A Crypto Key Generation from an Image with Application of Chinese Remainder Theorem

E. Pragnavi¹, G. Kishore Kumar²
Assistant Professor, Department of CSE, UCE (A) OU, Hyderabad, Telangana, India¹
Assistant Professor, Department of ECE, UCE (A) OU, Hyderabad, Telangana, India²

ABSTRACT: For secured communication, several methods in cryptography have been proposed. These encryption mechanisms has greater importance as they are used for enhancing the security of information but there are many issues to be addressed in them and are abused by the unauthorized parties. Cryptography means encryption and decryption of information using keys generated by various algorithms. Such algorithms have a disadvantage of difficulty in remembering the keys which can also be easily traced, shared and stored. In this era, Cryptography with images has gained great attention due to importance of images in most of the multimedia applications. In this paper, we propose a novel Chinese Remainder theorem (CRT) based technique where images are used in generation of key. In our approach, from the selected pixel values of a selected image the key for encryption and decryption is generated with CRT. Results shows that such keys from images with CRT are secure, stronger and also suitable keys of variable length can be obtained.

KEYWORDS: Encryption, Decryption, Information security, Images, CRT, key

I. INTRODUCTION

Data secrecy has become a great issue in multimedia data transmission applications as unauthorized access to data is increasing. To overcome such unauthorized accesses or modifications to information and to protect valuable information various types of cryptographic methods are introduced. Changing the original data to unreadable form using a key is the concept of cryptography. The key used here is generated involving typical process where the cryptanalyst cannot crack the key. Based on the utilization of the key there are two types of approaches existed in cryptography.

a) Symmetric Cryptography- a common key between the sender and receiver for encryption and decryption. Examples include AES, IDEA, DES etc

b) Asymmetric Key Cryptography-two keys exists for encryption and decryption process, one key named as public key and other as private key. Examples include RSA, Diffie-Hellman

The characteristic features that are considered for evaluating the strength of cryptographic algorithms are the functions used in sub key generation, size of the key, rounds involved in the key generation of the algorithm etc. Hence key generation process and the relation between key and algorithm should be made very typical. This can be attained by increasing the complexity in key generation process using images and an application technique Chinese Remainder Theorem. In this paper to make the key more secure, complex and strengthened, images and CRT are used where it becomes very difficult to crack the key by a cryptanalyst. The key to be selected for encryption depends on the key length required for an algorithm and the different values generated from the image based key generation process.

In this paper, a key is generated from the pixel values of selected points on a selected image and with the application of CRT. The input which is an RGB image is resized to particular size. The end user is allowed to select certain points on this resized image. Then the selected point pixel values on resized image are considered to form an output shown in matrix form. From this matrix randomly a set of numbers are selected and are verified for relative prime condition. Then CRT is applied on this relative prime set which results to set of keys. From this set of keys one value is randomly selected which will be a key of variable length for an encryption algorithm for online transmission of information. Our survey explains the usage of images in different methodologies which led to our new proposal.
A novel authentication method for a hand held phone with camera was proposed in [1] by Tetsuji Takada and Hideki Koike. Instead of text based passwords it uses user defined images. This method comprises of two steps firstly image registration and then notifications. Initially user registers his/her favorite images referred as pass image and later the user receives a mail on registered image for successful authentication.

A CRT based watermarking technique was proposed for authentication of multimedia contents in [2] by Jagdish.C.Patra, A.Karthika, Cedric Bornand. This technique involves embedding and extraction procedures. In embedding procedure the given image is divided into number of equal sized blocks based on number of watermark bits to be embedded. Applying CRT on the pixel intensity values of blocks, construction of new watermarked pixel values is obtained which are to be embedded in the blocks with some conditions satisfied. Finally, the extraction procedure is reverse of the embedded procedure with comparisons.

In this paper [3] by Ashraf Odeh, Aymen Abu-Errub, generation of key for encryption using binary image was proposed. In this approach, a 16x16 binary array of digital image is obtained which is later converted into 4x4 arrays. From this 4x4 decimal array is obtained. The new generated decimal array and the left diagonal of the original array are used in the generation of key which is used to encrypt the data. On the receiver side the process is repeated for generation of private key for decryption.

A fast algorithm is proposed in [4] by Abdulrahman Dirar Khalaf to encrypt and decrypt color image which involves two steps Image key generation and Image encryption. In this paper, initially the algorithm is designed to generate image key from the same image or any image selected by the sender and this selected image is rotated in three directions, cut, scrambled and XOR’ed to generate image key. Secondly, Image encryption will be completed by using XOR logic between the image key generated and scrambling image where scrambling occurs using Inverse Wavelet Transform obtaining the ciphered image. Decryption image can be obtained by reverse algorithm using the same symmetric key.

An image encryption method was proposed by considering the pixel level values of the image. In this paper [5] by Quist-Aphetsi Kester, the Red Green Blue color values of the image are obtained separately and each represented in 1 dimensional form. Then all these are shown in column matrix and later transpose of the matrix is calculated forming final matrix. Finally the ciphered image is obtained by considering the part values of the final matrix. To obtain the original image applies the method in reverse order.

For Image Cryptosystems, New Encryption Algorithm proposed by Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen [6]. During encryption, the image is compressed using a popular image compression technique named vector quantization concept and encrypted. This proposal achieves high security and low computations during encryption and decryption of images.

Seyed Mohammad Seyedzade, Reza Ebrahim Atani and Sattar Mirzakuchaki [7] proposed an algorithm based on SHA-512 hash function. Initially the image is divided into two halves. The algorithm consists of two sections in which one section deals with pre-processing of half image in order to shuffle the image data and the second section hash function is applied to obtain random number mask. This masked output is exclusively ORed with second half of the image for encryption.

A new and effective image encryption method using Differential Evolution Approach proposed by Ibrahim S I Abuhaiba and Maaly A S Hassan [8]. In this, 2D keyed Discrete Fourier transform is applied on the image which is to be encrypted and then the concepts of linear feedback shift register index generator, keyed mutations and simple diffusion mechanisms are used in the encryption process. The invertible process with same key for decryption.

New Image Encryption technique [9] based on the general approaches of Multiple Chaotic Systems proposed by Qais H. Alsafasfeh and Aouda A. Arfoad[9]. In this technique the Lorenz chaotic system and the Rossler chaotic system are used such that the pixel values of the image are shuffled and change the grey scale values to obtain encrypted image. This paper shows high security and high speed are the advantages from experimental analysis.

In this paper [10], a new biometric authentication system using finger-knuckle-print (FKP) imaging is proposed by Lin Zhang, Lei Zhang, David Zhang, Hailong Zhu. To capture the FKP images a specific device is constructed which are stored in an image database. The process carries on with local coordinate system and feature extraction. For matching two FPKs, a feature extraction scheme, which combines orientation and magnitude information extracted by Gabor filtering, is proposed achieving higher recognition rate.

Gaetan Le Guelvouit proposed an approach for public key steganography [11]. A warden concept is used in traditional public key steganography for sharing secret information which suffers from some issues. These can be
overcome by using same framework with trellis-coded quantization techniques leading to design of a more effective public-key scheme.

An authentication method for a moving image have been proposed in [12] by Ren Fujii, Yasunari Yoshitomi, Taro Asada, Masayoshi Tabuse. This paper proposes two methods i.e an authentication method for a moving image by using discrete wavelet transform and a method for selecting several frames in the moving image. This method avoids insertion of additional information into the actual moving image and encourages to used the extracted features of the image for authentication.

This paper continues with section 2 as problem statement with methodology and results, section 3 as future scope and conclusion.

II. PROBLEM STATEMENT

Information transmission through online without any breaches is the challenging task. To acquire this, a numerous techniques have been proposed. Presently, most of the applications are dealing with images to secure information transmissions. Use of images in Cryptography is the upcoming concept where the role of images is playing a prominent role. One of the novel techniques proposed by us using images is generation of a variable length key from pixel values of selected points on image with Chinese Remainder Theorem (CRT). As such the key can be more secure and strengthened for encryption algorithms and can form an efficient method for key generation of encryption algorithms.

2.1 Key Generation Technique:
This section continues with the technique of generation of key from images and CRT for encryption and decryption process. Initially a set of RGB images are displayed from which an image is selected and resized. This resized image is shown to end user where the end user has to select certain number of points on the resized image. Then the selected point pixel values of the image are displayed as a result. Then based on the predefined number, those many number of values are selected randomly from the displayed selected point pixel values. These randomly picked values are verified for relative prime condition. If the numbers are relatively prime, apply them as input to CRT. To secure key, make key disclosure, more complex and to make key stronger Chinese Remainder Theorem (CRT) is used. A set of values as a result of CRT forms a source for random selection of variable length key. A variable length key is selected accordingly to the algorithm in information encryption and decryption process.

**Chinese Remainder Theorem**

- Let $a_1, a_2, \ldots, a_n$ be pair wise relatively prime positive integers and let $b_1, b_2, \ldots, b_n$ be any integers. Then the system of linear congruence’s in one variable given by

$$X \equiv b_1 \mod a_1$$
$$X \equiv b_2 \mod a_2$$

... $\ldots$
$$X \equiv b_n \mod a_n$$

has a unique solution modulo $a_1a_2\ldots a_n$

**Applications of Chinese Remainder Theorem**

- Construction of Sequence numbering of Godel numbering uses the Chinese remainder theorem in the proof of Gödel's incompleteness theorems.
- Chinese Remainder theorem used in reduction in the computation of a Fast Fourier transform of size $n1n2$ to the computation of fast Fourier transforms of smaller sizes $n1$ and $n2$ by Good Thomas algorithm.
- Chinese Remainder Theorem used in most of the implementations of RSA during signing of HTTPS certificates and also used in secret sharing.
- One of the special applications includes techniques of Range ambiguity resolutions used with radar of medium pulse repetition frequency.
2.2 Methodology of applying CRT onto the selected points on image to get variable length Key for Encryption Algorithm:

- **Step 1**: During encryption process, a set of RGB images are displayed, of which an image is selected and resized.

- **Step 2**: On the resized image, a set of selection of points are performed generating pixel values of the selected points. These selection points can be limited to fixed number i.e \( M_\text{c} = 1, 2, \ldots k \). Our approach limited to 8 i.e \( M_\text{c} = 1, 2, \ldots 8 \). Then a matrix of size \((M_\text{c} \times 3)\) i.e \( F_v (M_\text{c} \times 3) \) is obtained considering the pixel values of mouse clicked points on image.

  Matrix \( F_v (M_\text{c} \times 3) \) where \( M_\text{c} \) is the number of selected points and 3 represents the Red, Green, Blue pixel values as columns.

- **Step 3**: From matrix \( F_v \), select a number of non-zero values based on the symmetric algorithm used. 
  \( M=\text{random}(x, F_v) \) where \( x \) is a variable defining number of values to be selected from \( F_v \).

- **Step 4**: These \( M \) numbers selected say \( M_1, M_2, M_3 \) from \( F_v \) are verified for relative prime relation.

- **Step 5**: For the CRT algorithm the above selected relative prime numbers are used as inputs. The result of CRT is \( P \) number of values which forms a source for random selection of variable length key. This variable length key which is randomly selected from \( P \) is used in information encryption and decryption process.

  \[ P = \text{CRT} (M_1, M_2, M_3) \]
  \( P \) means \{P1, P2, P3, P4 \ldots P\r\} where \( P \) is the result of CRT which forms a source for variable length keys \( P_1, P_2, P_3, \ldots P_r \).

- **Step 6**: From the above steps, from a single selected image \( P \), number of values generated which are forming sources for keys of encryption algorithms. The total number of \( P \) values increases as the \( M \) values increases which are used as keys in symmetric encryption algorithms.

2.3 Experimental Results

- **Input**: An image selected from given set of RGB images

**Results:**

**STEP 1: For generation of Resized Image from RGB image**

Fig 1:- Original Image

Fig 2:- 40 x 40 Resized Image
**STEP 2:** On the resized image, a set of selection of points on resized image is performed to obtain pixel values of selected points

![Selected points on the resized image](image)

**Step 3: Matrix from Selected points on image**

$$F_v = \begin{bmatrix}
169 & 202 & 239 \\
158 & 196 & 239 \\
196 & 227 & 238 \\
210 & 236 & 245 \\
197 & 107 & 61 \\
184 & 78 & 18 \\
\end{bmatrix}$$

![Matrix F_v generated from the selected points of the image](image)
M = random(x, Fv), x = 8 where x is a variable defining number of values to be selected from Fv.

i.e 210 239 61 78 236 196 107 197

**STEP 4:** Above randomly selected numbers of STEP 3 are verified for Relative prime condition

M1 = 239, M2 = 236, M3 = 107 are RELATIVE PRIME NUMBERS

**STEP 5:** Above relative prime numbers are taken as inputs to CRT and the output of CRT is P number of values which forms a source for random selection of variable length key are as shown.

As an example one of the randomly selected numbers from Step V is the key used in Encryption algorithms say DES algorithm.
III. CONCLUSION AND FUTURE SCOPE

In this paper the concept runs on how to generate the key from images and how to strengthen and secure the key for encryption algorithms. In our proposal the concentration is on the key which is most important for any encryption algorithms. In this, by considering image pixel values of the selected points, matrix is formed of which certain numbers are selected and are furthered used as a key for any encryption algorithms with the application of CRT. The concept can also be extended by increasing the number of input values to CRT as our approach has been limited to three numbers. The CRT results can also be extended for more good results. For secure information transformation our approach can form strong method during key generation. Our approach becomes complex for an attacker to predict the key as it is generated from images and CRT. Predicting an image and process of key generation for an attacker is impossible as the approach is image dependent for encryption algorithms. Results could be better if such work is implemented in real time systems.

REFERENCES

1. Tetsuji TAKADA1 and Hideki KOIKE2, Aware-E: Image-based Authentication for Mobile Phones using User’s Favorite Images