An Improved Cryptographic Technique to Encrypt Images using Extended Hill Cipher

Yashpalsingh Rajput
Research Scholar,
Government College of Engineering, Aurangabad

A K. Gulve
Asst. Professor,
Government College of Engineering, Aurangabad

ABSTRACT

This work proposes an improved scheme to encrypt the digital image for its security. The proposed system is divided into 3 main phases. In first phase, the single digit number into which the given digital image can be divided is calculated. In the second phase, bit rotation, reversal & randomization method is applied on each block of the image. In the third phase, the extended hill cipher technique is applied on the image which is an output of second phase. At the receiver end, if the receiver has appropriate decryption key, he can generate the image similar to the original image.

This paper is organized into following sections. Section 1 contains a general introduction to the cryptography, image encryption and hill cipher. Section 2 contains literature review on some existing image encryption research papers. Section 3 contains description of the proposed system. Finally paper is concluded in the Section 4.

General Terms

Image Security

Keywords

Cryptography, Image, Key, Encryption, Decryption, Hill Cipher

1. INTRODUCTION

Nowadays internet is going towards the multimedia data in which digital image covers large amount of it. But with the ongoing increasing use of multimedia applications, security risk against confidential data is also increasing [1]. Nowadays when larger amount of important and confidential information is stored on servers and transmitted over the internet. The security and safety of online information should be guaranteed. Digital image is also an important part of confidential information.

Security of any data like text information, digital images, etc. is an important aspect in communication and storage. Image security can be ensured by applying encryption to the digital images or by using various types of image watermarking techniques. Image watermarking techniques are used for copyright protection, authentication, etc. Image encryption techniques convert original digital image to encrypted image that is difficult to understand and to keeps the image confidential between users [2]. It is important that without decryption key no one can access the content. Image encryption has applications in online communication, multimedia systems, medical field, military communication; etc [3]. However, the traditional cryptosystems used for text encryption can also be used for image encryption, but it is not suitable for two reasons. One is that the digital images are usually larger in size than that of text. Therefore, the traditional system takes more time for encrypting the digital image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data [4].

Encryption is the process of transforming the data (text, image, or anything) into some other unreadable format using some mechanism so that any unauthorized person cannot read it or cannot understand. Only the authorized person i.e. a person who has an appropriate key can read original data.

Nowadays many types of sensitive & confidential information is stored on servers and transmitted over the web using e-mails, social network, etc. therefore security and safety of information should be ensured. Digital image is also an important part of our information. Therefore it's very important to protect our sensitive and confidential image from unauthorized disclosure. There are so many algorithms available to protect image from unauthorized access, some of which are briefly described in section 2.

1.1 Types of Cryptography

A technique in which secret or confidential messages are transferred in the encrypted form from sender to receiver over the communication line is called as Cryptography.

Cryptographic techniques are very useful to protect secret information. They protect the secret or confidential information by converting the information to some unintelligible form using a key. To retrieve the information, the encrypted information should be converted back to original information using some keys. Using different cryptographic techniques messages can be securely transmitted from one site to another. Cryptography technique needs some algorithm for encryption of data.

Based on the key, the cryptography can be classified into two categories [5]:

1. Symmetric key cryptography
2. Asymmetric key cryptography

Symmetric key cryptography sometimes also called as secret key cryptography or private key cryptography. In symmetric key cryptography, single key is used for encryption and decryption process i.e. using same key data can be encrypted and decrypted. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key. The sender and receiver must share same key. Digital image security can be achieved by applying standard symmetric key cryptography.

Asymmetric key cryptography sometimes also called as public key cryptography which uses different keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys. In public key cryptography, sender encrypts data using public key and sends it to one or more receivers. Each receiver can decrypt the data using their private keys.

Asymmetric key cryptography has very higher computational costs which are most of the time prohibitive for multimedia data. Symmetric key cryptography is comparatively lower cost and may be used for multimedia data. But the characteristic of multimedia data is totally different from text data. Text data does not possess any redundancy where as all multimedia data has got a lot of redundancy. The pixel value of a location shows strong correlation with the values of its neighboring pixels. This correlation proves to be attack points to any standard encryption algorithm. Because, if one can find out pixel value at any random point or location it can be easy for them to predict the pixel values of other neighboring pixels with somewhat variable accuracy using some prediction techniques.

The general image encryption process flow is shown in Figure 1.

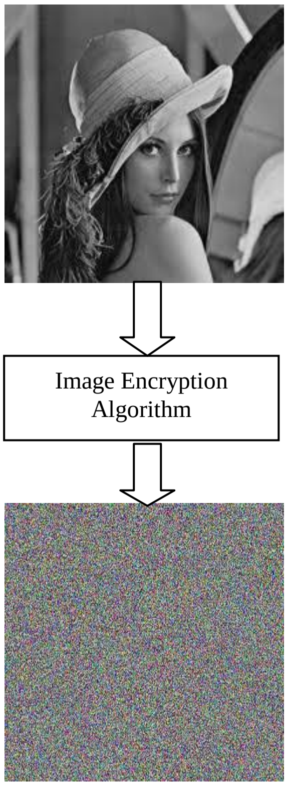

Fig. 1: Image Encryption

As shown in figure 1, a simple human readable image is converted to a form which is not readable to a human being using an image encryption algorithm. To get original readable image, the image must be decrypted using some key. There are so many image encryption algorithms available to protect image from unauthorized access which is described in section 2.

1.2 Hill Cipher

The Hill cipher (HC) algorithm is one of the famous and known symmetric key algorithms in the field of cryptography. It is a poly-alphabetic cipher based on linear algebra. It is proposed by the mathematician Lester Hill in 1929 in the journal of mathematics. Hill cipher requires a matrix based polygraphic system [6] [7].

For example {abcdef…} = ab cd ef… or abc def… and so on.

The core of Hill cipher is matrix manipulations. For encryption, algorithm takes *m* successive plaintext characters and instead of that substitutes *m* cipher characters. In Hill cipher, each character is assigned a numerical value like $a = 0$, $b = 1$, …, $z = 25$. The substitution of ciphertext characters in the place of plaintext characters leads to *m* linear equation. For $m = 3$, the system can be described as follows:

$$C=KP$$

where C and P are column vectors of length 3, representing the plaintext and ciphertext, respectively and K is a 3 x 3 matrix, which acts as key for encryption. All operations performed with modulus of 26. In Hill cipher key is an invertible m x m matrix, where m is block length. Decryption process uses inverse of matrix K. The inverse matrix K^{-1} of a matrix K is defined by following equation.

$$KK^{-1} = K^{-1}K=I$$

where 'I' is the identity matrix. But the inverse of matrix does not always exist and when it exists, it satisfies above equation. The inverse matrix K^{-1} is used to decrypt the ciphertext. In general it can be written as follows:

Encryption Process:

$$C=E_k(P)=Kp$$

Decryption Process:

$$P=D_k(C)=K^{-1}C= K^{-1}Kp=P$$

If the block length considered as m, there are 26^m different m characters blocks are possible.

2. LITERATURE SURVEY

This section consists of brief description of few image encryption methods.

2.1 A New Encryption Algorithm for Image Cryptosystems (2001)

This algorithm was proposed by Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen [4]. The method was based on vector quantization. The system was divided into three different phases. In encryption phase, vector quantization is applied for compressing the original image into a set of indices. In transmission phase, set of indices and encrypted data sent with a secret key to receiver by a public transmission channel. In decryption phase, receiver can decrypt the encrypted data using the secret key.

2.2 Lossless Image Compression and Encryption Using SCAN (2001)

This method was proposed by S.S. Maniccam and N.G. Bourbakis [8]. The method is only suitable for binary gray-scale images. This method performs two operations i.e. lossless compression and encryption of binary gray-scale images. The SCAN methodology is used to perform compression and encryption schemes. The SCAN is a formal language-based 2D spatial-accessing methodology generates a wide range of scanning paths or space filling curves.

2.3 Technique for Image Encryption Using Digital Signatures (2003)

This technique was proposed by Aloka Sinha and Kehar Singh [9]. In this technique, at the sender end the digital signature of the original image is added to the encoded version of the original image. A best suitable error code such as BCH (Bose-Chaudhuri Hochquenghem) code is followed for performing image encoding. At the receiver end, after decryption of that image, the digital signature verifies the authenticity of the original image.

2.4 Multi-Level Image Encryption by Binary Phase XOR Operation (2003)

The technique was proposed by Chang-Mok Shin, Dong-Hoan Seo, Kyo-Bo Cho, Ha-Woon Lee and So-Joong Kim [10]. They proposed a multilevel image encryption by using binary phase XOR operations and image dividing technique. They first divide a multilevel image to binary images having equal grey levels. Then binary image is converted to binary phase encoding and then these images are encrypted with binary random phase images by using binary phase XOR.

2.5 Image Encryption Using Block-Based Transformation Algorithm (2008)

The technique was proposed by Mohammad Ali Bani Younes and Aman [11]. The block-transformation and a popular encryption and decryption algorithm called Blowfish. The original image was divided into blocks and using the transformation algorithm it was rearranged and then the Blowfish algorithm is used for encrypting the transformed image.

2.6 Image Encryption Using Advanced Hill Cipher Algorithm (2009)

The method was proposed by Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda which uses an advanced Hill (AdvHill) cipher algorithm [12]. The advanced Hill cipher algorithm uses an Involutory key matrix for encryption.

They proposed AdvHill cipher algorithm using the old one. And it is observed that original Hill Cipher is unable to 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 gray scale as well as color images.

2.7 Image Encryption Using Affine Transform and XOR Operation (2011)

This method was proposed by Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar [13]. They introduced a new algorithm using affine transform which was based on shuffling the image pixels. The method consists of two phase encryption decryption algorithm. In first phase using XOR operation they encrypted the resulting image and in second phase using the affine transformation, the pixel values were redistributed to different locations with 4 bit keys. The transformed image then divided into 2 pixels X 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The result proves that the correlation between pixel values was significantly decreased after the affine transform.

2.8 SD-EI: A Cryptographic Technique to Encrypt Images (2012)

This technique was proposed by Somdip Dey [3]. The SD-EI technique consists of two stages: In first stage, each pixel of image is converted to its equivalent 8-bit binary number and in that 8-bit binary number; the number of bits equal to the length of password are rotated and then reversed. In second stage, extended Hill Cipher technique was applied by using involuntary matrix, which is generated by same password used in second stage encryption to make it more secure.

3. PROPOSED SYSTEM

In this section, the main idea used in the proposed system is described. As shown the diagram below, the proposed system, which is used to encrypt the image, is divided into the following 3 main phases:

Phase-1: Image is divided into 1 to 9 (N) horizontal blocks randomly depending on the number obtained from the key. By keeping first horizontal block as it is, all other horizontal blocks are replaced by the result of XOR of horizontal blocks with first horizontal block.

Phase-2: Image encryption technique by using bits rotation, reversal and randomization method based on key.

Phase-3: The Extended Hill Cipher technique for Image Encryption.

Each above phase consists of number of sub-phases. The detailed description for each of above phase is described as follows.

The flow for proposed system is shown in Figure 2.

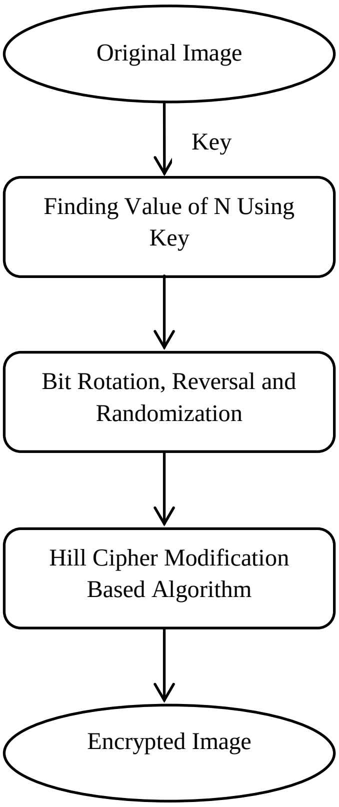
Original Image
Key
Finding Value of N Using Key
Bit Rotation, Reversal and Randomization
Hill Cipher Modification Based Algorithm
Encrypted Image

Fig. 2: Flow Diagram for Proposed System

3.1 PHASE-1: Image Blocks Generation

In order to disturb the correlation among pixels and increase the entropy value, the proposed system divides the images into the horizontal row-wise blocks and performs XOR of these blocks before passing the image to the encryption algorithm.

In this step, an image to be encrypted and a key is provided. The key provided consists of alphanumeric characters.

To divide the image into the random number of horizontal blocks is explained as follows.

Consider the example key provided is ‘image’.

First find the sum (MAINSUM) of ASCII values of each character in the key.
For given key ‘image’:

MAINSUM:= ASCII(i)+ ASCII(m)+ ASCII(a)+ ASCII(g)+ ASCII(e)

i.e. MAINSUM: = 105+109+97+103+101
MAINSUM: = 515

Now find sum of the digits in the MAINSUM and keep finding sum until we get a single digit number (FINSUM).
FINSUM: = SumofDigits (515)
FINSUM: = 5+1+5
FINSUM: = 11
11 is not a single digit number, to get a single digit number again add the digits of 11,

FINSUM: = SumofDigits (11)
FINSUM: = 1+1
FINSUM: =2

As FINSUM obtained is a single digit number it means final number will always be in between the numbers from 1 to 9. Then divide the digital image into the number of horizontal blocks depending on the value of FINSUM. It means image can be divided into the numbers of horizontal blocks in the range from 1 to 9.

Here FINSUM: = 2,
The image is divided into 2 horizontal blocks.

After dividing the images into n numbers of rows, and keeping first horizontal block as it is, and all other horizontal blocks are replaced with the result of XOR of the corresponding horizontal block with first horizontal block. i.e. each horizontal block is XORed with first horizontal block. Here first horizontal block acts as a key for XOR operation. Original image blocks can be recovered by XORing the result block again with first horizontal block.

3.2 PHASE-2: Bits Rotation, Reversal and Randomization

In this phase, value of each pixel of the image obtained as the result of PHASE-1 is converted into equivalent 8-bit binary number. Now length of key is considered for bit rotation and reversal. i.e., Number of bits to be rotated to left and reversed will be decided by the length of key. Let L be the length of the key and L_R be the number of bits to be rotated to left and reversed [3]. The relation between L and L_R is represented by following equation.

$$L_R = L \bmod 7$$

where ‘7’ number indicates the number of iterations required to reverse an entire byte.
After bit rotation and reversal, randomization technique is applied. Instead of making use of inbuilt randomization techniques the proposed system uses shifting operation for randomization of image bits. It uses a sequence of shifting operations in anticlockwise direction i.e. left shifting, down shifting, right shifting and up shifting operations on the image bits. By performing different shifting operations on the bits, the bits get shifted accordingly which affects on the weight of the image pixels and correlation among image pixels.

Since, the color of each pixel is decided by the weight of that pixel; the change occurred in the weight of each pixel of input image due to Bits Rotation, Reversal and Randomization generates the encrypted image. Anyone knowing a pixel value may predict the neighbor pixel values reasonably well using some prediction techniques. So, the proposed system breaks this correlation among image pixels by performing Bits Rotation, Reversal and Randomization operations.

3.3 PHASE-3: The Extended Hill Cipher Technique for Image Encryption

Hill Cipher does not hide all features of the images containing large areas of single color. Recent research and development efforts have been done to improve the security of Hill Cipher.
The proposed work uses extended hill cipher technique for image encryption which is presented by Somdip Dey in [3].

4. CONCLUSION

This method of encryption can be applied to any of the formats of images like jpg, tiff, png, etc. The proposed system is an improvement over existing digital image encryption methods using a combination of block based image transformation and encryption techniques. Correlation among pixels was decreased when the proposed method was applied to the blocks.
For better transformation the block size should be small, because fewer pixels keep their neighbors. In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. The future work for this system is to make modifications so that the system will work for stegano images.

5. ACKNOWLEDGMENT

Yashpalsingh Rajput expresses his gratitude to all the faculty members of the Computer Science Department, Government College of Engineering, [Autonomous], Aurangabad, India, for their support and enthusiasm. He also thanks to Prof. A. K. Gulve, Professor, Computer Science & Engineering Department, Government College of Engineering, [Autonomous], Aurangabad, for his constant support and helping out with the preparation of this paper.

6. REFERENCES

[1] Abhinav Srivastava, “A survey report on Different Techniques of Image Encryption”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Vol. 2, Issue 6, June 2012, pp. 163 - 167.

[2] Rajinder Kaur, Er. Kanwalpreet Singh, “Comparative Analysis and Implementation of Image Encryption Algorithms”, International Journal of Computer Science and Mobile Computing, Vol. 2, Issue 4, April 2013, pp. 170 – 176.

[3] Somdip Dey, “SD-AI: A Cryptographic Technique to Encrypt Images”, International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 26-28 June 2012, pp. 28 - 32.

[4] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, “A New Encryption Algorithm for Image Cryptosystems”, The Journal of Systems and Software, Vol. 58, 2001, pp. 83 – 91.

[5] Garry C. Kessler, “An Overview of Cryptography”, http://www.garykessler.net/library/crypto.html#intro

[6] “Practical Cryptography - HILL CIPHER”, http://practicalcryptography.com/ciphers/hill-cipher/

[7] Vidit kumar Singh, "Hill Cipher–Essays-Vidschauhan", http://www.studymode.com/essays/Hill-Cipher-1592453.html

[8] S. S. Maniccam, N. G. Bourbakis, "Lossless Image Compression and Encryption Using SCAN", Pattern Recognition, Vol. 34, 2001, pp. 1229 - 1245.

[9] Aloka Sinha and Kehar Singh., "Technique for Image Encryption Using Digital Signatures", Optics Communications, ARTICLE IN PRESS, 2003, pp. 1 - 6, www.elsevier.com/locate/optcom

[10] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Cho, Ha-Woo Lee and Soo-Joong Kim, "Multi-Level Image Encryption by Binary Phase XOR Operations", The 5th Pacific Rim Conference on Lasers and Electro-Optics, CLEO/Pacific Rim 2003, Taipei 106, Taiwan, 15-19 Dec. 2003.

[11] Mohammad Ali Bani Younes and Aman, "Image Encryption Using Block-Based Transformation Algorithm", in IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03, February 2008.

[12] 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, pp. 663 - 667.

[13] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar, "Image Encryption Using Affine Transform and XOR Operation", International Conference on Signal Processing, Communication, Computing and Networking Technologies, 2011, pp. 309 - 312.