www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 11793-11796

"An Effective Image Encryption Based On The Combination Of Scan And Elgamal Method"

Mr. Ravi Mohan [1] Hira Lal Dhruw[2] Raghvendra[3]
Asst. Prof. & HOD
Shri Ram Institute of Science & Technology
Jabalpur (M.P.), India
Department of Electronics and Telecommunication Engineering
M. Tech (VLSI Design) Scholar,
hira.dhruw@gmail.com
Shri Ram Institute of Science & Technology
Jabalpur (M.P.), India
Dept.of Electronics and Telecommunication Engineering
M.E. (CSE) Scholar,
patel.raghvendra@gmail.com
Shri Ram Institute of Science & Technology
Jabalpur (M.P.), India
Dept. of Computer Sc. & Engineering

***Abstract*—** The requirements of information security within an organization have undergone tremendous changes. Before the widespread use of data processing equipment, the security of sensitive documents depends on filing cabinets with a combination lock for storing paper-based files or documents. However the scenario has change with the introduction of computer in handling businesses in organizations. At the same time, advances in networking and communication technology bring the business organizations worldwide working together as one entity. Due to the impact of this globalization, vast amount of various digital documents such as texts, images, videos, or audio travels from one destination to another via the network line. However some of these documents might be sensitive and confidential and therefore need to be protected. Image Encryption is the process of encoding messages in such a way that eavesdroppers or hackers cannot read it, however that authorized parties. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private.

1.0 INTRODUCTION

The main aim of this thesis is to develop a novel encryption algorithm for increasing the security of encryption so that only the intended person is able to decrypt the image. In this algorithm, original image is first encrypted using SCAN based encryption operation followed by Elgamal based encryption method.

1.1 DIGITAL IMAGES

Digital images are composed of pixels (short for picture elements). Each pixel represents the color (or gray level for black and white photos) at a single point in the image, so a pixel is like a tiny dot of a particular color. By measuring the color of an image at a large number of points, we can create a digital approximation of the image from which a copy of the original can be reconstructed. Pixels are a little like grain particles in a conventional photographic image, but arranged in a regular pattern of rows and columns and store information somewhat differently. A digital image is a rectangular array of pixels sometimes called a bitmap.

1.2 TYPES OF DIGITAL IMAGES

1.2.1 Black and White Images

Figure 1.2.1: (a) Black and white image.
(b) Black and white image with gray scale.

1.2.2 Color Images.

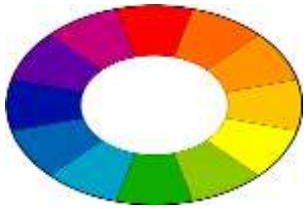


Figure 1.2.2: Color image

1.2.3 Binary or Bit level Images.

Figure 1.2.3: Binary image

1.2.4 Indexed Color Images.

Figure1.2.5: Indexed color image

1.3 GOALS OF CRYPTOGRAPHY

Cryptography is a study of techniques (called cryptosystems) that are used to accomplish the following four goals.

1.Confidentiality.
2.Data integrity.
3.Authentication.
4.Non-repudiation.

1.4 PRINCIPLES OF ENCRYPTION

The basic idea of encryption is to modify the message in such a way that only a legal recipient can reconstruct its content.A discrete-valued cryptosystem can be characterized by:

A set of possible plaintexts, P.
A set of possible cipher texts, C.
A set of possible cipher keys, K.
A set of possible encryption and decryption transformations, E and D.

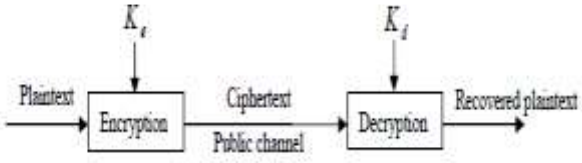
An encryption system is also called a cipher, or a cryptosystem. The message for encryption is called plaintext, and the encrypted message is called cipher text.

$$C = E_{K_e}(P)$$

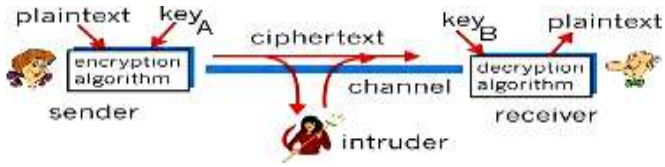
Similarly, the decryption procedure is defined as:

$$P = D_{K_d}(C)$$

A block diagram for encryption/decryption of a cipher.



(a)



(b)

Figure.1.4: Encryption/Decryption of a cipher.

1.5 CLASIFICATION OF ENCRYPTION ALGORITHEMS.

1.5.1Classification According to Encryption Structure.
1.5.2 Classification According to Keys.

1.6 There are two types of cryptosystems:

1.6.1 Symmetric (private) key cryptosystems.
1.6.2 Asymmetric (public) key cryptosystems.

Most people have chosen to call the first group simply symmetric key cryptosystems, and the popular name for the second group is just public key cryptosystems.

1.7 ELGAMAL ENCRYPTION.

This method is based on the fact that if p is a large prime number then the primitive root of this number p is a number r which satisfy the following property [45]

R (mod p) $\neq r^2 \pmod p \neq r^2 \pmod p \neq \ldots \neq r^{p-1} \pmod p \neq 0 \ldots$

i.e. mod of p taken over the power of number r yield distinct and non-zero number and all are also relative prime to p. For example consider a prime number 7.The primitive root can be any integer number from 1 to 6 which satisfy the equation (1).From the table it is clear that only number 3 and 5 satisfy the equation (4.1) and hence these number are primitive root of prime number 7.

r1	r2	r3	r4	r5	r6
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	3	1	5
6	1	6	1	6	1

Figure 1.7: Prime numbers for Elgamal encryption

1.7.1 PROCEDURE FOR ELGAMAL ENCRYPTION.

In this method a user has to choose the private key on the basis of which, a public key is calculated. Let p be a prime number of large value and α be the primitive root of p. Suppose the selected private key is represented by r then the public key β is computed by

$$\beta = \alpha^r \pmod{p}$$

Choose any random integer and compute b by

$$b = \alpha^k \pmod{p}$$

If the plain text is T then compute cipher text by

$$C = \beta^k T \pmod{p}$$

Now, for decryption at the receiver side can be computed by

$$T = C b^{-r} \pmod{p}$$

This is due to the fact that

$$C\, b^{-r} = \beta^k T (\alpha^k)^{-r}$$
$$= (\alpha^r)^k T (\alpha^k)^{-r}$$
$$= \alpha^{rk} = T$$

(4.6)

Algorithm steps for Elgamal method are as follows-

1.7.2 ENCRYPTION PROCESS

Step 1 First of all choose any large prime number p
Step 2 Compute the primitive root of p and choose any one primitive root α.
Step 3 Select a private key 'a' and compute the corresponding public key using equation 4.2.
Step 4 Take the first pixel of the Red channel and encrypt it using equation 4.4 for a selected random number 'k'
Step 5 Repeat step 4 for the pixel of Green channel
Step 6 Repeat step 4 for the pixel of blue channel.
Step 7 Repeat step 3 to 6 till the entire pixel gets encrypted.
Step 8 Merge all encrypted Red, Green and Blue pixel to get the encrypted image.

1.7.2 DECRYPTION PROCESS

Step 1 Get the encrypted image and separate the Red, Green and Blue channel.
Step 2 Compute the value of 'b' using equation
Step 4 Take the first encrypted pixel of Red channel and decrypt it using equation .
Step 5 Repeat step 4 for Green and Blue channel.
Step 6 Merge all the decrypted Red, Green and Blue pixel to get back the decrypted image.

1.8 PROPOSED METHOD

Proposed encryption process consists of two part .The first part encrypt the original image using scanning technique. Scanning technique works by changing the pixel position only. The value of each pixel remain intact. In the second part the encrypted image obtained by the first part is again encrypted using Elgamal method.

1.9 ENCRYPTION PROCESS

Encryption process is summarized as-

1. Get the Original Image.
2. Encrypt the Image by applying SCAN method and generate the key1.
3. The encrypted image obtained after step 2 is again encrypted by applying Elgamal method as described above and using key2. The whole process of encryption is shown by flowchart and schematic diagram.

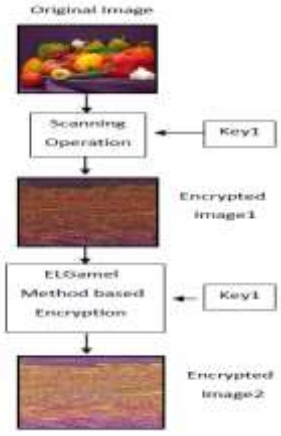


Figure 1.9: Encryption Process Schematic diagram

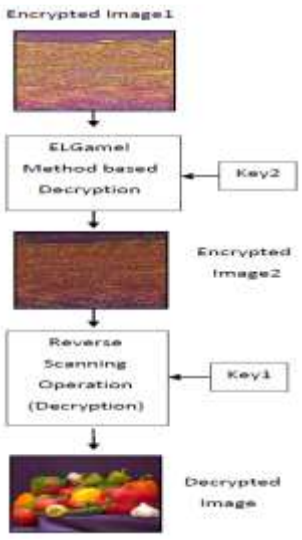


Figure 1.9: Schematic diagram of Decryption process

1.10 GOAL OF THESIS

The main aim of this thesis is to develop a novel encryption algorithm for increasing the security of encryption so that only the intended person is able to decrypt the image. In this algorithm, original image is first encrypted using SCAN based encryption operation followed by Elgamal based encryption method.

1.11 FUTURE SCOPE OF WORK

Extensions of this work could be the investigation of new scanning patterns applied efficiently to image processing. Such texture synthesis using SCAN words matrix elements rearrangement for parallel storage and manipulation. In future work we will implement it in hardware using DSP chip, and accelerate the process speed.

1.12 CONCLUSION

There are so many technique to make an image secure. In this research we define so many techniques. Some of the encryption techniques used selective part of an image for encryption and some others apply encryption algorithm on whole image bit by bit. Each technique has its own suitability area. Each technique has its own limitations.

1.13 REFERENCES

[1] Mazleena Salleh, Subariah Ibrahim & Ismail Fauzi Isnin *"Image Encryption Algorithm based on chaotic Mapping"* Jurnal Teknologi, 39(D) Dis. 2003: 1–12 Universiti Teknologi Malaysia

[2] S.lian " *Multimedia Content Encryption : Techniques and Application"*, CRC,2008.

[3] www.google.com.

[4]www,Wikipedia.com.

[5] Jonathan Sachs,"*Digital Image Basics"*,1996-1999

[6] B. Schneier, "*Applied Cryptography"*, Second Edition, John Wiley and Sons, New York, 1996.

[7] L. Kocarev*, "Chaos-Based Cryptography: A Brief Overview*", IEEE Circ. Syst. Mag., Vol. 1, No. 3, pp. 6 21, 2001.

[8] D. Stinson*, "Cryptography: Theory and Practice"*, (2nd) Chapman & Hall / CRC Boca Raton, USA, 2002.

[9] Y. Mao, S. Lian, and G. Chen, "*A novel fast image encryption scheme based on 3D chaotic Baker maps*." International Journal of Bifurcation and Chaos, vol. 14, no. 10, pp. 3616–3624, 2004.

[10] S. Li*, "Analyses and New Designs of Digital Chaotic Ciphers"* , Ph. D. Thesis, School of Electronics & Information Engineering, Xi an Jiaotong University, Xi an, China, June 2003