Analysis of Security Issues and their solutions In Transmitting Images Over Wireless Networks

[1]Ms. Manju Rani, [2]Dr. Sudesh Kumar
[1]M.Tech Scholar , BRCMCET ,Bahal Bhiwani
[2]Associate Professor , *BRCMCET Bahal, Bhiwani*

Abstract—The great advances in wireless communication networks have led to high desire for a strong digital data transmission. However, illegal data access has become more easy and prevalent in wireless networks. In order to protect valuable data from undesirable readers, data encryption has become a critical issue. This paper provides an in depth analysis of security issues in transmitting images over wireless networks. It analyzes and compares the previous research on various image encryption techniques. Also we propose some novel solutions which are simple to implements for providing a better security in transmitting images over wireless networks.

Index Terms— Image Encryption, JPEG Images, Shared Key Encryption, Visual Cryptography

I.INTRODUCTION

With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and encryption is one the ways to ensure security. Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. Furthermore, special and reliable security in Storage and transmission of digital images is needed in many applications, such as cable-TV, online personal photograph album, medical imaging systems, military image communications and confidential video conferences, etc. In order to fulfill such a task, many image encryption methods have been proposed.

Encryption is a very common technique for promoting the image security. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet communication, multimedia systems, medical imaging, Tele-medicine and military Communication, etc. The evolution of encryption is moving towards a future of endless possibilities. Everyday new methods of encryption techniques are discovered. This paper holds some of those recent existing encryption techniques and their security issues. The performance of all those encryption techniques are studied and

discussed in later sections of this paper.

The image encryption algorithms can be classified into three major groups: (i) position permutation based algorithm [1] (ii) value transformation based algorithm and [2, 3] (iii) visual transformation based algorithm [1]

II. CRYPTOGRAPHY AND CHAOTIC MAPS

A)Cryptography :-

The many schemes used for enciphering constitute the area of study known as cryptography. There are three types of cryptography:

Secret Key Cryptography:

This type of cryptography technique uses just a single key. The sender applies a key to encrypt a message while the receiver applies the same key to decrypt the message. Since only single key is used so we say that this is a symmetric encryption. The biggest problem with this technique is the distribution of key as this algorithm makes use of single key for encryption or decryption.

Public Key Cryptography :

This type of cryptography technique involves two key crypto systems in which a secure communication can take place between receiver and sender over insecure communication channel. Since a pair of keys is applied here so this technique is also known as asymmetric encryption. In this method, each party has a private key and a public key. The private is secret and is not revealed while the public key is shared with all those whom you want to communicate with. If Alice wants to send a message to bob, then Alice will encrypt it with Bob's public key and Bob can decrypt the message with its private key

Hash Functions :

This technique does not involve any key. Rather it uses a fixed length hash value that is computed on the basis of the plain text message. Hash functions are used to check the integrity of the message to ensure that the message has not be altered, compromised or affected by virus. Cryptography technique needs some algorithm for encryption of data. Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, we need to ensure information security and safety. Image is also an important part of our information Therefore it's very important to protect our image from unauthorized access.

B)Chaos System :

[4]Chaos theory, as a branch of the theory of nonlinear dynamical systems, has brought to our attention a somewhat surprising fact: low-dimensional dynamical systems are capable of complex and unpredictable behavior. What is the origin of chaos in deterministic systems? For simplicity we consider here a discrete-time dynamical system defined by iteration of the function F: X → X, X — RN. The set of points {**x**, F(**x**), F2(**x**), …} is called a trajectory (or orbit) of the initial condition **x**. We assume that F has a chaotic attractor. Informally, an attractor is called chaotic if the motion on it is unpredictable: two nearby states on the attractor have different and unrelated behavior within the attractor. The evolution of a deterministic system is completely determined by the vector field F and the initial condition **x**. However, to specify completely the initial condition an infinite amount of information and a measuring system with an infinite precision

are required, which are both intractable.

Chaos is a phenomenon that occurs in nonlinear definable systems sensitive to initial conditions and has a pseudo-random behavior. Dynamic chaotic systems in case of Liapunov exponential equations meet will remain stable in chaos mode. An important characteristic that has caused this phenomenon to take into consideration for many cryptographic systems is being definable despite of its pseudo-random behavior. Due to pseudo-random behavior, the output of the vision system seems random in attackers' view, while in receiver's view, the system can be defined and decryption is possible. Many cryptographic algorithms based on chaos theory are presented till now [5, 6, 7] and some of them are somehow employed in way that are capable of image encryption addition to text encryption. Image encryption must have special features such as suitable speed for image massive data ciphering. Text encryption methods are not suitable for implementation on the image. Practically, we need to transmit a reasonable amount of information, which requires a large sample space and that in turn implies a large number of keys. The distribution of a large number of keys is liable to cause horrendous management problems. So, one of the main advantages of chaotic system's realization is facilitated key management approach because this method only needs to protect and secure transmission of secret key (parameters and initial values of chaotic system), which has a little volume and therefore not only a little memory is needed to maintain it but also there is more confidence during its transfer. The unauthorized access to short length keys is significantly less possible than the large length keys during data transmission through the insecure channel.

III.LITERATURE SURVEY

In this section, this paper presents the research work of some prominent authors in the same field and explaining 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” 2010[8]. This paper 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 that that MAES gives better encryption results in terms of security against statistical attacks and increased performance.

Hai Yu, Zhiliang Zhu “An Efficient Encryption Algorithm Based on Image Reconstruction” 2009[9].

An efficient image encryption algorithm is proposed, 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. Two parts of information, the significant one and the unimportant one, are treated differently and processed separately. Simulations and cryptanalysis both show that the proposed image encryption scheme is more efficient and yields better level of security.

Zhang Yun-peng , Zhai Zheng-jun “ Digital Image Encryption Algorithm Based on Chaos and Improved DES” 2009[10].

This paper is based on the chaotic encryption and Improved DES encryption and a combination of image encryption algorithm is used to find the gaps.In this paper new encryption logistic Map produced pseudo random sequence on RGB image and make double times encryption with improved DES . Combination of Chaos And improved DES makes the final algorithm more secure ,faster and more suitable for digital image encryption

K.C.Ravishankar,M.G. Venkateshmurthy “Region Based Selective Image Encryption” 2006[11].

The proposed technique 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 give a fair amount of reduction in the encryption time.Once the segmentation and permutation of regions is completed, the regions are encrypted independently.

Paul A.J P. Mythili K. Paulose Jacob “Matrix based Cryptographic Procedure for Efficient Image Encryption” 2011[12].

In this paper a fast symmetric key encryption procedure,Matrix Array symmetric Key Encryption (MASK) based on matrix manipulation is presented .this provides fast conversion of plaintext and images into ciphertext and cipher images.. The encryption scheme presented here is a block cipher with a block size of 128 bits and key size of 128 bits. Mask Result is also compared with AES .The performance test results indicate the suitability of MASK for fast image encryption.

Haojiang Gao *, Yisheng Zhang, Shuyun Liang, Dequn Li “A New Chaotic Image Encryption Algorithm“2006[13]

This paper, have proposed a new image encryption scheme based on a chaotic system.it is based on power and tangent function instead of linear function. It uses chaotic sequence generated by NCA map to encrypt image data with different keys for different images . plain-image image can be encrypted by use of XOR operation with the integer sequence.

Aditee Gautam, Meenakshi Panwar, Dr.P.R Gupta “A New Image Encryption Approach Using Block Based Transformation Algorithm” 2011[14].

In this paper a block based transformation algorithm is used in which image is divided into number of blocks. These blocks are transformed before going through an encryption process. At the receiver side these blocks are retransformed in to their original position and decryption process is performed Advantage of this approach, is that it reproduce the original image with no loss of information for the encryption and decryption process we used a blowfish algorithm.

Modified AES Based Algorithm for Image encryption, 2007.

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki[15] analyze the Advanced Encryption Standard (AES), and in their image encryption technique they add a key stream generator (A5/1, W7) to AES to ensure improving the encryption performance.

Image Encryption Using Block-Based Transformation Algorithm, 2008

Mohammad Ali Bani Younes and Aman [16] introduce a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm. Their results showed that the correlation between image elements was significantly decreased. Their results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm, 2008

Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jena [17] present image encryption technique using the Hill cipher. They are generating self-invertible matrix for Hill Cipher algorithm. Using this key matrix they encrypted gray scale as well as colour images. Their algorithm works well for all types of gray scale as well as colour images except for the images with background of same gray level or same colour.

An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption, 2008

Mohammad Ali Bani Younes and Aman Jantan [18] introduce a new permutation technique based on the combination of image permutation and a well known encryption algorithm called RijnDael. The original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process, and then the generated image was encrypted using the RijnDael algorithm. Their results showed that the correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved.

Image Encryption Using Advanced Hill Cipher Algorithm, 2009

Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda [19] have proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption. They have taken different images and encrypted them using original Hill cipher algorithm and their proposed AdvHill cipher algorithm. And it is clearly noticeable that original Hill Cipher can't encrypt the images properly if the image consists of large area covered with same colour or gray level. But their proposed algorithm works for any images with different gray scale as well as colour images.

Digital image encryption algorithm based on chaos and improved DES, 2009

Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan and Dai Wei-di [20] researches on the chaotic encryption, DES encryption and a combination of image encryption algorithm. In their technique firstly, new encryption scheme uses the logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement DES.Their result show high starting value sensitivity, and high security and the encryption speed.

A Novel Image Encryption Algorithm Based on Hash Function, 2010

Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki [21] proposed a novel algorithm for image encryption based on SHA-512 hash function. The algorithm consists of two main sections: The first does preprocessing operation to shuffle one half of image. The second uses hash function to generate a random number mask. The mask is then XORed with the other part of the image which is going to be encrypted.

A Digital Image Encryption Algorithm Based Composition of Two Chaotic Logistic Maps, 2010

Ismail Amr Ismail, Mohammed Amin, and Hossam Diab[22] introduces an efficient chaos-based stream cipher, composing two chaotic logistic maps and a large enough external secret key for image encryption. In the proposed image encryption scheme, an external secret key of 104 bit and two chaotic logistic maps are employed to confuse the relationship between the cipher image and the plain image. Further, to make the cipher more robust against any attack, the secret key is modified after encrypting of each pixel of the plain image. The robustness of the proposed system is further reinforced by a feedback mechanism, which makes the encryption of each plain pixel depends on the key, the value of the previous cipher pixel and the output of the logistic map (data dependent property).

IV CONCLUSION

In this paper, many of the important encryption techniques have been presented and analyzed in order to make familiar with the various encryption algorithms used in encrypting the image which has been transferred over network. The results of the simulation show that every algorithm has advantages and disadvantages based on their techniques which are applied on images. On the basis of study of all the above mentioned research papers thoroughly, the following suggestions can be drawn: To protect multimedia contents, Chaos based algorithm should be implemented. More complex & compressed algorithm should be used to provide high speed and security to the System. Modified version of various algorithms is used to increase the security level.

REFERENCES

[1] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryption algorithm and its VLSI architecture", Pattern Recognition and Image Analysis, vol.IO, no.2, pp.236-247, 2000.

[2] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203),229-234.

[3] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001),1229- 1245.

[4] Alireza Jolfaei, Abdolrasoul Mirghadri, “An Image Encryption Approach Using Chaos And Stream Cipher” JATIT, 2010.

[5] Z.H. Guan, F. Huang, and W. Guan, “Chaos- Based Image Encryption Algorithm,” Physics Letters A, vol. 346, 2005, pp. 153– 157.

[6] M. Suneel, “Cryptographic Pseudo-random Sequences from the Chaotic Henon Map,” Sadhana, vol. 34, no. 5, 2009, pp. 689–701.

[7] V. Patidar, N.K. Pareek, G. Purohit, and K.K. Sud, “Modified Substitution–Diffusion Image Cipher Using Chaotic Standard and Logistic Maps,” Commun Nonlinear SciNumer Simulat, vol. 15, 2010, pp. 2755–2765.

[8] 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).

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

[10] Z.Yun-peng , Z. Zheng-jun “ Digital Image Encryption Algorithm Based on Chaos and Improved DES “Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2000.

[11] K.C. Ravishankar, M.G. Venkateshmurthy “Region Based Selective Image Encryption” 1-424-0220-4/06 ©2006 IEEE.

[12] Paul A.J P. M. K. Paulose Jacob “Matrix based Cryptographic Procedure for Efficient Image Encryption” 978-1-4244-9477-4/11 ©2011 IEEE.

[13] H.Gao,Y.Zhang, S. Liang, D.Li “A New Chaotic Image Encryption Algorithm “Chaos, Solitons and Fractals 29 (2006) 393–399. [7]. A.Gautam, M. Panwar, Dr.P.R Gupta “A New Image Encryption

Approach Using Block Based Transformation Algorithm” 2011 (IJAEST) Vol No. 8, Issue No. 1, 090 - 096 .

[14] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, ―A Modified AES Based Algorithm for Image Encryption‖, World Academy of Science, Engineering and Technology 27 2007.

[15] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, ―A Modified AES Based Algorithm for Image Encryption‖, World Academy of Science, Engineering and Technology 27 2007.

[16] Mohammad Ali Bani Younes and Aman Jantan ―Image Encryption Using Block-Based Transformation Algorithm IAENG International Journal of Computer Science, 35,2008.

[17] Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jen‖, Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm‖1st t International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008

[18] Mohammad Ali Bani Younes and Aman Jantan, ―An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption‖, IJCSNS International Journal of Computer Science and Network Security, VOL.8 , April 2008.

[19] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda,‖ Image Encryption Using Advanced Hill Cipher Algorithm‖, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[20] 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.

[21] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, ―A Novel Image Encryption Algorithm Based on Hash Function‖ 6th Iranian Conference on Machine Vision and Image Processing, 2010.

[22] Ismail Amr Ismail, Mohammed Amin, Hossam Diab. A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps‖, International Journal of Network Security, Vol.11, No.1, PP.1 - 10, July 2010.