A Review Of Different Techniques Used In Image Encryption

Sunil Singh Rathode [1], Challa Srikar Reddy [2], Sai Praveen Reddy [3]
[1]Department of ECE, VignanaBharathi Institute of Tecnology, Aushapur-501301,
[2]Department of ECE, VignanaBharathi Institute of Tecnology, Aushapur-501301,
[3]Department of ECE, VignanaBharathi Institute of Tecnology, Aushapur-501301

in transmission is easily intercepted by unknown persons or hackers. In order to enhance the image information security, image encryption becomes an important research direction.In this paper, we survey on existing work which is used different techniques for image encryption and we also give general introduction about cryptography.

***Keywords*— Asymmetric key cryptography, Decryption, Encryption, Image encryption, Symmetric key cryptography,Visual cryptography,Facial blurring,Pixel shifting.**

I. INTRODUCTION

Security of data(image) to maintain its confidentiality, proper access control, integrity and availability is a major issue in data communication. As soon as a sensitive message was etched on a clay tablet or drawn on the royal walls, then it must have been foremost in the sender's mind that the information should not get intercepted and read by a rival.Codes, hence, form an important part of our history; starting from the paintings of Da Vinci and Michelangelo to the ancient Roman steganographic practices the necessity of data hiding was obvious.

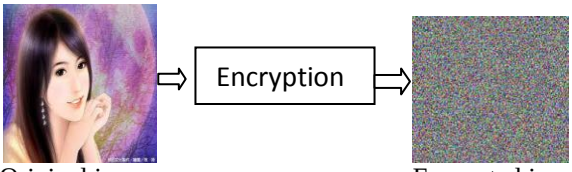
Cryptography, the science of encryption plays a central role in mobile phone communication, e-commerce, Pay-TV, sending private e-mails, transmitting financial information and touches on many aspects of daily lives

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

to cipher text is called Encryption or Enciphering.

Decryption: Restoring plain text from cipher text is called decryption or Deciphering.

Cryptography : The many schemes used for enciphering constitute the area of study known as cryptography.



Original image Encrypted image

Types of Cryptography:

There are two main types of cryptography:

- Secret key cryptography
- Public key cryptography
  - Hash function

Secret key cryptography is also known as *symmetric key* cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

Public key cryptography, also called *asymmetric key cryptography*, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys.

Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus.

Cryptography technique is used when secret message are transferred from one party to another over a communication line. 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.

To ensure this there are so many algorithams available to protect the images from unauthorized intruders.

II. Image Encryption Techniques

In this section, a few newly proposed techniques for image encryption, has been introduced.

1) *A New Block Image Encryption Algorithm by Fridrich, 1997*
Jiri Fridrich presented an encryption algorithm that adapted certain invertible chaotic two-dimensional maps to create new symmetric block encryption schemes. This scheme is especially useful for encryption of large amount of data, such as digital images.

2) *A Technique for Image Encryption using Digital Signatures, 2003*
Aloka Sinha and Kehar Singh have proposed a new technique to encrypt an image for secure image transmission. The digital signature of the original image is added to the encoded version of the original image. Image encoding is done by using an appropriate error control code, such as a Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver end, after the decryption of the image, the digital signature has been used to verify the authenticity of the image.

3) A Technique for Image Encryption using multi level and image dividing technique, 2003
Chang-Mok Shin**,** Dong-Hoan Seo**,** Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim[16] proposed image encryption by using binary exclusive OR operation and image dividing technique. They converted binary images to binary phase encoding and then encrypt these images with binary random phase images by binary phase XOR operation. Encrypted gray image was then obtained by combining each binary encrypted images.

4) Image Encryption Using Advanced Hill Cipher Algorithm
In this paper, we have proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption The objective of this paper is to overcome the drawback of using a random key matrix in Hill cipher algorithm for encryption, where we may not be able to decrypt the encrypted message, if the key matrix is not invertible. Divide the image into blocks apply the involutory key matrix to each block and create a temporary block using the ith pixel value of each block again multiply it with involuntary key matrix and find transpose of it transfer it to destination.

5) *Image Encryption Using Block-Based Transformation Algorithm,2006*
In this paper the original image is divided into random number of blocks the original image is divided into a random number of blocks that are then shuffled within the image. The generated (or transformed) image is then fed to the Blowfish encryption algorithm.

6) H-S-X Cryptosystem and Its Application to Image Encryption, 2009
In this paper, we have proposed a novel technique which is a modified version of Hill cipher algorithm for image encryption named H-S-X (Hill-Shift-XOR) which can be applied to any type of images whether they are colour or gray. First color image is decomposed into (R-G-B) components. Second, encrypt each component (R-G-B) separately by the algorithm. Finally, concatenate the encrypted components together to get the encrypted color image.

7) Image Encryption Using DCT and Stream Cipher, 2009
The proposed method based on the idea of decomposing the image into 8x8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT. Then, the DCT coefficients correlated to the higher frequencies of the image block are encrypted using Non-Linear Shift Back. The concept behind encrypting only some selective DCT coefficients based on the fact that the image details are situated in the higher frequencies, while the human eye is most sensitive to lower frequencies than to higher frequencies. Encrypt the selected coefficients by XORing the generated bit stream from the NLFSR +Key with the coefficient bits, the sign bit of the selected coefficients will not be encrypted.

8) Choase Based Image Encryption Using Block-Based Transformation Algorithm
The proposed algorithm is for image compression and encryption. The proposed algorithm with block size of 8-bit applies wavelet transform for each block for image compression and 256-bit secret key used for image encryption.The key is used to generate a pad that is then merged with the plaintext a byte at a time.

9) Fast encryption algorithm(FEAL)
The Fast Encryption Algorithm (FEAL) is a symmetric encryption algorithm, also called as Japanese Encryption algorithm.It is implemented using MATLAB. . For encryption, the input image is split into 16 sub-images of size 16x16 pixel resolution each. The sub images are encrypted separately and combined to get the actual encrypted image. Same process is used for decryption also. During decryption procedure, cipher image are converted into 16x16 pixel sub-images and the performed decryption key substitution.

10) A visual cryptographic encryption technique to secure medical images
In this encryption process, an input image which was

a plain image was operated on by a function to generate a secret key from it. The key was then used to encrypt the image by shuffling the pixels of the plain image based on an algorithm. The ciphered image was obtained at the end and it can either be stored or transmitted over a communication network. The received image was then operated on again by a function to obtain the key in order to decrypt the image.

11) A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption 2010

This 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.

12) An Efficient Encryption Algorithm Based on Image Reconstruction 2009

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.

13) Digital Image Encryption Algorithm Based on Chaos and Improved DES" 2009

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.

14) Matrix based Cryptographic Procedure for Efficient Image Encryption 2011

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 128bits 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.

15) An Efficient Chaos-based Image Encryption Scheme Using Affine Modular Maps 2012

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

16) New algorithm for color image encryption using chaotic map and spatial bit level permutation" 2012

This 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.

17) A cryptographic technique of facial blurring of images

In this method,the facial selected portion of image used will have their RGB colors are extracted from and then encrypted to have ciphered image portion.the ciphering of image for paper will be done by using the RGB pixel values of the selected portion of the images.there are no chages of the bit valuews and there is no pixel expansion at the end of the encryption process.instead the numerical values are transposed,reshaped and concatenated with the RGB values shifted away from its respective positions aand the RGB values interchanged in order to obtain the cipher image.This implies that the total change in the sum of all values in the image is zero.

18) Image encryption with combination of pixel rearrangement

For the pixel rearrangement, all the pixels of image are first stored in an array where array sorting is performed. By the sorting method, all the pixels are get compound sort in ascending order of any value i.e. R, G, B and the top we gets 0, 0, 0 pixel if present and 255, 255, 255 in the last position if present. Precedence of sorting is independent of value i.e. R, G, B because the motivation for sorting was reducing the correlation between pixel values. This correlation method by arranging the pixel values in sorting order is better than block shifting as discussed in earlier section.

III. Conclusion

At present times where major communication is done wireless using internet network to transfer data.so major concerns are regarding the security of such personal or nations defence data. In this paper, we have surveyed existing work on image encryption.we also discussed about cryptography and various techniques used for image encryption . We conclude that all techniques are useful for real-time image encryption. Techniques describes in this paper that can provide security functions and an overall visual check, which might be suitable in some applications. So no one can access image which transferring on open network.

In general, a well-studied, fast and secure conventional cryptosystem should be chosen, surely those algorithms, which provides higher security.

References:

[1] Ravi Shankar yadav,mhd.rizwan beg,manish madhava tripathi-image encryption technique a critical comparision-IJCSEITR-vol 3,issue 1 ,mar 2013 (67-74)

[2] William stallings, –Cryptography and Network Security:Principles & Practices‖, second edition.

[3] 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 272007.

[4] 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

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

[6] 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.

[7] 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.

[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] Ibrahim S I Abuhaiba , Maaly A S Hassan, –Image Encryption Using Differential Evolution Approach In Frequency Domain‖

[10] 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.

[11] 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.

[12] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, –Image Encryption Using Affine Transform and XOR Operation‖,International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).

[13] Sesha Pallavi Indrakanti , P.S.Avadhani,‖ Permutation based Image Encryption Technique‖, International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, 2011.

[14] Rasul Enayatifar , Abdul Hanan Abdullah, –Image Security via Genetic Algorithm‖, 2011 International Conference on Computer and Software Modeling IPCSIT vol.14.

[15] Komal d patel,Sonal belani||image encryption using different techniques:A review,2011 IJETAE vol 1,issue 1,nov 2011

[16] Kuldeep Singh, Komalpreet Kaur,‖ Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it‖, International Journal of Computer Applications (0975 –8887) Volume 23– No.6, June 2011.

[17] Rajinder kaur,ER.kanwalprit singh||image encryption techniques:A selected review,2013 (IOSR-JCE) vol9,issue 6,pp(80-83)

[18] Quist-Aphetsi Kester||a cryptographic image encryption technique for facial blurring of images(IJATER)vol3 issue 3 may 2013

[19] Qais H. Alsafasfeh , Aouda A. Arfoa,‖ Image Encryption Based on the General Approach for Multiple Chaotic Systems‖,Journal of Signal and Information Processing, 2011.