for public key encryption. In this the used key size is quite smaller. This study firstly converted the image into elliptical curve and then a grid of image was formed. Then

the coordinate's point of the grid was encrypted and transmitted to the receiver. The ECC was utilized for encryption process as well as for decryption on receiver side.

Table1. Analysis of different encryption techniques

Sr. No.	Encryption Technique	ANALYSIS
1.	Rivest Shamir and Adleman (RSA) algorithm [5]	RSA can be used in Mobile nodes; because they are vulnerable to many attacks due to their broadcast nature. RSA is not suitable for WSN because of high time complexity and consumption demand.
2.	Diffie-Hellman Algorithm [7]	Here keys are exchanged between two users; unknown to each other. A proposed for two goals: authenticated key agreement and authenticated key agreement with key confirmation in the asymmetric (public-key) setting. It can be used in Internet and nearly in every encryption technology used in the Internet today, including SSL, SSH, IPSec, PKI.
3.	Digital Signature Algorithm [11]	Used by the receiver to verify that the message received is unaltered; a digital signature is used for performing this task. Hash function is used to generate dynamic and smaller size of bits which depends on each byte of data. Result of Hash function depends on size of data.
4.	Elliptic Curve Cryptography (ECC) [8]	Public-key algorithms that can provide shorter key lengths and, depending upon the environment and application in which it is used, improved performance over system based on integer factorization and discrete logarithms. Performance of ECC with other algorithms is, it is 5 to 15, 20 and 60, and sometimes 400 times faster than others depend on ECC bit.

The above table depicts different encryption techniques such as RSA, Diffie-Hellman, Digital Signatures and Elliptic Curve Cryptography. These techniques are discussed briefly with their respective features.

IV. CONCLUSION

Image Encryption plays an important role in increasing growth of digital data storage as well as communication over the open network. This paper made an attempt in identifying several image encryption methods used for the encryption purpose. From the survey reviewed, it has been concluded that ECC technique provides efficient results as it ensures fast processing in comparison with other encryption techniques.

REFERENCES

[1]. Madhu B., Ganga Holi, Srikant Murthy K. "An Overview of Image Security Techniques", International Journal of Computer Applications, Vol 154, 2016.

[2]. Fahad bin Muhaya, Muhammad Usama and Fahim Akhter "Chaos based Secure Storage and

Transmission of Digital Medical Images" Applied Mathematics & Information Sciences An international Journal, Vol 8, Pp27-33, 2014.

[3]. ManelDridi et al, "Cryptography of medical images based on a combination between chaotic and neural network", IET Image Processing, pp. 1-10, 2016

[4]. Hongjun Liu, "Image encryption using DNA complementary rule and chaotic maps", ELSEVIER, Vol 12 (5), pp 1457-1466, 2012

[5]. **M**amta Jain, "Secure Medical Image Steganography with RSA Cryptography using Decision Tree", IEEE 2017

[6]. Mamta Juneja et al., "A Review of Cryptography Techniques and Implementation of AES for Images", IJCSEE, Vol 1 (4), Pp 1-5, 2013,

[7]. Nidhal Khdhair, "New Image Encryption Algorithm Based on Diffie –Hellman and Singular Value Decomposition", IJARCCE, Vol 5(1), Pp 1-5, 2016,

[8]. Dr. Parmanand Astya, "Image encryption and decryption using Elliptic curve cryptography", IJARSE, Vol 3 (10), Pp 1-8, 2014

[9]. X. F.Guo X.cong" An Image Encryption Algorithm based on Scrambling and Substitution using Hybrid Chaotic Systems"2011 Seventh International Conference on Computational Intelligence and Security

[10]. B. Acharya, S.K.Panigrahy, S.K.Patra, and Ganapati Panda,‖ Image Encryption Using AdvancedHill Cipher Algorithm", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[11]. Nitin Jirwan, Ajay Singh and Dr. Sandip Vijay, "Review and Analysis of Cryptography Techniques", International Journal of Scientific & Engineering Research, Vol. 4, No. 3, March-2013

[12]. Er. ManpreetKaur and Er. Jasjeet Kaur, "Data Encryption Using Different Techniques: A Review", International Journal of Advanced Research in Computer Science, Vol. 8, No. 4, Pp. 252-255, May 2017

[13]. Priyanka Takkar , Ashish Girdhar and V.P. Singh, "Image encryption algorithm using chaotic sequences and flipping", Computing, Communication and Automation (ICCCA), 2017 International Conference on, May 2017

[14]. Kamali, M. R., Hossein, S., Shakerian, R., & Hedayati, M. "A new modified version of advanced encryption standard based algorithm for image encryption". International Conference on Electronics and Information Engineering (ICEIE), 2010, 1(Iceie), Pp. 141–145, 2010

[15]. Aihong, Z., Lian, L., & Shuai, Z. "Research on method of color image protective transmission based on logistic map" In International Conference on Computer Application and System Modeling (ICCASM), Oct. 2010, Vol. 9, No. Iccasm, pp. 266–269, 2010