IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 6, Ver. IV (Nov – Dec. 2015), PP 08-11
www.iosrjournals.org

A Cryptographic Key Generation on a 2D Graphics using RGB pixel Shuffling and Transposition

[1]Swapnali Krushnarao Londhe., [2]Megha Dilip Jagtap.,
[3]Ranjeet Ravindra Shinde., [4]P.P. Belsare
[1]Student of Dept. of Computer Engg., Engg., S.B.P.C.O.E.Indapur,SPPU Pune, India.
[2]Student of Dept. of Computer S.B.P.C.O.E.Indapur, Pune, India.
[3]Asst.Prof. of Dept.of Computer S.B.P.C.O.E.Indapur, Pune, India.

Abstract: *Now a day with incredible change in social media network such as 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 this research encryption and decryption scheme is used based on image pixel shuffling and transposition. We can use cipher algorithm for generating key using RGB values of the pixel. For that purpose we use m*n size image on which different operations are performed. This algorithm was implemented in java language.*

Keywords: *Cryptography, Encryption, Decryption, Cipher text, Pixel, 2D graphics image, Integrity, key*

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 is many online services present in which communication take 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. These 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[1]. 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 pixel s its nothing but the array of pixel having rectangular shape. 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.

Paper having following structure, II section is related to related work. III section gives information related to proposed system, IV section represent the advantages, V section proposes experimental work with some mathematical part.VI provides the overall summary of our paper its concludes the paper.

II. Related work

Xiukun Li, Xianggian Wu*, Ning Qi, Kuanguan Wang has proposed a Novel Cryptographic algorithm containing Iris features nothing but the iris textural features. Its algorithm having Add/minus operational and read -Solomon error correcting. He defines the Region of Interest which used to differentiate different images [3]. Using another technique for a novel cryptographic some extension is given by a shujiang Xu.yinglong

Wang, Yucui Geo &Cong Wang. He uses a nonlinear chaotic map and means of XOR operations to encrypt a novel image. In which two rounds are proposed for encryptions [4].

Krishan ,G.S and Loganathan proposed a new scheme based on a visual cryptography in which binary images is used as the key input .The secret communicated images than decomposed into three monochromatic images based on YCbCr color space & this monochromatic images converted into binary images were encrypted using key called share -1[5].This technique is extended by christy and seenivasgam. He uses Back Propagation Network (BPN) to produce the two shares. Using this technique images has been produced having same features like original [6].

B. santhi, K.S.Ravichandran, A.P. Arun & L. Chakkarapani explains using images Features. Its uses Gray Level co-occurrence matrix of an image to extract the properties of an image [7] . Kester, QA proposed a cryptographic algorithm, which is based on a matrix and shared secrete key. He extends his research and use RGB Pixel to encrypt & decrypt the images [8].

Ruisong Ye and Wei Zhou proposed a chaos based scheme for image encryption .In which chaotic orbits is constructed by using a 3d skew tent map with three control parameters. This generation is used to scramble the pixel positions .This approach having same good qualities such as sensitivity to initial control parameters pseudo-randomness [9]. Extension to this approach for increasing the security purpose, Asia Mahdi Naser alzubaidi propose a encryption technique using pixel shuffling with Henon chaotic. He divides scrambled image into sixty four blocks rotate each one in clockwise direction with go angle. For making distortion, two dimension Arnold Cat Mapping is applied and original position of pixel is reordered back to its original position [10].

Amnesh Goel and Nidhi proposed a contrastive method. This method uses RGB values of pixels for rearranging the pixel within image than encryption take place [11].

Panchami V , Varghese Paul , Amithab Wahi proposed a techniques in which massage encoded using Unicode and encrypted using the RGB color .Hexadecimal values present for cipher color its distributes into two equal parts and 1^{st} parts act as a message and 2^{nd} is a key[12].

III. Proposed work

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.

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].

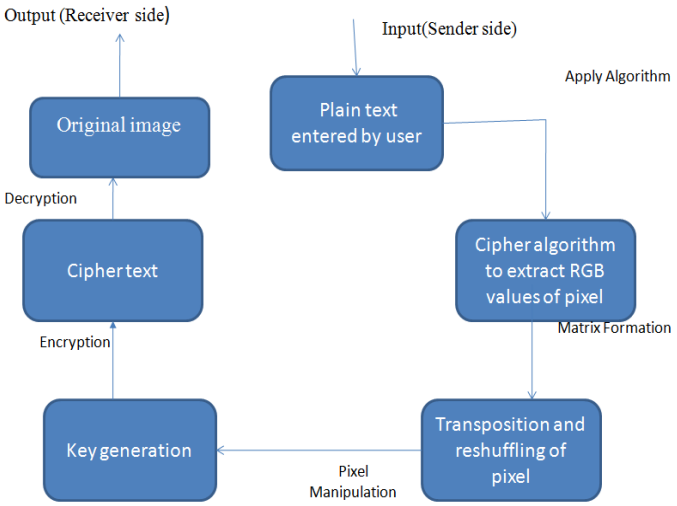

Figure 1:- Encryption and decryption of image

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.

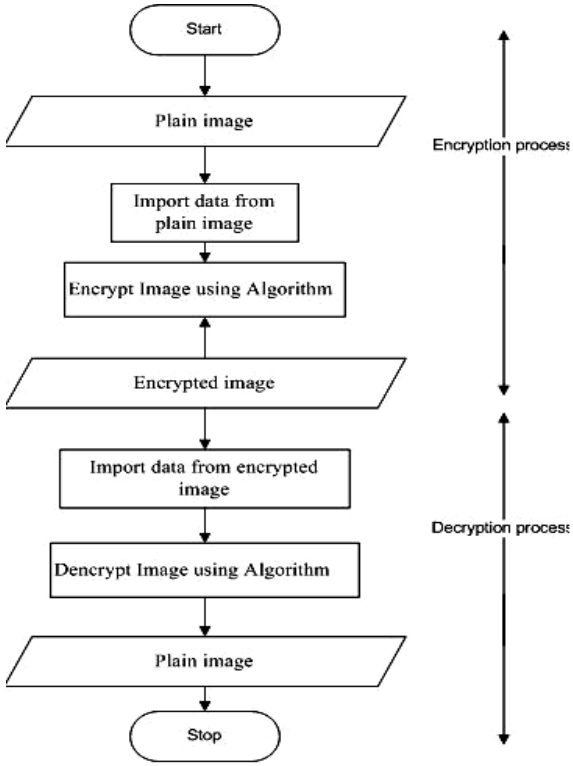

Figure 2: The flow chart diagram for the encryption and decryption process.

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.

IV. Advantages

In terms of security analysis transposition and reshuffling of the RGB values of 2D graphics is really effective. Security of image against all the attacks is increased due to extra swapping of component. Using RGB values we extract all the exact features of the image and it's quite easy to generate exact shape and size of the original image.

V. Experimental work

We can extract all pixel values only when image is given as an input. We can apply cipher algorithm having following steps.

Step -2. Start
Step -2. Import data and form image by interpreting each element.
Step -3. Extract all r, g, b component from image.
Step -4. Reshape all r, g, b component in to one dimensional array for each.
Step -5. Let, t= [y; 1; p] which is a column matrix.
Step -6. Transpose 't' .
Step -7. Reshape 't' into one dimensional array.
Step -8. Let, n= Total number of array.
Step -9. Let, r= (1^{st} part of n): ($1/3^{rd}$ part of n) as one dimensional array.
Step -10. Let, b= ($1/3^{rd}$ part of n): ($2/3^{rd}$ part of n) as one dimensional array.
Step -11. Let, g= ($2/3^{rd}$ part of n): (nth) as one dimensional array.
Step -12. Transform its with its original dimensions.
Step -13. Finally all data will convert into an image.

For decrypt the image from cipher text to plain text inverse of algorithm is used.

VI. Conclusion

This paper proposed a cryptographic key generation on a 2D graphics using RGB pixel shuffling & transposition. In this paper any size images using as an input. Small change in image creates a number of keys. In proposed cipher algorithm in each stage different keys are generated using the RGB pixel values on which different operations are performed.

In future we can combines different RGB values of pixel in each other and generate a new pattern for key generation.

References

[1]. Pratik Shrivastava, Retesh jain, K.S.Raghu Wanshi, A modified. Approach of key manipulation in cryptography using 2D graphics Image,2014.
[2]. Quist Aphetsi Kester,MIEEE, Image Encryption based on the RGB PIXEL Transposition and Shuffling,2013.
[3]. Xiukum Li, Xianggian Wu* , Ning Qi, Kuanquan Wang.Anovel cryptographic Algorithm based on iris feature ,2008.
[4]. Shujiang Xu,Yinglong Wang,Yucui Guo,Cong Wang, "A Novel Image Encryption Scheme based on a Nonlinear Chaotic Map", IJIGSP, vol.2, no.1, pp.61-68, 2010.
[5]. 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
[6]. 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.
[7]. B. Santhi, K.S. Ravichandran, A.P. Arun and L. Chakkarapani Novel Cryptographic Key Generation Method Using Image Features,2012.
[8]. 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
[9]. Ruisong Ye,Wei Zhou,"A Chaos-based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice", IJCNIS, vol.4, no.1, pp.38-44, 2012
[10]. Asia mahdi Naser Alzubaid,. Color Image Encryption & decryption using pixel shuffling with Henon chaotic syste,2014.
[11]. Amnesh Goel,Nidhi Chandra,"A Technique for Image Encryption with
[12]. 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.
[13]. Panchami V, Varghes Amithab Wahi, A New Color ORIENTED Cryptographic Algorithm Based on Unicode And RGB Color Model,2014