ISSN (Online): 2455-7838
SJIF Impact Factor (2015): 3.476

EPRA International Journal of

Research & Development

(IJRD)

Volume:1, Issue:5, July 2016

Published By :
EPRA Journals

SJIF Impact Factor: 3.476 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 1 | Issue: 5 | July | 2016

A RESEARCH ON "A MODIFIED TECHNIQUE FOR GENERATION OF KEY FROM 2D GRAPHICS IMAGE FOR CRYPTOGRAPHY"

Ku.Prerana Bul[1]
[1]Department of Electronics & Telecommunication,
Sipna College of Engineering & Technology, Amravati, India

Prof. A. V. Malviya[2]
[2]Department of Electronics & Telecommunication,
Sipna College of Engineering & Technology, Amravati, India

ABSTRACT

Cryptography is basically securing data during the communication between different systems. To provide the security of data during communication in cryptography we together require the Algorithm and Key. The confidentiality and integrity of the data during communication depends partially on algorithm and partially on key. Due to human perception the size of key in cryptography is limited. 2Dimension graphics image is not possible to design exactly the same pattern. In this paper a modified technique is being proposed for increasing the security of the data. For increasing the security we are basically concentrating on the key part of the cryptography we basically uses the 2Dimension graphics image which is designed by the user. Cryptography consists of encryption and decryption. We concentrate on encryption and decryption for generation of key. 2Dimension Graphics image is composed of pixels in which each pixel have different or same ASCII value. We used hexadecimal or 2D graphics image as in the form of generation of key. From the large collection of pixel the proposed algorithm will generate key which can be used in encryption as well as in decryption.

KEYWORDS: *Cryptography, Encrypting, Decrypting, Key, Human-Memorizability, Confidentiality, Integrity, 2D Graphics Image, Pixel, Randomization.*

I. INTRODUCTION

In Today's world many systems are going to provide their services online. For example every business, Government Sector, Banking Sector, Education System etc is going to be provide their services online. As these services are going to online there is a lot of probability that these services are going to be cracked or hacked by the unauthorized user. So to provide the integrity, security, confidentiality of services during all these communication some techniques has been developed. Among all these parameters security is one of the major concern in Internet. Steganography is the way to provide the security by hiding the original data. In this paper we used hash technique.

Covering media will hold the original data and it is split ted throughout the covering media. Secret message is the original data. Steganography function will perform the operation of placing the original data in the covering media and its inverse function will do the reverse operation.Optional steganography key is optionally required in the steganography function [1].

Cryptography is also one of the ways to enhance the

Security during the communication. Cryptography involves two techniques one is converting the plain text (i.e. understandable format) into cipher text (i.e. Non understandable format) & Decryption is converting the cipher text into plain text. To perform the Encryption and Decryption on data we require two things one is algorithm and another is key. This Cipher text is transmitted in the open network to reach at the receiver side. On the receiver side when the cipher text is reached than cipher text together with key is again applied in the algorithm to get the desired output (i.e. Plain text) Cryptography is applied in different field (i.e. it can used to encrypt image, audio, video, text) For generating the cipher text from the plain text the algorithm performs two processes one is Substitution and another is Transposition. Substitution is substituting the original character with some another character and Transposition is doing the permutation among the original characters (i.e. it shuffles the position of original character from their original places) [2]. To enhance the security in cryptography we can either modify the algorithm or we can modify the key generation technique. In this paper we have concentrated on the key part of the cryptography we have proposed one modified approach of key generation and manipulation technique using 2D graphics image.2D graphics image have the property that by simply viewing or listening its dimensions it is not possible to design the same Graphics image. Digital images are composed of pixels. 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. A digital image is a rectangular array of pixels sometimes called a bitmap. Types of Digital Images For photographic purposes, there are two important types of digital images—color and black and white. Color images are made up of colored pixels while black and white images are made of pixels in different shades of gray. Black and White Images a is made up of pixels each of which holds a single number corresponding to the gray level of the image at a particular location. These gray levels span the full range from black to white in a series of very fine steps, normally 256 different grays. Color Images is made up of pixels each of which holds three numbers corresponding to the red, green, and blue levels of the image at a particular location. Red, green, and blue are the primary colors for mixing light—these so-called additive primary colors are different from the subtractive primary colors used for mixing paints (cyan, magenta, and yellow). Any color can be created by mixing the correct amounts of red, green, and blue light. Binary images use only a single bit to represent each pixel. Since a bit can only exist in two states—on or off, every pixel in a binary image must be one of two colors, usually black or white. This inability to represent intermediate shades of gray is what limits their usefulness in dealing with photographic images. Indexed Color Images are created using a limited palette of colors, typically 256 different colors. These images are referred to as indexed color images because the data for each pixel consists of a palette index indicating which of the colors in the palette applies to that pixel. There are several problems with using indexed color to represent photographic images.

II. RELATED WORK

Xiukun Li *et.al*, [1] have proposed A Novel Cryptographic Algorithm based on Iris Feature which uses iris textural features, Add/Minus operation is defined. This ROI is sufficient to differentiate between different images. The Gabor Filter is also used for calculation. Due to noise the mean of similar images is different. Then the normalized iris feature vector is calculated from the filtered image and by using Add/Subtract operation encryption and decryption operation is perform [1].

Atul Kahate, Cryptography and Network Security[3] Have proposed cryptography concept easily.

Next then feature extraction is done on the basis of high rank among all the properties from the matrix. From the feature extracted the key is generated and that key is used for encryption and decryption is performed [2].

III. PROPOSED METHODOLOGY

In this paper we concentrate on the key part of the

cryptography. In this paper user is provided with an interface in which user is free to designed any type of pattern, shape, signature etc. which can be easily remembered by the user. The designed pattern is of size 1260*800. The designed

pattern constitutes of pixels and each pixel has some color which is represented by binary value. We can create any type of free design for security according to its creativity.

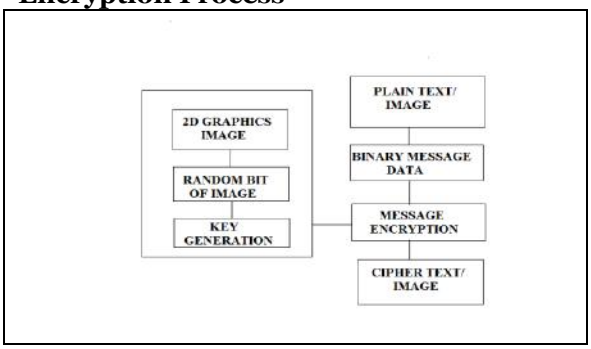
The proposed algorithmis given below.

Proposed Algorithm

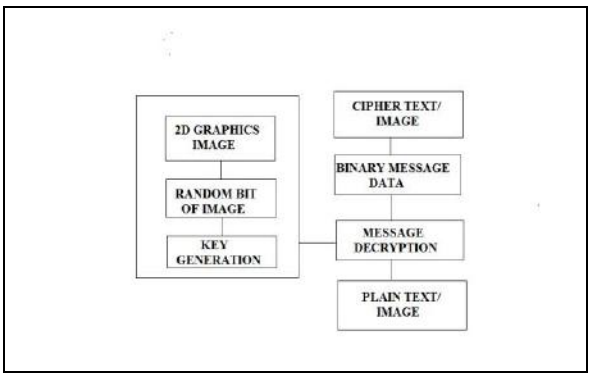
1. Read the user created Graphical image.
2. Read the pixels and shuffle among them there position (i.e. exchange the 1st pixel value with the last position pixel value, 2nd pixel value with the second last position pixel value and soon until we reached to the centre pixel value).
3. Create a group of pixels (i.e. 64 bits).
4. Shuffle the groups among their position (i.e. Exchange the 1st position group with the last position group, 2nd position group with the second last position group and soon until we reached to the center position).
5. Initiate i=1
6. Declare array to store key in array Result[16].
7. Declare two variables var1 and var2.
8. Store the 1st group value in var1 and 2nd group value in var2.
9. While i < size of array

a. Perform the XOR operation between var1 and var2.
b. Store the result of XOR operation in ith block of array.
c. Store the value of result obtained in var1 and next group value into var2.
d. Increment the value of variable i and go to step 9.
10. Results obtained from Step9 are applied in each phase of AES algorithm as independent sub-keys.

Encryption Process



Decryption Process



IV. CONCLUSION

This Paper proposed a modified approach of generating key using 2D Graphics. It states that the user is free to design the any type of key pattern according to the creativity. In the proposed algorithm a different key is generated for each stage of AES. The same image can be used for different text encryption. By using RGB or Gray Scale image we Design a key. In colorful 2D graphics pattern eachpixel will contain the RGB value. Form this color image we can generate the key.

V. REFERENCES

1. *Xiukrun Li, Xiangqian Wu, Ning Qi Kuanquan Wang, A novel Cryptographic Algorithm based on Iris Feature,2008*
2. *B. Santhi, K.S. Ravichandran, A.P. Arun and L. Chakkarapani, A Novel Cryptographic Key Generation Method Using Image Features, 2012.*
3. *Atul Kahate, Cryptography and Network Security, 2nd edition,Tata Mcgraw Hill Education Private Limited, 2011*
4. *Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay, and Sugata Sanyal, L. L. 1993. Steganography and Steganalysis: Different Approaches.*
5. *Roszizti Ibrahim Suk Kaun Steganography Algorithm to Hide Secret Message inside an Image[J]. Technology and Application of Compute,2011.*
6. *Der-Cyuna Lou, Chen-Hao Hu, LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis[J], Information Sciences,2012.*
7. *Yifeng Sun, Fenlin Liu,Selecting cover for image steganography by correlation coefficient [C], 2010 Second International Workshop on Education Technology and Computer Science.*
8. *Marwaha,P. Visual cryptographic steganography in images[C], Computer Communication and Networking Technologies(ICCCNT),2010 International Conference.*
9. *C.Cachin, "an information-theoretic model steganography," in IH98, LNCS 1525,Heidelberg: Springer-Verlag, 1998.*