A SECURE KEYLESS COLORED IMAGE ENCRYPTION

Mr. Amit B. Chougule[1], Ms. Nilam Nisar Shaikh[2]

[1]*Computer Science and Engineering Department, B.V. College of Engineering, Kolhapur/Shivaji University, (India)*

[2] *Computer Engineering Department, S.S.P.M. College of Engineering, Kankavli/Mumbai University, (India)*

ABSTRACT

Image encryption basically can be done with two different approaches, the first being encrypting the images through encryption algorithms using keys, and the second approach divides the image into random shares to maintain the images secrecy. The limitation of first approach is heavy computation cost and key management issues. Similarly the poor qualities of the recovered image from the random shares limit the applications of the second approach. A different approach to image encryption is encrypting the images without the use of secret keys. This paper expresses the way of secure colored image encryption without use of encryption key. It can be analyzed that with this new approach being implemented, random shares can be generated with minimal computation, with no pixel expansion and the original secret image can be recovered from the random shares without any loss of image quality. This method is robust to withstand brute force attacks.

Keywords: Image Encryption, Image Decryption, Random Shares, Sieving, Shuffling, Combining.

I. INTRODUCTION

In recent days, security is a big threat in the transmission medium due to the development of the Internet and multimedia contents such as audio, image, video, etc. It enables us to easily purchase digital contents via the net. However, it causes several problems, such as violation of ownership and illegal distribution of the copy. The basic idea followed is based on cryptography technique. Encryption is the first process in which the plain text or readable text is converted into cipher text or unreadable text. The second process is called decryption process in which the cipher text or unreadable text is converted to plain text or readable text. To encrypt data, an encryption algorithm is used at the sender, to reveal the data at the receiving end a decryption algorithm is used. Here secure colored image encryption technique is used, which does not uses keys for both encryption and decryption.

This paper concentrates more on the image secrecy without keys. Encryption of images is broadly classified into lossless and lossy encryption [7]. There are studies on image encryption using the keys with digital signatures [1], chaos theory [2] and vector quantization. These techniques have some drawbacks that they are limited with the key size and high computation and also weak security. To overcome all these limitations the concept of keyless colored image encryption is developed which involves secret sharing of image by dividing it into multiple shares. A hacker cannot perceive any clues about a secret image from individual random share images.

II. EXISTING WORK

The approach of an image encryption using keys is similar to the conventional encryption methods such as RSA, DES which involve use of an algorithm and a key to encrypt an image. Some of the proposed techniques for encrypting images use Digital Signatures, Chaos Theory, and Vector Quantization etc.

C.C. Thien, J.C. Lin use two transparent images [15]. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information.

A technique for image encryption using digital signature by Aloka Sinha and Lehar Singh [16] suggest that the digital signature of the original image is added to the encoded version of the original image. The encoding of the image is done using an appropriate error control code. At the receiver end, after the decryption of the image, the digital signature can be used to verify the authenticity of the image.

There are several parameters in the chaos system [17], and it is sensible to the original value and unpredictable. The results of several experimental, statistical analysis and key sensitivity tests show that the this image encryption scheme based on Henon chaotic maps provides an efficient and secure way for image encryption.

Hence a novel approach without the use of encryption keys for the colored image encryption is proposed. The approach employs Sieving, Division and Shuffling to generate random shares such that with minimal computation, the original secret image can be recovered from the random shares without any loss of image quality.

III. PROPOSED SCHEME

The main objective of this scheme is to provide conventional colored image encryption without using keys. A secret image is splitted into multiple random images and with minimum computation cost the original secret image can be retrieved back. The original secret image can be retrieved in totality. This approach does Sieving, Division and Shuffling to generate random shares with minimal computation. It employs low storage and less bandwidth requirements.

Proposed technique involves image encryption without using keys by splitting an image into multiple shares. The shares so generated reveal no information about the original secret image and to retrieve the secret image all the shares are required.

The scheme can be implemented with the SDS algorithm and involves three steps.

Step I: the secret image is split into primary colors (Sieving)

Step II: these splitted images are randomly divided (Division)

Step II: these divided shares are then shuffled each within itself (Shuffling)

Finally these shuffled shares are combined to generate the desired random shares.

IV. METHODOLOGY

The proposed scheme can be design and implemented in following manner.

4.1 Sieving

The secret colored image is splited into primary colors. Sieving involves filtering the combined RGB components into individual R, G and B components .The granularity of the sieve depends on the range of values that R/G/B component may take individually.

4.2. Division

After filtering the original image into R, G and B components, divide the R, G and B components into z shares each.

R (RA, RB, RC, … RZ)

G (GA, GB, GC, … GZ)

B (BA, BB, BC, … BZ)

While dividing each element, RA-Z, GA-Z and BA-Z is assigned values randomly.

The shares so generated should be such that (RA, RB, RC, … , RZ) should regenerate R and similarly for G and B components.

4.3 Shuffling

This involves shuffling the elements in the individual shares. The sequence in which the elements within the shares are shuffled depends on the value of one of the other shares generated from the same primary color. In other words RB decides how RA is shuffled, RC decides how RB is shuffled, RZ decides how RZ-1 is shuffled and similarly RA decides how RZ is shuffled.

4.4 Design Details

The proposed scheme design involves generating two random shares. Figure shows steps involved in generating two random shares.

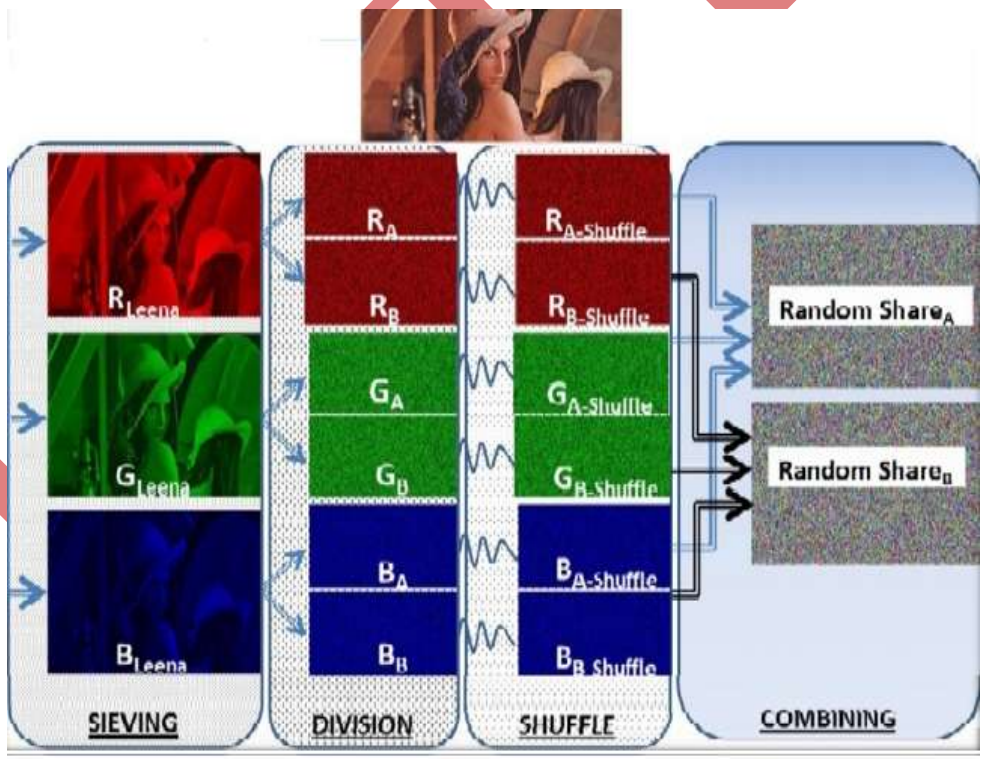

Fig. Steps Involved In Generating Two Random Shares

V. CONCLUSION

This paper is a new enhanced visual cryptographic which is a hybrid of the traditional visual cryptographic scheme and the conventional image encryption schemes. The original secret image can be retrieved in totality. There is no pixel expansion and hence storage requirement per random share is same as original image. Key

management is not an issue since there are no secret keys involved. The scheme is robust to withstand brute force attacks. It is suitable for authentication based application.

REFERENCES

[1] Aloka Sinha and Kehar Singh, "A technique for image encryption using digital signature", *OpticsCommunications (2003), 218(4-6), pp 29-234,online [http://eprint.iitd.ac.in/dspace/handle/2074/1161]*

[2] 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.*

[3] Malik, S. ;Sardana, A. ; Jaya, J."A Keyless Approach to Image Encryption*", Communication Systems and Network Technologies (CSNT), 2012*

[4] Sudharsanan, S."Shared key encryption of JPEG color images", *Consumer Electronics, IEEE Transactions on Volume: 51 , Issue: 4 Digital ObjectIdentifier:10.1109/TCE.2005.1561845 Publication Year: 2005 , Page(s): 1204 – 1211.*

[5] Arpad Incze, "Pixel sieve method for secret sharing & visual cryptography" *RoEduNet IEEE International Conference Proceeding Sibiu 24-26 June 2010, ISSN 2068-1038, p. 89-96*

[6] R. Lukac, K.N. Plataniotis "Bit-level based secret sharing for image encryption", *The Journal of Pattern Recognition Society, 2005.*

[7] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", *Pattern Recognition 34 (2001), pp 1229-1245.*

[8] 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.*

[9] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin ,"Sharing A Secret Two-Tone Image In Two Gray-Level Images*", Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005.*

[10] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multiple-Image Encryption By Rotating Random Grids*", Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256 , 2008.*

[11] F. Liu1, C.K. Wu X.J. Lin , "Colour Visual Cryptography Schemes", *IET Information Security, vol.2, No. 4, pp 151-165, 2008.*

[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] C.C.Chang, T.-X. Yu,Sharing a secret gray image in multiple images, *Proceedings of First International Symposium on Cyber Worlds, 2002, pp. 230–240.*

[14] C.C. Thien, J.C. Lin, "Secret image sharing", *Computers & Graphics, Vol. 26, No. 5, 2002, pp. 765-770.*

[15] M. Naor and A. Shamir, Visual cryptography, *in Proc. EUROCRYPT 94, Berlin,Germany, 1995, vol. 950, pp. 112, Springer-Verlag, LNCS.*

[16] Aloka Sinha and Kehar Singh, A technique for image encryption using digital signature, *Optics Communications(2003), 218(4-6), pp 229-234, online [http://eprint.iitd.ac.in/dspace/handle/2074/1161]*

[17] S.S.Maniccam, N.G. Bourbakis, Lossless image compression and encryption using SCAN, *Pattern Recognition 34 (2001), pp 1229-1245.*

[18] *Siddharth Malik, Anjali Sardana Department of Electronics and Computer Engi-neering Indian Institute of Technology Roorkee, India 2012.*