Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 10, October 2013, pg.203 – 207

REVIEW ARTICLE

A Review on Keyless User Defined Reversible Encryption for Color Image

Pratibha S. Ghode
IIIrd SEM, M.Tech – CSE, Abha Gaikwad-Patil College of Engineering, Nagpur, India
pratibha201986@gmail.com

Prof. Pragati Patil
Assistant Professor, Abha Gaikwad-Patil College of Engineering, Nagpur, India
pragatimit@gmail.com

Abstract– Some limitation of Key oriented techniques, to maintain the key records and increase high computational cost. To overcome this limitation to proposed an improved reversible image encryption random hiding approach for keyless image encryption. The objective of this paper to increase the secrecy and confidentiality of images is a multimedia and vibrant area of research. There are two different approaches being followed in image encryption, the first approach to key oriented encryption and second approach to keyless to random encryption technique for every pixel and to maintain the originality of an image without any loss of quality.

Keywords– Random hiding; Reversible Encryption

I. INTRODUCTION

In computer and communication systems security issues play a crucial role and must be addressed before hand to guard against illicit attacks As security of data on any kind of system has became the first priority for the organization, the methods which are used to ensure security not only need to be strong and efficient, but should also be easy to execute and implemented. With progress in technology, encryption came up with a big boom, taken as a weapon of ultimate security. It is an earliest art and it is defined as the science of writing in secret code.

The advent of internet introduced to its users a whole new dimension as to how data can be shared from one part of the world to the other in near real time. However along with these opportunities came the challenges, such as, how to maintain the confidentiality of the data being transmitted. This gave a fillip to the already vibrant research area of cryptography.

II. RELATED WORK

A mathematical procedure is used for performing encryption of an image. Through the use of an algorithm, information is made into meaningless cipher text and requires the use of a key to transform the data back into its original form. Blowfish, AES , DES, RSA, RC4, RC5, and RC6 are examples of encryption algorithms. An encryption algorithm along with a key is used in the encryption and decryption of image which forms the basis of network security.

Encryption of images is basically classified into three categories based on the nature of recovered image encryption.

- Key oriented Encryption
- Image Splitting
- Multiple Shares

(A)Key oriented Encryption:

This approach is basically similar to the conventional encryption [9] methods which involved using a key algorithm [7] to encrypt and decrypt an image. Some of the proposed techniques for encrypting images use "Digital Signatures[2]", "Multimedia", "Military", Vector Quantization" etc. There are some limitations with these techniques; they involve use of secret keys and maintained the key.

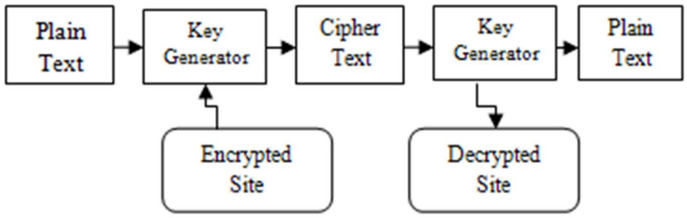

Fig: 1 Key Oriented Encrypted/Decrypted

In addition, in some cases the available are limited key space in image encryption. Also high computation cost involved in image encryption. That is also weak security functions of image key oriented management.

(B)Image splitting:

In this technique image splitting is performed in which an image at pixel level is divided into two or more shares. Saeed Alharthi and Pradeep K. Atrey [2] in 1979 are credited for introducing the idea of dividing a secret data into 2 random shares. The individual shares do not convey any information about the image, but a proper arrangement of these shares will help regenerate the original image.

This technique does not require any key management and also no computation in description but the main limitation of this approach pattern will be identified.

(C)Multiple shares:

In multiple shares technique to splitting an image into multiple shares proposed in 2011 Siddharth Malik, Anjali Sardana [1]. The shares so generated reveal no information about the original secret image and to retrieve the secret image all the shares are required. In this approach used SDS algorithm. SDS means Sieving, Division, and Shuffling.

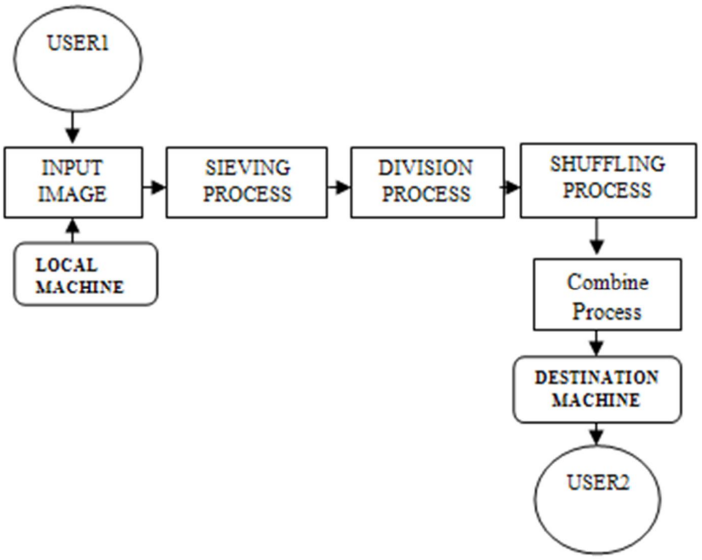

Fig: 2 SDS Algorithm

In the first step sieving technique generates the secret image is split into RGB colors. In the second steps Division technique generates the split images are randomly divided. In the three steps shuffling technique shuffled each shares and finally combined all shares. In above limitation of process to easily identify sequences counter.

III. PROBLEM DEFINITION

Existing system the design of an encryption algorithm must provide security against unauthorized attacks. Key-oriented algorithms are very efficient but they were very bulky to manage as key handling must be done. To improved quality of existing system, keyless random hiding techniques can be used. Techniques of keyless encryption of images allow secure transmission of image. Random hiding is a technique that embeds the important images into a cover image such that the important images are imperceptible and can be securely transmitted to the receiver.

This system is used to shuffle the position of the image pixels, [9] and then use reversible encryption technique to confuse the relationship between the original image and the cipher image.There is no key involved in the encryption process. Only Random hiding techniques are used. The main purpose of this research is to improve and avoid the attackers by using the Reversible Encryption.

	RED	GREEN	BLUE
BLACK	0	0	0
RED	1	0	0
GREEN	0	1	0
BLUE	0	0	1
YELLOW	1	1	0
CYAN	0	1	1
MAGENTA	1	0	1
WHITE	1	1	1

Table: 1 RGB Color 2^3Combination

The additive and subtractive color models are mainly used to represent the colors. In the additive (RGB) color model, [1] three primary colors at is Red, Green, Blue are mixed to get 8 different colors. The example of additive model is color monitor of computer. The subtractive (CMY) color model the colors are represented by the degree of the light reflected by the colored objects. In this model Cyan (C) Magenta (M) and Yellow (Y) color are used to produce the desired range of colors. The example of subtractive model is color printers.

IV. PROJECT OBJECTIVES

The main objective of this proposed work is to implement every combination of RGB color image for each pixel as encryption and decryption time. The objectives are:-
_ to make data more securable.
_ to encrypt or decrypt RGB color image data.

This paper will describe a new approach to implement the different combination of RGB using each and every pixel of image and encrypted them. In this proposed work provide the without loss of pixel of any image provided original image quality.

V. INVESTIGATIONAL OUTCOME

For image processing we need to identify the R,G,B of every pixel so using mouse move event and get pixel function we can extract pixel R.G.B. After processing every pixel we separate the pixel R, G, B in different picture box hence we get different shade images. While processing we also get the image properties. Then we apply random hiding techniques for each R, G, and B pixels. In reversible encryption, if we add x number which is dependent on Width and Height (W x H) of image to a pixel, then we subtract the x number from the pixel at the receiver site.

VI. CONCLUSION

This survey paper presents approach of A Keyless approach to color image Encryption is based on the concept of Random encryption. The algorithm does not use the traditional approach of using an encryption key; but defines a different combination of colors of each pixel of images and reversible image hidden technique for sender site and receiver site to maintain the originality of an image without any loss. Keyless approach to lossless image encryption is a new multimedia topic.

VII. REFERENCES

1. "A Keyless approach to image encryption" Siddharth Malik, Anjali Sardana(2011).
2. An improved scheme for secret image sharing Adi Shamir in 1979.
3. A Hyper-chaos Based Image Encryption Algorithm Chen zaiping, Li haifen, Dong enzeng, Du yang in 2010
4. AlokaSinha and Kehar Singh, "A technique for image encryption using digital signature", Optics communications(2003).
5. S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001), pp 1229-1245.
6. X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
7. Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software 58 (2001), pp. 83-91.

8. Mohammad Reza Keyvanpour, Famoosh Merrikh-Bayat in 2010 “A New Encryption Method For Secure Embedding”
9. Nidhi Sethi and Deepika Sharma in 2012 “A New Cryptology Approach for Image Encryption”
10. Analysis on an Image Encryption Algorithm Shubo Liu1,2, Jing Sun1, Zhengquan Xu2, Jin Liu2 2008
11. M. Lakshmi, S. Kavitha, keyless user defined optimal security encryptionISSN:2319-7242 Volume 2 Issue 6 June, 2013 Page No. 1788-1793
12. Du-Shiau Tsai , GwoboaHorng , Tzung-Her Chen , Yao-Te Huang , “A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint”, Information Sciences 179 3247–3254 Elsevier, 2009.
13. Xin Zhang and Weibin Chen, “A new chaotic algorithm for image encryption”, International Conference on Audio, Language and Image Processing, 2008. (ICALIP 2008), pp 889-892.

