International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Industrial Automation and Computing (ICIAC- 12-13th April 2014)

RESEARCH ARTICLE OPEN ACCESS

An Approach For Secure Image Transmission

Ms. Prakruti Bisen, Prof. Dipak Wajgi
Department of Computer Engineering,
St. Vincent Pallotti College of Engineering and Technology
Nagpur, India bisenprakruti@gmail.com , Wajgi@rediffmail.com

Abstract: In the digital world, image plays an important role of information storage. Number of new techniques is invented to provide all the aspects of security to data. In this paper an approach is presented for secure image transmission through network. Technique of encryption along with segmentation is proposed for greater security.
Keywords: AES, Fragments, Segmentation, Cryptosystem

I. Introduction

In the digital world, images are important information. So far in cryptography lots of works which have done related to text information. Encryption techniques so far used for text information may not work in same direction for visual. Digital images are attractive data types with widespread use and many users are interesting to implement content protection on them to keep from copyright, preview or malfunction. On much system like military image databases, providing security is must. It is very important to protect confidential image data from unauthorized access. Encryption is the preferred technique for protecting the transmitted data [1]. However, number of other techniques instead of encryption is also available for converting valuable piece of information into such form which access is prohibited to unauthorized users. There are various encryption systems for encrypting and decrypting images are available. In information systems, aspects of security like confidentiality, security, privacy and non-repudiation need to be achieved. Cryptography is the method for providing encryption and decryption. Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted.

Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main goal of cryptography is keeping data secure form unauthorized attackers. The reverse of data encryption is data decryption, which recuperate the original data. Since cryptography first known usage in ancient Egypt it has passed through different stages and was affected by any major event that affected the way people handled information. In modern days cryptography is no longer limited to secure sensitive military information but recognized as one of the major components of the security policy of any organization and considered industry standard for providing information security, trust, controlling access to resources, and electronic financial transactions. The original data that to be transmitted or stored is called plaintext, the one that can be readable and understandable either by a person or by a computer

Widely there are two types of cryptographic method available namely, symmetric key and asymmetric key cryptosystem. Symmetric key cryptosystem enjoys widespread use when it comes to protecting digital data in networks. Here, a same secret key is used for both encryption and decryption process. This secret key is only shared by the sender and receiver of the communicating parties and kept confidential to other entities. The secrecy of the message will be protected well, when the secret key is kept confidential and distributed securely. [2]

Here we have proposed an idea of using AES which is a symmetric key algorithm for encrypting and decrypting images. For providing greater security aspect in the case of secure image transmission over the network we have propose segmenting image along with encryption and sending this small parts of images through different paths in the network to ensure greater security and privacy from attackers. Rest of the paper is organized as follows: In section 2 we have given literature survey. In section 3, detailed about proposed approach is provided finally conclusion is drawn in section 4.

II. LITERATURE SURVEY

In this section, the research work of some authors in the same field area presented and explained a short description of various techniques used for image Encryption.

Seyed Hossein Kamali, Reza Shakerian "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption" [3] proposed a new encryption scheme as a modification of AES algorithm based on both Shift Row Transformations. In this if the value in the first row and first column is even, the first and fourth rows are unchanged and each bytes in the second and third rows of the state are cyclically shifted right over different number, else the first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes..Experimental result shows it gives better encryption results in terms of security against statistical attacks Hai Yu, Zhiliang Zhu "An Efficient Encryption Algorithm Based on Image Reconstruction" [4], proposed a efficient image encryption algorithm which is based on image reconstruction using some adjacent pixel characteristics. According to the different characteristics of different bit level binary images, the proposed encryption scheme reconstructs the image at the bit level. Simulations and cryptanalysis both show that the proposed image encryption scheme is more effective and yields better level of security.

K.C.Ravishankar, M.G. Venkateshmurthy "Region Based Selective Image Encryption" [5] anticipated technique that segments the image into regions of fixed size. These regions act as units for processing the image. Selective Encryption makes it possible to encrypt only a part of the image leaving the rest of the image unaltered. Here, the regions covering the part of the image are considered for encryption. Selective Reconstruction deals with decrypting only a part of the encrypted image. Both the methods provides considerable amount of reduction in the encryption time. The regions are encrypted independently after segmentation and permutation of regions.

A Shamir, "How to share a secret" [6] provides general aspects and approaches of design an image cryptosystem. They have given a general introduction for cryptography and image encryption followed by different techniques and finally general security analysis methods for image encryption is provided.

Chin Chen Chang, Min-Shain Hwang, Tung Shou Chen,"A new encryption algorithm for image cryptosystem" [7] put forward new image encryption technique. This is based on vector quantization of confusion and diffusion of codebook. Zhang Yun-peng, et all [8] ,"Digital image encryption algorithm based on chaos and improved DES " presented an experimental results on the combination of image encryption algorithm like chaotic encryption, DES encryption for image encryption.In their algorithm, for making the pseudo-random sequence, logistic chaos sequencer was used. This algorithm had high security and the encryption speed. Simulation had shown the result of experiment after applying chaos and Des algorithm and result has proven the greater security against vulnerable attacks. Rajinder kaul et all [9], "comparative analysis and implementation of image encryption algorithm" presented an efficient algorithm for image security. They have present three different types of algorithm namely: selective encryption, selective image encryption using chaotic map and new image encryption approach using block based transform algorithm. Selective image encryption include chaos based key generation algorithm and selective encryption, both are performed individually and merged at the end. For chaos based key generation Henon map is used. And the third techniques shuffle the blocks containing images and fed into new output image.

Bibhudendra Acharya et all [10], "Image Encryption Using Advanced Hill Cipher Algorithm" in their paper proposed an advanced Hill (AdvHill) cipher algorithm which uses an involuntary key matrix method for encrypting image. They have consider different images and encrypted them using original Hill cipher algorithm and their proposed AdvHill cipher algorithm. And in the results it is clarified that original Hill Cipher can't encrypt the images properly if the image consists of large area covered with same color or gray level. But their proposed algorithm works for any images with different grayscale as well as color images.

III. Proposed Approach

In this section, we have proposed an approach for improving security measures while transmitting an image through network. The AES algorithm is used for encryption and decryption of image. It is a symmetric key algorithm in which both sender and receiver posses same secret key for encryption and decryption. AES is a fastest among the entire algorithm so far used for image encryption. It uses 10, 12, or 14 rounds. The key size that can be 128,192 or 256 bits depends on the number of rounds. It contains various rounds along with several stages. [9]

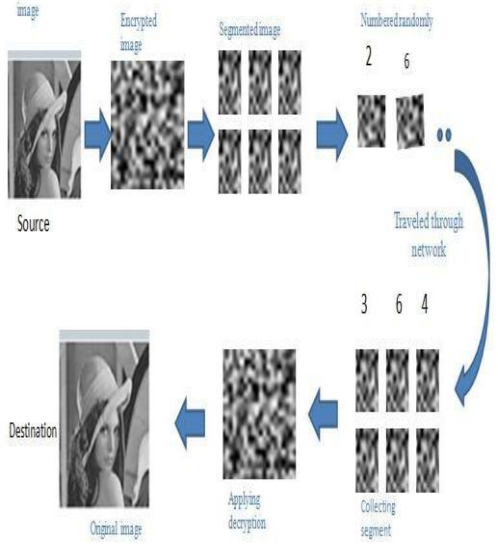
Here we are going to use 10 rounds and 128 key sizes at a time. After encryption, image will segmented into number of parts. Each individual fragment will carry special random number and will pursue different path to reach the destination as illustrated in figure 1.

At destination side, each part of image will be combined together in proper sequence using random numbers. In this way each part will unite to reform

the original image. To the whole encrypted image at destination side, decryption process of AES will apply to get the original information. As we know, decryption process of AES is not same as encryption. Thus it ensures more safety to the information.

Hence, each fragments will follow different paths, attacker would not going to have an intimation of which fragment has follow which path to reach at destination.

Thus this approach ensures security and privacy of image travelling through network from vulnerable attacks.



IV. CONCLUSION

In this paper, the encryption methods (Symmetric key encryption and Asymmetric key encryption) are highlighted along with their examples. Also we have surveyed existing research on image encryption in a new approach using other techniques more than only encryption. These techniques were partial encryption, chaos maps, public key and block transformation which applied to improve and enhance the efficiency of an image encryption algorithm. Finally, a secure approach is presented for enhancing more security of image while travelling through networks.

REFERENCES

[1]. M. Ali Moh'd Bani Younes, "An Approach To Enhance Image Encryption Using Blockbased Transformation Algorithm" Phd Thesis, University Sains Malaysia, 2009.

[2]. Ali Soleymani, Zulkarnain Md Ali and Md Jan Nordin,"A survey on principal aspects of secure image transmission", World Academy of Science, Engineering and technology 66 2012.

[3]. S.H. Kamali, R. Shakerian "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption" *2010 International Conference on Electronics and Information Engineering (ICEIE 2010).*

[4]. H. Yu, Z. Zhu "An Efficient Encryption Algorithm Based on Image Reconstruction" *2009 International Workshop on Chaos-Fractals Theories and Applications.*

[5]. K.C. Ravishankar, M.G. Venkateshmurthy "Region Based Selective Image Encryption" *1-424-0220-4/06 ©2006 IEEE.* [5]. Paul A.J P. M. K. Paulose Jacob "Matrix based Cryptographic Procedure for Efficient Image Encryption" *978-1-4244-9477-4/11 ©2011 IEEE.*

[6] A Shamir,"How to share a secret", Communication of the ACM, Vol 22, no.11, pp. 612-613, 1979.

[7] Chin Chen Chang, Min-Shain Hwang, Tung Shou Chen,"A new encryption algorithm for image cryptosystem" , the journal of sytem and softwre 58, *3-91, 2001.

[8] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan , Dai Wei-di," Digital image encryption algorithm based on chaos and improved DES", IEEE International Conference on Systems, Man and Cybernetics, 2009.

[9]. Rajinder Kaul, Kanwalpreet Singh,"comparative analysis and implementation of image encryption algorithm", IJSMC, Vol 2, Issues 4, 2013