IJMTST

Volume: 2 | Issue: 05 | May 2016 | ISSN: 2455-3778

A Cryptographic Key Generation Using 2D Graphics pixel Shuffling

Londhe Swapnali[1] | Jagtap Megha[2] | Shinde Ranjeet[3] | Belsare[4]

[1]Department of Computer Engineering, S.B Patil College, Indapur, India
[2]Department of Computer Engineering, S.B Patil College, Indapur, India
[3]Department of Computer Engineering, S.B Patil College, Indapur, India
[4]Department of Computer Engineering, S.B Patil College, Indapur, India

ABSTRACT

*Now a day with incredible change in social media network like mobile communication and computer, all type of a data such as audio, video, images are used for the communication .Privacy for that data is an important issue .Cryptography is one of the technique used for stopping unauthorized access and increasing integrity of that data. In research area encryption and decryption scheme is used based on image pixel shuffling and transposition. For security purpose we can use cipher algorithm for generating key using RGB values of the pixel instead of using only pixel values. For that purpose in our proposed system we are using m*n size image on which different operations can be performed. Our proposed system is more secure as compare to existing system.*

KEYWORDS: *Cryptography, Encryption, Decryption, Cipher text, Pixel, 2D graphics image, Integrity, key Network.*

Copyright © 2015 International Journal for Modern Trends in Science and Technology
All rights reserved.

I. Introduction

We cannot think about the world without communication .Now a day's hiding of data from unauthorized person is an important task .There are many online services present in which communication takes place through social media network. In that case there is high probability of hacking [1].Integrity of a data is not maintained well.

Different techniques are used to maintain a security in all social networks communication. The techniques such as cryptography and stenography. Cryptography is the best technique to increase the security between communications. It's applied on a different type of data such as text, image, video etc. In cryptography two different processes are there, first is encryption in which specific key is used to encrypt the data. It is a process of converting plain text in to cipher text and second is decryption in which cipher text is converting into plain text. Two things are important for performing encryption and decryption, first is algorithm and second is key. Plain text is combined with the algorithm to form a key. This generated key is then used for the encryption process .This cipher text is applied to the algorithm for generating the plain text. Symmetric and asymmetric are the two approaches of encryption .In symmetric same cryptographic key is used for encryption and decryption but in decryption different key's are used for processing. In this approach keys are identical or combination of different keys.

Image is made up of different color pixels. Every pixel having different colors at a single point, so pixel is a single color dot. Digital approximation can be resulted from that color dot using this values reconstruction of that image take place. Digital image having two types first is color image made up of color pixels. Color pixel holds primary colors such as red, blue and green. This values proportion used for creating secondary colors. If each primary contain the 256 levels then four byte memory required for each. Bi-level image having single bit to represent each pixel. It's having only two states with color black and white [2].

In this paper we focused on key part. In image based cryptographic technique, cipher algorithm of m*n size image used for fetching RGB pixel values. Encryption and decryption of an m*n size image is based on the RGB pixel values. Property of 2D graphics image is only viewing and listing image dimensions is sometimes impossible for generating the image.

Rest of the paper is organized as, 2nd section is related to related work. 3rd section gives information related to proposed system, 4th section represent the advantages, 5th section proposes experimental work with some mathematical part.6th section provides the overall summary of our paper with conclusion of the paper.

II. Proposed System

In previous existing system key generation is take place using the pixel values of the 2D graphics image. In which proposed algorithm used for extracting the pixel values as well as creating the key from pixel [1]. For increasing the security of image during the communication and transmission we propose new techniques. In last module we use RSA algorithm for encryption and same key is used for decryption process of 2D graphics image [2].

In this paper user having freedom to generate any type of pattern signature etc. having fixed size of design pattern .Any image is made up of using different colors pixels. Each pixel having three components ass RGB . This RGB values first of all extracted and after shuffling we get cipher image. It's done only by using a RGB values[2].

In this method we not use the bit values of pixel as well as pixel expansion at the end of the encryption and decryption process. Pixel having numeric values which interchanged or the RGB values displaced from their original position to create a cipher text. When we add all values in between image no change take place in original size and shape in image. All the features of an image remain unchanged during the process of encryption and decryption [2].

Figure.1 describes the architecture of encryption and decryption. We provides user interface for designing the pattern .According to cipher algorithm we fetch the all RGB values and manipulation take place using reshuffling ,transposition techniques for generating key. Image decomposed into three components which act upon the cipher algorithm. That components form the all features and characteristics of original image. Within image boundaries all the RGB values are shuffled and interchanged, created array is different for all components.

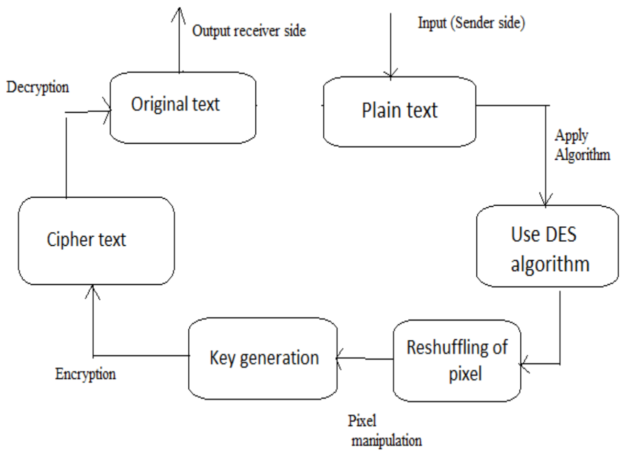


Figure 1:- Encryption and decryption of image

III. Flow of Project

Figure.2 describes the flow of encryption and decryption process. In which first of all we accept the image, fetch all the RGB components using cipher algorithm and convert plain text in to cipher text. We use RSA algorithm for the encryption process. In which key is combined with cipher text for performing encryption process. Decryption process take place by importing all data and using reveres process of encryption. This process is done for generating original image with its shape and size.

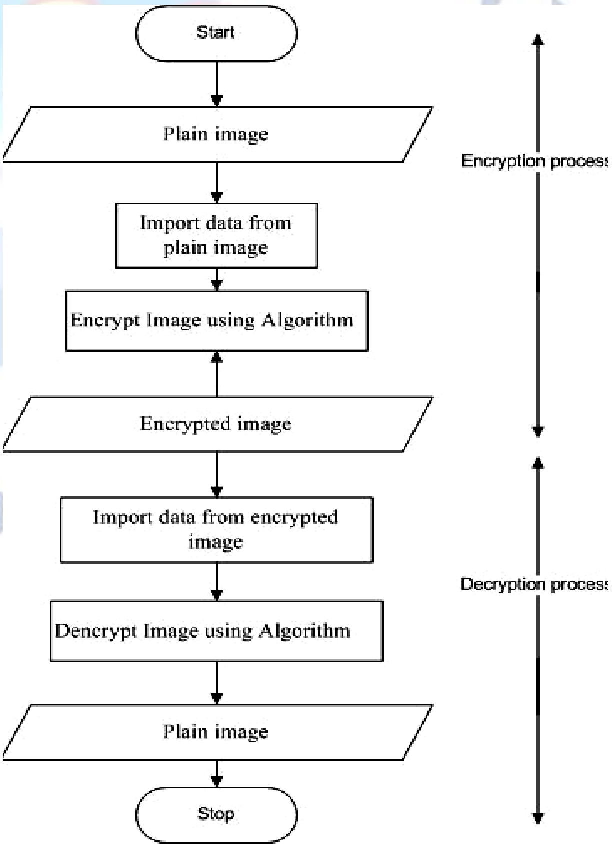

Start
Plain image
Import data from plain image
Encrypt Image using Algorithm
Encrypted image
Import data from encrypted image
Dencrypt Image using Algorithm
Plain image
Stop
Encryption process
Decryption process

Figure 2: The flow chart diagram for the encryption and decryption process.

IV. 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.

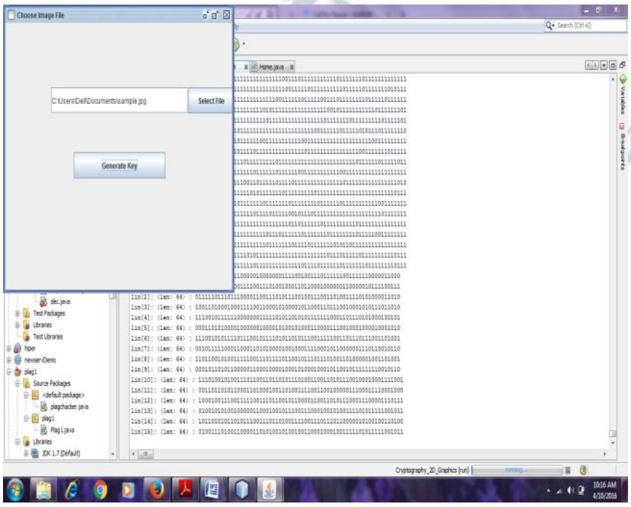
c. Store the value of result obtained in var1 and next group value into var2.

d. Increment the value of variable i and go to step

10. Results obtained from Step9 are applied in each phase of DES algorithm as independent sub-keys.

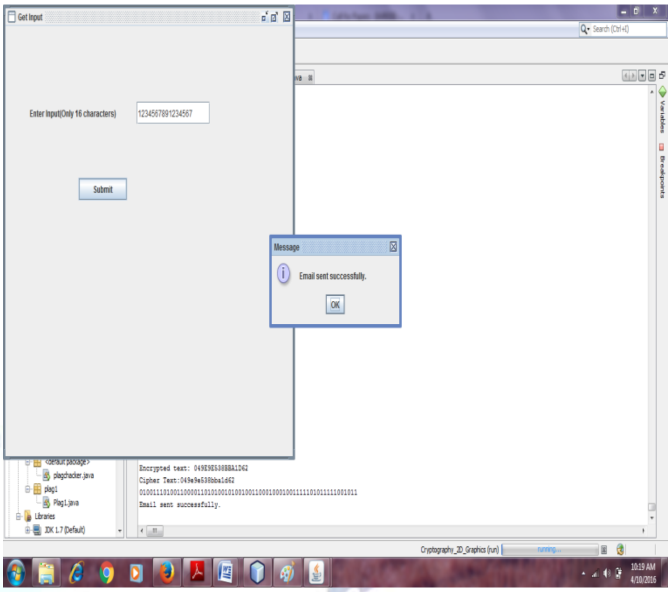
V. Results and Discussion

In the fig 3, it shows the key generation using given input image. Input we can fetch from anywhere after that using DES algorithm we generate a key.


Choose Image File
C:\Users\Dell\Documents\sample.jpg
Select File
Generate Key
Home.java
Cryptography_2D_Graphics (run)

```
lin[2]: (len: 64) : 0111110111011100001100111010111001001110011010011110101000011010
lin[3]: (len: 64) : 1001101000100011110011000101000010110001101110010001010111011010
lin[4]: (len: 64) : 1110010111111000000011111010110101011111110001101110101000100101
lin[5]: (len: 64) : 0001101010000100000010000101001010001100001110010001000010001010
lin[6]: (len: 64) : 1110010101111011100101111010110101110011111001101110111001101001
lin[7]: (len: 64) : 0010111110001100011010100001001000111100010110000001110110010110
lin[8]: (len: 64) : 1101100101001111100111011110110010111011101001101000001001101001
lin[9]: (len: 64) : 0001011010110000011000100001000101000100010110010111111110010110
lin[10]: (len: 64) : 1110100101001110110011011010111010011001101011100100010001111001
lin[11]: (len: 64) : 0011011010110001101000100110100111100110010000011100011110001000
lin[12]: (len: 64) : 1000100111001111100111011001011000011001101011100011100001110111
lin[13]: (len: 64) : 0100101010010000011000100101110011100010010100111101011111001011
lin[14]: (len: 64) : 1011010101101011100111011010011110011101110110000010100100110100
lin[15]: (len: 64) : 0100111010011000011010100101001001100010001001111010111111001011
```

Fig. 3 Key generation Process



Enter Input(Only 16 characters) 1234567891234567

Email sent successfully.

```
Encrypted text: 049E9E538BBA1D62
Cipher Text:049e9e538bba1d62
0100111010011000011010100101001001100010001001111010111111001011
Email sent successfully.
```

Fig. 4 Encrypted text insertion and mail sending

In the fig 4, which text we have to encrypt its inserted .In initial stage we insert only 16 characters for encryption purpose. After that cipher text and generated key sended on receiver mail for decryption purpose for getting original text.

VI. Conclusion

In this paper we have proposed cryptographic key generation on a 2D graphics using RGB pixel shuffling & transposition. For our proposed system we use any size of image as an input. Small change in image creates a number of keys. In proposed system at each stage cipher algorithm generates different keys using the RGB pixel values on which different operations are performed. Existing system uses pixel values only but our proposed system extracts RGB pixel values of given image. This will be helpful for increasing security of given 2D graphics image. In future we can combines different RGB values of pixel with each other and generate a new pattern for key.

References

[1] Pratik Shrivastava, Reteshjain, K.S. RaghuWanshi, A modified. Approach of key manipulation in cryptography using 2D graphics Image, Published in Proceeding ICESC '14 Proceedings of the 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies Pages 194-197, IEEE Computer Society Washington, DC, USA ©2014.

[2] Xiukum Li, Xianggian Wu*, Ning Qi, KuanquanWang. A novel cryptographic Algorithm based on iris feature, 2008.

[3] ShujiangXu, YinglongWang, YucuiGuo, Cong Wang, "A Novel Image Encryption Scheme based on a Nonlinear Chaotic Map", IJIGSP, vol.2, no.1, pp.61-68, 2010.

[4] Krishnan, G.S.; Loganathan, D.; , "Color image cryptography scheme based on visual cryptography," Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on , vol., no., pp.404-407, 21-22 July 2011.

[5] Christy, J.I.; Seenivasagam, V. , "Construction of color Extended Visual Cryptographic scheme using Back Propagation Network for color images," Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on , vol., no., pp.1101-1108, 21-22 March 2011.

[6] B. Santhi, K.S. Ravichandran, A.P. Arun and L. Chakkarapani Novel Cryptographic Key Generation Method Using Image Features, 2012.

[7] Kester, Quist-Aphetsi; , "A public-key exchange cryptographic technique using matrix," Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on , vol., no., pp.78-81, 25-27 Oct. 2012.

[8] RuisongYe, WeiZhou,"A Chaos-based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice", IJCNIS, vol.4, no.1, pp.38-44, 2012.

[9] Asia mahdiNaserAlzubaid, Cotor Image Encryption & decryption using pixel shuffling with Henon chaotic syste, 2014.

[10] AmneshGoel, NidhiChandra,"A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group Wise Of RGB Values and Explosive Inter-Pixel Displacement", IJIGSP, vol.4, no.2, pp.16-22, 2012.

[11] Panchami V, Varghes Amithab Wahi, A New Color ORIENTED Cryptographic Algorithm Based on Unicode And RGB Color Model, 2014.

International Journal for Modern Trends in Science and Technology IJMTST