IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 6 (Mar. - Apr. 2013), PP 80-83
www.iosrjournals.org

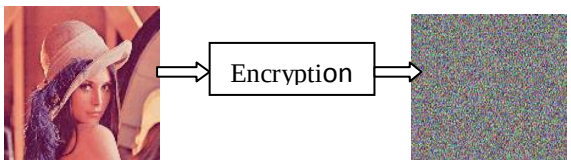
Image Encryption Techniques:A Selected Review

Rajinder Kaur[1], Er.Kanwalprit Singh[2]
[1] *(Student,UCoE ,PunjabiUniversity,Patiala,India)*
[2] *(Assitant Professor,UCoE ,PunjabiUniversity,Patiala,India)*

Abstract:- *Due to the rapid growth of digital communication and multimedia application, security becomes an important issue of communication and storage of images. Encryption is one of the ways to ensure high security images are used in many fields such as medical science, military.Modern cryptography provides essential techniques for securing information and protecting multimedia data. In recent years, encryption technology has been developed quickly and many image encryption methods have been used to protect confidential image data from unauthorized access .In this paper survey of different image encryption techniques have been discussed from which researchers can get an idea for efficient techniques to be used.*
Keywords: *Cryptography, Decryption, Encryption, Image Encryption , Key Space.*

I. Introduction

With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and Encryption is a common technique to uphold image 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. The process of encoding plain text messages into cipher text messages is called **encryption**.and the reverse process of transforming cipher text back to plain text is called as **decryption**. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication. Color images are being transmitted and stored in large amount over the Internet and wireless networks, which take advantage of rapid development in multimedia and network technologies. In recent years, plenty of color image encryption approaches have been proposed. Until now, various data encryption algorithms have been proposed and widely used, such as AES, RSA, or IDEA most of which are used in text or binary data. It is difficult to use them directly in multimedia data and inefficient for color image encryption because of high correlation among pixels. For multimedia data are often of high redundancy,of large volumes and require real-time interactions.



Original Image Encrypted Image

Fig.1

This paper is organized as follows In Section 1; we present general guide line about cryptography. In Section 2, we survey on already existing research paper. Finally, we conclude in section 3.

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

1.1 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.

1.2 Public Key Cryptography

This type of cryptography technique involves two key crypto system 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

1.3 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.

II. Literature Review

In this section, we are presenting the research work of some prominent authors in the same field and explaining a short description of various techniques used for image Encryption.

A. Seyed Hossein Kamali, Reza Shakerian **"A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption"** 2010[1]

proposed a new encryption scheme as a modification of AES algorithm based on both ShiftRow 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.

B. Hai Yu, Zhiliang Zhu **"An Efficient Encryption Algorithm Based on Image Reconstruction"** 2009[2]

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.

C. Zhang Yun-peng , Zhai Zheng-jun **" Digital Image Encryption Algorithm Based on Chaos and Improved DES**" 2009[3]

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

D. K.C.Ravishankar,M.G. Venkateshmurthy **"Region Based Selective Image Encryption"** 2006[4]

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.

E.Paul A.J P. Mythili K. Paulose Jacob **"Matrix based Cryptographic Procedure for Efficient Image Encryption"** 2011[5]

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

F. Haojiang Gao *, Yisheng Zhang, Shuyun Liang, Dequn Li "**A New Chaotic Image Encryption Algorithm "** 2006[6]

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.

G. Aditee Gautam, Meenakshi Panwar, Dr.P.R Gupta **"A New Image Encryption Approach Using Block Based Transformation Algorithm"** 2011[7]

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.

H. Qiu-Hua Lin, Fu-Liang Yin, and Yong-Rui Zheng" **Secure image communication using blind source separation"** 2004 IEEE.[8]

In this paper, an image encryption method is proposed by using the linear mixing model of blind source separation *(BSS).* It can simultaneously encrypt multiple images with the same size by mixing them with the same number of statistically independent key images, the size of which is equal to that of the images to be encrypted. Since these multiple images cover mutually through mixing among them while the key imnges cover them, and there is not any restriction on the key space, the proposed method has high level of security.

I. Ruisong Ye Haiying Zhao **"An Efficient Chaos-based Image Encryption Scheme Using Affine Modular Maps"** 2012[9]

An efficient image encryption scheme based on affine modular maps is proposed in the paper. The proposed scheme can shuffle the plain-image efficiently in the permutation process. An effective two-way diffusion process is also presented to change the gray values of the whole image pixels. All the experimental results show that encryption scheme is secure, its highly sensitivity to the cipher keys and plain-images. It is easy to manipulate and can be applied to any images with unequal width and height as well

J. Rui liu, Xiaoping tian "**New algorithm for color image encryption using chaotic map and spatial bit level permutation"** 2012[10]

proposed a new algorithm for color image encryption using chaotic map and spatial bit-level permutation (SBLP).Firstly, use Logistic chaotic sequence to shuffle the positions of image pixels, then transform it into a binary matrix and permute the matrix at bit-level by the scrambling mapping generated by SBLP. then use another Logistic chaotic sequence to rearrange the position of the current image pixels. Experimental results show that the proposed algorithm can achieve good encryption result and low time complexity, This makes it suitable for securinvideo surveillance systems, multimedia applications and real-time applications such as mobile phone services.

K.Xiang Fei□Guo Xiao-cong **"An Image Encryption Algorithm based on Scrambling and Substitution using Hybrid Chaotic Systems"** 2011[11]

The paper presents an image encryption algorithm based on two-dimensional (2D) Logistic map and complicated Chua's system., uses the different ways to scramble a color image,, so gets a new encrypted image. and then uses the chaotic sequences generated by optimization models of Chua's system to produce new pixel values. The results of the simulation and analysis show that the new algorithm has good properties of confusion and diffusion, the key space is large and the algorithm is very sensitive to the initial values .

L. Bibhudendra Acharya Saroj Kumar Panigrahy, SaratKumar Patra, and Ganapati Panda **"Image Encryption Using Advanced Hill Cipher Algorithm"** 2009[12]

This paper 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 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 colour images.

III. 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 are used to increased the security level.

References

[1]. 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)*.

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

[3]. 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.*

[4]. 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]. 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* .

[8]. Q.Hua Lin, Fu-Liang Yin, and Y.R. Zheng" Secure image communication using blind source separation*" 2004 IEEE.*

[9] . 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*

[10] .R. liu, X. tian "New algorithm for color image encryption using chaotic map and spatial bit level permutation *"Journal of Theoretical and Applied Information Technology 15 September 2012. Vol. 43 No.1 © 2005 - 2012 JATIT & LLS.*

[11]. 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*

[12]. 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*.