International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 4, April - 2013

"SDS Technique For Secret Image Encryption"

Venkatesh M.R.
M.Tech Student, VTU
Computer Networking, EWIT
Bangalore.

Roopanjali. Daddi.
Assistant Professor,
Department Of ISE, EWIT
Bangalore.

Abstract - In this paper we study the approach of image encryption using the concept of image SDS that is sieving, dividing and shuffling. There are two approaches for encrypting images; first one by using algorithm and keys and, second approach is dividing the image into shares for secrecy. Since the first approach suffered from some disadvantages such as limited key size and high cost of building the secure algorithms, we are adopting the second approach for securing the image. This paper describes SDS technique for image encryption.

***Key terms*– SDS, Encryption, secure algorithms.**

I. Introduction

Now a days the transmission of data through computer networks is increasing rapidly. So the security of the transmitted data becomes mandatory. Cryptography is the desired technique to provide security of the transmitted data. There are two processes in cryptography. 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, we apply an encryption algorithm at the sender end and to reveal the data at the receiving end, we apply a decryption algorithm. So in cryptography we have to use an encryption as well as a decryption algorithm. But we need to consider the situation where there is no option to use the decryption algorithm during the decryption process. In VC (Visual cryptography) mainly visual information is encrypted using encryption algorithm but here there is no need of decryption algorithm to revel the visual information. Here the decryption process is done simply by human visual system. During the encryption process we simply add some noise in the original image to hide the original information and during the decryption process we reduce the noise to unhide the original information.

The Encryption mainly concentrates the hiding the data based on some of the algorithms. The algorithms can deal with the concept of public key encryption and private key encryption. These both have different sets of the algorithms and have their own advantages and disadvantages. Although securing the information over the network is necessary because there can be loss of data either by any of the intruder or the hacker. Thus providing security is more compulsory and mandatory over the network. The network here may consider the internet, in which there can be several users accessing the files of information. There can be misuse of the information provided to the particular user. Thus the cryptography plays a major role in the internet also. The cryptography provides the Confidentiality, Integrity and Authentication also. Thus there are numbers of the cryptographic algorithms. In this paper we are concentrating on the image secrecy. Encryption of images are broadly classified into lossless and lossy encryption [1]. There are studies on image encryption using the keys are digital signatures [2], chaos theory [3] and vector quantization [4]. These techniques have some drawbacks that they are limited with the key size and high computation is involved and also weak security is an issue [5]. The concept of VC was developed which involves secret sharing of image by dividing it into multiple shares. The advancements made in this line of research, the quality of the recovered secret images still remains an area of concern due to the poor quality of these recovered images (including loss of contrast and colors). Despite its limitations the greatest strength of these schemes is that firstly, there is no requirement of key management and secondly the decryption involves no computation. VC technology uses the concept of encryption of the images only but the decryption mainly involves the human visual system. Despite its limitations the greatest strength of these schemes is that firstly, there is no requirement of key management and secondly the decryption involves no computation. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images, as the visual cryptography involves the multiple shares or this concept can also deal with splitting of images. In which the splitting takes place at the pixel level into multiple shares (two or more), such that individually the shares convey no information about the image, but the qualified set of

these shares will help to regenerate the original image [1].

Visual Cryptography is based on cryptography where *n* images are encoded in a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all shares are stacked together. This paper presents an improved algorithm based on Chang's and Yu visual cryptography scheme for hiding a colored image into multiple colored cover images. This scheme achieves lossless recovery and reduces the noise in the cover images without adding any computational complexity.

II. Related Work

The related work corresponds to the working of image encryption and splitting of the image for security purposes. There can be the combination of splitting and encryption which results in the hybrid approach, which is applied for the current algorithm [1]. The idea of Image splitting involves the splitting of the secret image into n random shares such that these shares individually reveal no information about the secret image. The random image shares printed on transparencies and stacked up revealing the original image. Image encryption initially was applied to the grey scale images proposed from Xin and Chen in 2008. The last and hybrid approach using some kind of an encryption key the image is split into random shares. Incze et al [6] proposed the concept of sieves for encrypting the images. Sieve is typically a binary key. The original image is placed over the sieve. A pixel from the original image situated above a hole of the sieve goes through and form one share of the image.

III. Proposed Algorithm

The algorithm is mainly divided into three steps they are: sieving, dividing and, shuffling. The sieving involves the secret image splitting into primary colors. The second important step is division, which involves the random division of the split image. In the third step, the divided Shares are shuffled randomly [1].
The steps involved in the algorithm are depicted as follows:

Step1: input the secret image.
Sieve is applied for input image then the output for the input image will be based on the primary colors.
Sieve (input image)
Output will be the R, G, B components.
Step 2: Division is based on the number of pixels.
Let n be the total number of pixels (0 to n-1).
Let R_i G_i B_i is the individual values of the pixel in the R G B components.
Total number of shares is Z
Total number of bits representing the primary colors is x.
MAX_VAL=2^x
Step3: Shuffle $R_{(A-Z)}$ $G_{(A-Z)}$ $B_{(A-Z)}$ for all shares.
Step4: Combine A to Z.

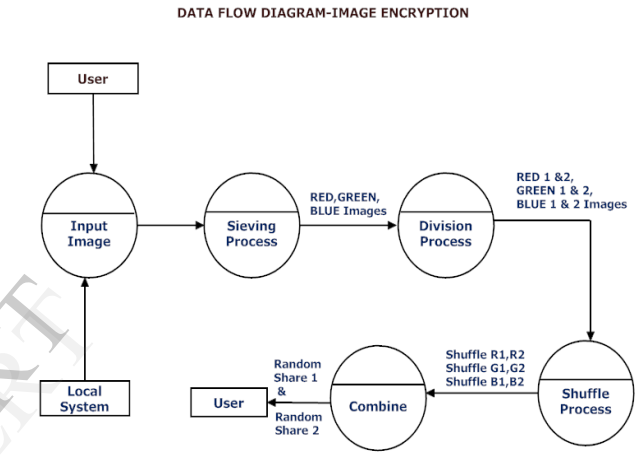

Figure 1. Data Flow Diagram

Image encryption may be classified as lossy / lossless image encryption. The conventional VC schemes all generate a degraded image quality of the recovered image and hence some modifications to VC often referred to as Variants to Visual Secret Sharing schemes have also been proposed. Hence a true comparison of our scheme would involve comparing it to the other proposed VCSs as also its variants. Most of the digital cameras today support 24 bit true color schemes and upwards, hence it is natural that most of the secret sharing schemes would need to support 24 bit color schemes. [7],[8],[9] do not support 24 bit true color scheme.

Our scheme along with Tsai et.al scheme [10] supports 4 bit true color schemes. Another important factor is how the size of the share increases with increase in the number of shares and the number of colors. This is a very critical factor when considering the bandwidth constraint i.e. transmitting the shares on the net as also the storage size of each of these shares. In the extended Thien and Lin's [11] scheme supporting true color, the size of each share increases three times. Similarly in Lukac and Plantonis [12] (n,n) threshold scheme each share becomes 2n-1

times larger, thus with increase in number of shares i.e. n, the size of the share doubles for each new participant. In our scheme the size of the random share is not a function of the number of colors in the image or the number of shares. The size of the random share thus is always constant i.e. equal to the size of the secret image. Thus the proposed schemes performs better on the bandwidth and storage requirement parameters.

In our proposed technique both during encryption and decryption the computation cost is low since the majority of the operations use logical XOR, OR and AND operators. The scheme [10] involves 3 steps, initial training, encoding and decoding. The initial training phase involves Principal Component Analysis (PCA) and Forward Neural Network (FNN). The initial training phase itself involves heavy computation cost though the encoding and the decoding phases in [10] and our scheme are comparable.

Conclusion

New enhanced visual cryptographic scheme is presented, which is a hybrid of the traditional VCS and the conventional image encryption schemes. A secret image is split into multiple random images and with minimum computation, the original secret image can be retrieved back. The proposed algorithm has the following merits (a) The original secret image can be retrieved in totality (b) There is no pixel expansion and hence storage requirement per random share is same as original image (c) Key management is not an issue since there are no secret keys involved as encryption is carried out based on the distribution of values amongst various shares (d) the scheme is robust to withstand brute force attacks.

REFERENCES

[1] "A Keyless approach to image encryption" Siddharth Malik, Anjali Sardana.
[2] Aloka Sinha and Kehar Singh, "A technique for im`age encryption using digital signature", Optics communications(2003), 218(4-6), pp 229-234, online [http://eprint.iitd.ac.in/dspace/handle/2074/1161].
[3] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001), pp 1229-1245.
[4] 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.
[5] S.Behnia,A.Akhshani,S.Ahadpour,H.Mahmodi,A. Akha-van, A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps,*Physics Letters* A 366(2007):391-396.
[6] Arpad Incze, "Pixel sieve method for secret sharing & visual cryptography" RoEduNet IEEE International Conference Proceeding Sibiu.
[7] M. Naor and A. Shamir, "Visual cryptography," in *Proc. EUROCRYPT' 94*, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.
[8] H.-C. Wu, C.-C. Chang, "Sharing Visual Multi-Secrets Using Circle Shares", Comput. Stand. Interfaces 134 (28) ,pp. 123–135, (2005).
[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] Du-Shiau Tsai , Gwoboa Horng , 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.
[11] C.C. Thien, J.C. Lin, "Secret image sharing", Computers & Graphics, Vol. 26, No. 5, 2002, pp. 765-770.
[12] R. Lukac, K.N. Plataniotis "Bit-level based secret sharing for image encryption", The Journal of Pattern Recognition Society, 2005.