Block Based Image Encryption Schemes: A Review

Abdul Yabar Rafiqi
Research Scholar
Noida

Archana Singh
Assistance Professor
Noida

Abstract - The image data transferring applications are utilized by numerous users today. Various clients that use social applications receive most of the images from users. The vital information present on the images can be extracted and copied through an attack on any on these applications. All such applications have been introduced to the mobile devices as well. There is various data security frameworks present in order to protect the data from various types of attacks to occur within the web applications. The encryption or steganogrpahy or both the systems are utilized together in some applications for providing secure systems. In this paper, various techniques are reviewed which are based on the block based encryption.

Keywords - *Image Encryption, Block based encryption, Stegnography*

I. INTRODUCTION

At present, DigitalImage Processing technology is progressing and penetrating in all the aspects of life including medical field, industrial, communication and intelligent robots etc. as the computer technology has been grown rapidly. Thus, the image information has attained an extensive popularity. Image data security plays an imperative role especially in the special military, commercial and medicinal sectors. The images reveal informative attributes which are more intuitive than the textual information. The amount of information stored in images has maximized. In this phase, the deployment of images is done as the major carrier of information. The information society brings this convenience. However, more caution regarding the disasters which are occurred due to the information leakage has also taken into consideration [1]. The essential task for human is to protect the information in secure way and avoid the losses which are occurred because of leakage of information. Image encryption is considered as the best scheme for protecting the digital image during transmission. Encryption can be defined as the changed data or bits of any certain source that are known to only sender and receiver.

The image encryption algorithms have included two kinds of techniques. The first is scrambling and the second is diffusion. The positions of the pixels are converted to attain the scrambling. The correlation amid the adjacent pixels is reduced and the encryption is obtained in the transformation of positions of the pixels. The values of the pixels are changed by carrying out the diffusion. Diffusion encryption is capable of improving the uncertainty and breaking the statistical attributes of the cipher images. The encryption technique has contained 3 basic components such as data, encryption engine and key management. The data whose security is required can be encrypted using the encryption algorithm [2]. The sender decides the type of algorithm and the variable for their implementation as a key. After that, this encrypted data is decrypted to utilize a proper key which is shared by the sender. The image encryption deals in the field of cryptography. It is classified into two algorithms. The first is symmetric encryption and the second one is asymmetric encryption. The symmetric or secret key encryption has utilized a similar key in order to encrypt and decrypt a message. Only authentic sender and recipient who want to perform communication have knowledge regarding the secret which is kept through encryption and decryption keys. The entire message protection is enhanced by assigning diverse keys to the distinct parties. The potential of the symmetric key encryption is based on the confidentiality of encryption and decryption keys. The classification of symmetric encryption algorithms is done in two parts: block cipher and stream cipher depending upon the grouping of message bits [3]. The block cipher is applied to encrypt the characters of messages having fixed size at same time and transmitting them to the receiver end. The block size for the stream cipher having only one character and it is not found more suitable for software processing because the length of the key is similar to the length of the message. There are some stages consisted in the execution of the stream cipher. The initial stage includes the incorporation of a single character of plaintext with a single character from key stream for generating the single character of ciphertext. After that, the transmission of character of ciphertext is done between the initial stage and the second stage. The asymmetric key encryption is called public key encryption that makes the utilization of various keys in order to encrypt and decrypt the message. The message is encrypted with the key using the public key. The decryption key is known as the secret or private key deploys for decrypting the message. The asymmetric key encryption's potential is implemented with digital signature. After that, the message authentication detection is employed to offer this key to the users.Data Encryption Standard (DES) is a symmetric-key algorithm utilizes to encrypt the

electronic data. The DES is a kind of block cipher. The major change executed is that the formation of Data Encryption Standard is specially done for resisting against the differential cryptanalysis import. At the same time, the cryptographic key and algorithm are implemented on a block of data more moderately as compares to one bit at instant [4]. The performance of this algorithm depends upon the utilization of same key for encrypting and decrypting a message. It has two inputs in the encryption function namely the plaintext and the key. Advanced Encryption Standard (AES) algorithm is a replacement of Data Encryption Standard for improving a security level for classified information with great speed. The AES is carried out in software and hardware on various platforms particularly in small devices for sensitive data. This algorithm consists of three family members named as AES-128, AES-192, and AES-256. The block having size of128-bits is facilitated in Advanced Encryption Standard with a varied key length having 128, 192 and 256-bits. A number of round keys are deployed in this process [5]. These keys are carried out along with other mathematical functions on an array known as a state array of data within blocks of a specified size. Ron Rivest, Adi Shamir, and Len Adlemen (RSA) algorithm had been designed by Ron Rivest, Adi Shamir, and Len Adlemen in 1978. A key size which greater than 1024-bits is employed in RSA and Block size is relied on the size of a key. The RSA is a block cipher and takes 1 round for the transformation of one message into cipher text. The factorization product of two large prime numbers denoted by p and q is the basis of this process and the block size relies on the product of these to a prime number. The modulus and exponent operations are deployed to produce these keys [6]. The digital signatures and non-repudiation of data is obtained in this algorithm for confirming the origin of the sender and achieving confidentiality, integrity, authenticity. Image Encryption based on chaotic system is a popular encryption algorithm. Chaotic system is a nonlinear dynamic system that is capable of generating pseudo-random sequence with good randomness and is appropriate to encrypt the data. The chaotic system is deployed to encrypt the digital images on the basis of excellent randomness of this system. The integration of chaotic system is often accomplished with image encryption techniques on the basis of spatial domain. Numerous encryption schemes are recommended with this chaotic system [7].The blowfish is a block cipher planned on the basis of Feistel structure works having data block size of 64 bits along with 16 processing rounds. This algorithm includes an adjustable key whose length starts from 32-bits up to 448-bits which relies on S-Boxes. Every S-box has 32-bits of data. Key expansion and data encryption are two major parts of Blowfish algorithm. A more processing time is taken by this algorithm because of variation in its key size. But this algorithm is quicker and more effective in comparison with another encryption symmetric algorithm. It has potential for defeating the brute-force attack because of the time consumption in the sub-key generation that leads to raise the complexity.

II. LITERATURE REVIEW

Fu Jie, et.al (2019) suggested a visually secure image encryption method on the basis of compressive sensing and IWT [8]. There were two stages included in this method. In the initial stage, the sparse and Random Bernoulli measurement matrix was implemented to compress and encrypt the plain image on the basis of compressive sensing. After that, 2D-LASM was employed to generate a sequence. This sequence permuted the pixel position of the compressed image. The second stage included the utilization of another color image as CI. Subsequently, the useful image was acquired using IWT. The outcomes of experiment demonstrated that the suggested was adaptable for encryption and it was feasible.

Jieyu Zheng, et.al (2020) intended a new technique to encrypt the image on the basis of dynamic DNA sequences encryption and enhanced 2D-LSMM [9]. The input of the sine map was controlled with the help of logistic map. The chaotic sequence of intended technique was deployed to determine the encoding and operation rules of DNA sequences. The outcomes of simulation and security analysis depicted that the proper encryption and resistance against various attacks had provided by the means of intended technique.

Shyamli Jain, et.al (2018) recommended an encryption technique on color image for which component based PRPE and FRFT was implemented [10]. The encoding was used so that the input RGB color image was transformed into HSV format. The FRFT was acted as a key using which extra degree of security was obtained in diverse orders. The encryption level of different methods was utilized for computing the robustness of image in terms of MSE and PSNR. The outcomes of simulation represented that a high security was obtained using the recommended approach and it was useful for color image.

K. Sreelakshmi, et.al (2020) emphasized on designing an encryption method to transmit the color images on un-trusted channel securely [11]. A bi-directional diffusion was carried out for 8-bit colored image. The image was protected in transmission with the implementation of designed technique. A fixed block size of 8 × 8 that assisted in increasing the robustness to deal with cipher text only attacks had employed to perform the encryption stages. Several tests were executed to evaluate the performance of designed method. The outcomes exhibited that the designed algorithm had robustness for tackling different cryptanalytic attacks.

Avishek Kumar, et.al (2018) introduced an asymmetric image encryption method in which the concepts of interference, phase-truncation and QR were integrated [12]. The Arnold transformation was utilized to initially scramble the input image. The classification of scrambled image was done onto pixel blocks. Phase truncation was utilized to the binary matrix whose encoding was performed into two POMs. The binary matrix that was grouped into QR codes and decoded into pixel blocks had acquired integrating the POMs under decryption. The decrypted image was retrieved from the descrambling operation. The introduced method had provided security and tolerance against noise. The encryption was performed in digital manner.

R. Santhiya Devi, et.al (2019) suggested a novel multiple segmented multiple-image encryption approach for which secure force algorithm named MCSPS and chaotic permutation schemes had employed [13]. There were 3 different methods executed to improve the security of suggested algorithm so that every segmented image was encrypted. The security of the suggested framework was computed against statistical and differential analysis using a number of metrics. The outcomes of experiment revealed that the suggested algorithm had robustness against the statistical and differential attacks.

Comparison Table:

Author	Year	Description	Outcome
Fu Jie, Ping Ping, Gao Zeyu, Mao Yingchi,	2019	Suggested a visually secure image encryption method on the basis of compressive sensing and IWT.	The outcomes of experiment demonstrated that the suggested was adaptable for encryption and it was feasible.
Jieyu Zheng, LingFeng Liu	2020	Intended a new technique to encrypt the image on the basis of dynamic DNA sequences encryption and enhanced 2D-LSMM.	The outcomes of simulation and security analysis depicted that the proper encryption and resistance against various attacks had provided by the means of intended technique.
Shyamli Jain, Ajay Khunteta	2018	Recommended an encryption technique on color image for which component based PRPE and FRFT was implemented.	The outcomes of simulation represented that a high security was obtained using the recommended approach and it was useful for color image.
K. Sreelakshmi, Renjith V. Ravi	2020	Designed an encryption method to transmit the color images on un-trusted channel securely.	The outcomes exhibited that the designed algorithm had robustness for tackling different cryptanalytic attacks.
Avishek Kumar, Naveen K. Nishchal	2018	Introduced an asymmetric image encryption method in which the concepts of interference, phase-truncation and QR were integrated.	The introduced method had provided security and tolerance against noise.
R. Santhiya Devi, K Thenmozhi, RengarajanAmirtharajan, PraveenkumarPadmapriya	2019	Suggested a novel multiple segmented multiple-image encryption approach for which secure force algorithm named MCSPS and chaotic permutation schemes had employed.	The outcomes of experiment revealed that the suggested algorithm had robustness against the statistical and differential attacks.

III. CONCLUSION

The block-based method divides the image into various blocks which are then shuffled from their positions. This results in dissipating the high correlation amongst the pixels and also increases the entropy value. There are two phases in which the encryption algorithm is divided. The first phase includes the block division of the fixed size and the second phase includes the rearrangement of blocks and then at the end the transformation algorithm is applied. It is concluded that block based encryption scheme give high security as compared to basic encryption methods

IV. REFERENCES

[1]. Manish Kumar, Rachid Ait MaalemLahcen,R. N. Mohapatra, Chandan Alwala, and Surya Vamsi Krishna Kurella, “Review of Image Encryption Techniques”, 2020, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 22, Issue 1

[2]. Payal Sharma, Manju Godara, Ramanpreet Singh, “Digital Image Encryption Techniques: A Review”, 2012, International Journal of Computing & Business Research

[3]. Jun Lang, “The reality-preserving multiple-parameter fractional fourier transform and its application to image encryption”, 2012, 5th International Congress on Image and Signal Processing

[4]. RozaAfarin, Saeed Mozaffari, "Image encryption using genetic algorithm", 2013, 8th Iranian Conference on Machine Vision and Image Processing (MVIP)
[5]. Piyush Kumar Singh, Ravi Shankar Singh, Kabindra Nath Rai, "An image encryption algorithm based on XOR operation with approximation component in wavelet transform", 2015, Fifth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG)
[6]. Zhuhong Shao, Jiasong Wu, Jean Louis Coatrieux, GouenouCoatrieux, Huazhong Shu, "Quaternion gyrator transform and its application to color image encryption", 2013, IEEE International Conference on Image Processing
[7]. Juliano B. Lima, Edmar S. da Silva, Ricardo M. Campello de Souza, "A finite field cosine transform-based image processing scheme for color image encryption", 2015, IEEE Global Conference on Signal and Information Processing (GlobalSIP)
[8]. Fu Jie, Ping Ping, Gao Zeyu, Mao Yingchi, "A Meaningful Visually Secure Image Encryption Scheme", 2019, IEEE Fifth International Conference on Big Data Computing Service and Applications (BigDataService)
[9]. Jieyu Zheng, LingFeng Liu, "Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map", 2020, IET Image Processing
[10]. Shyamli Jain, Ajay Khunteta, "Color Image Encryption by Component Based Partial Random Phase Encoding", 2018, International Conference on Inventive Research in Computing Applications (ICIRCA)
[11]. K. Sreelakshmi, Renjith V. Ravi, "A Bidirectional Diffusion Based Image Encryption Scheme for Color Images", 2020, 7th International Conference on Smart Structures and Systems (ICSSS)
[12]. Avishek Kumar, Naveen K. Nishchal, "An image encryption scheme employing quick response codes", 2018, 3rd International Conference on Microwave and Photonics (ICMAP)
[13]. R. Santhiya Devi, K Thenmozhi, RengarajanAmirtharajan, PraveenkumarPadmapriya, "A Novel Multiple Segmented Image Encryption", 2019, International Conference on Computer Communication and Informatics (ICCCI)