World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 3.419

A SIMPLE AND EFFICIENT VISUAL CRYPTOGRAPHY SCHEME FOR SHARING MULTIPLE SECRET IMAGES

Kalyan Das[1], Aromita Sen[2] and Prof. Samir Kumar Bandyopadhyay*[3]

[1]Department of Information Technology, St' Thomas College of Engineering and Technology Kolkata, India.

[2]Department of Computer Science and Engg, St' Thomas College of Engineering and Technology Kolkata, India.

[3] Department of Computer Science and Engineering, University of Calcutta, India.

Article Received on 15/12/2015 Article Revised on 08/01/2016 Article Accepted on 02/02/2016

***Correspondence for Author**
Prof. (Dr.) Samir Kumar Bandyopadhyay
Professor, Department of Computer Science & Engineering, University of Calcutta, India.
skb1@vsnl.com

ABSTRACT

Visual cryptography is special type of technique for encipher the confidential visual information (e.g. printed text, handwritten notes, and picture) in such a way, that decipher can be performed by human visual system (HVS) without any complex process, providing high security. In this paper a simple but robust visual cryptography scheme is proposed. In this scheme the secret is encrypted using symmetric key encryption algorithm, and then this encrypted data will be hidden into an image file, divided into parts called shares and then they are Distributed to the participants. Thus accomplishing both data encoding and hiding. Only piling of shares does not revile the secret until shares are stacked together in a particular fashion and provided with the key. It can be used to hide the original secret information from an intruder or an unwanted user. The shares are very safe because separately they reveal nothing about the secret image. The algorithm proposed by this scheme reduces a considerable time for encryption and decryption in a much easier way and ensures the lossless transmissions of images. The proposed encryption algorithm in this study has been tested on some images and showed good results.

KEYWORDS: Visual Cryptography, Visual cryptographic scheme, Symmetric Key Encryption, Multiple Secret sharing.

1. 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. To deal with the security problems of secret images, various image secret sharing schemes have been developed. And also the required amount of computation to encrypt the images and the overhead required to maintain the keys and perform the computation is a matter of concern. This gave rise to new technologies in the area of Image Cryptography which would require less computation and less storage. 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. Model proposed by Naor and Shamir is based on threshold scheme where a binary secret image is encrypted into multiple shares. Since it can be employed by anyone without any cryptographic knowledge and does not require any computations while decrypting, many researches' have been focused on it. This technique does not require any key management nor does it require any algorithm for decryption. In our scheme we have used palindrome number concept to encrypt the secret image which is a simple and efficient way for cryptography.

2. RELATED WORK

The basic model of Visual Cryptography was introduced by Naor and Shamir [3] in 1994 accepts binary image I(x, y) as secret image, which is divided into 'n' number of shares. Each pixel of image I(x, y) is represented by 'm' black and white sub pixels in each of the 'n' shared images. Naor and Shamir proposed a *k* out of *n* scheme and assumed that the image or message is a collection of binary data 0 and 1displayed as black and white pixels. According to their algorithm, the secret image is turned into *n* shares and the secret is revealed if any *k* of them are stacked together. So the image remains hidden if less than *k* shares are stacked. Decryption is achieved by stacking the shares and thus introduces noise. It is impossible to get any information about the secret images from individual shares. But the main disadvantage is, if someone get all the shares he/she can easily retrieve the secret message by stacking the shares.

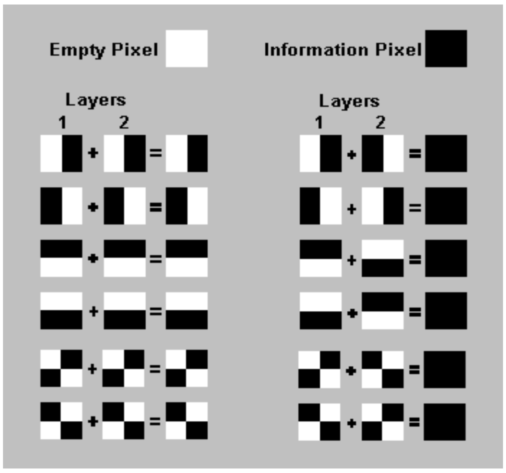


Figure 1.

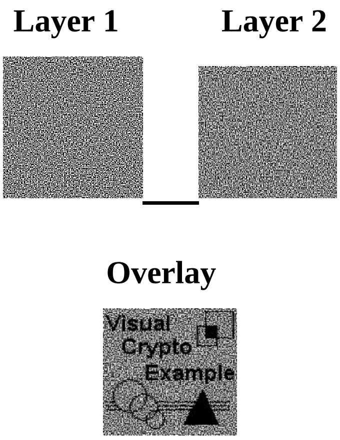


Figure 2: Example of traditional (2, 2)-VCS with image size 128x128.

3. PROPOSED SCHEME

The proposed scheme consider security of image in terms of encrypting it with the help of palindrome nature and then breaking into shares using symmetric key, hence if someone access all the shares in unauthorized way, he/she can't decrypt it completely without symmetric key and the shares. This scheme manages decrypted images of same size as original ones. The quality of the image revealed is same as the original image. This algorithm has perfect reconstruction property and there is no loss of picture quality. The scheme is divided into several parts:

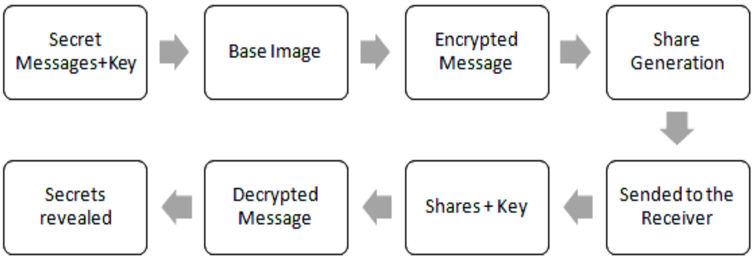


Figure 3. Flow chart representation of the proposed scheme

4. METHODOLOGY

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

➢ **Pre-processing**

- Read any Random Color Image (Base Image) to hide the message.
- Read all the pixels in the base image in uint8 format (8 bpp).
- Make all the pixel values as non-palindrome i.e. the LSB of the pixel values will differ from their MSB.

- **Encryption**

- Read all the three Secret Image (Message 1, 2, 3) and hide in the different levels of the base image.
- If any message pixel is black (Message(i,j)=0) then change the corresponding pixel in the random image to the nearest palindrome value i.e. by making the LSB of the pixel value same as the MSB.
- Otherwise no modification is done with the pixel values of the base image.
- It results the encrypted image.

- **Share generation**

- Take any three Random Color images of same size as that of the Secret image.
- Distribute the values of the encrypted image with the help of the symmetric key. (3 digit Key, where digits are ranging from 1 – 4).

- **Network**

- Send the share images to the client.
- The same key used in share generation is needed to retrieve the messages at the time of retrieval from shares.

- **Retrieval**

- At the receiver side the shares are processed with the help of the keys to get back the Encrypted image of same size.
- For each share the particular bits of the key will be used. So the key along with the shares should be arranged in a particular manner in order to get the exact image.

- **Decryption**

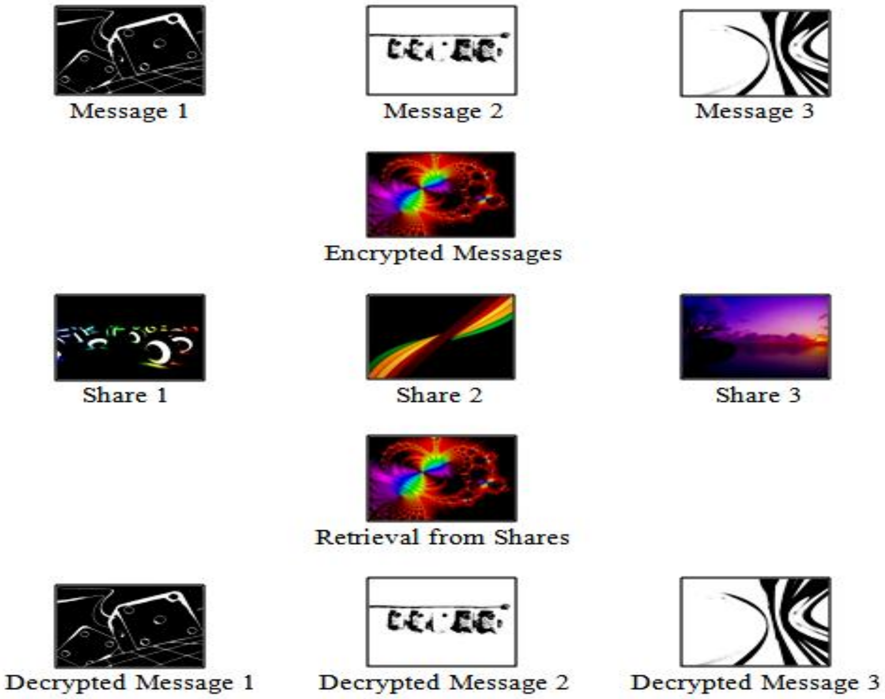
- Read the Encrypted image.
- If pixel contains any palindrome value then it indicates a message pixel is black in the corresponding position of the secret image (message(i,j)=0)else white (message(i,j)=1).

5. IMPLEMENTATIONAL DETAILS

In this paper, the number of pixel in the decoded image is same as in the original secret. The secret image is encoded using palindromic nature which doesn’t allow anyone to identify the secret visually. The size of secret image must be smaller or equal to the cover images. After testing on many different images the results are as our expectation and the shares are clear without any visual abnormality. The above mentioned scheme is implemented into "MATLAB R2009a". All that is required is to transmit key on a secret channel while encrypted form can be transmitted on an unsecure channel.

6. EXPERIMENTAL RESULTS

The results were validated using Structural Similarity (SSIM) index [15] for measuring the quality between two images. The SSIM index can be viewed as a quality measure of one of the images being compared provided the other image is regarded as of perfect quality. The quality measures are calculated between the original image and the decrypted image and we have got SSIM value=1 which proves a lossless decryption procedure.



7. CONCLUSION

As conclusion it can be said that; visual information where size and security is more concerned and the proposed visual cryptography has a simple, lossless implementation module. In this paper, we have presented a new visual cryptographic system which can be used to hide multiple images into color images in encrypted form. The original secret image can be retrieved in totality. The encryption procedure is totally new and can't be disguised easily by the intruder as it don't effects the base image that much and the message is hidden as a part of it. So from the shares or the encrypted message there is no chance of any visual disturbance. But, this scheme increases some kind of computation at time of encryption and decryption. (For encryption and hiding procedure it takes 19.175858 seconds and at the receiver side it takes 1.237009 seconds for 640*480 sized 3 message images).The algorithm encryption and decryption of images uses symmetric key, which allow users to have confidentiality and security in transmission of the image based data. The key used is of size 24bit. This scheme is best suitable for pictures having secret in the form of binary image.

8. FUTURE WORK

The future work is to improve the security of retrieval of the encoded message. This scheme can be extended for colored images and providing more security. We can also try to reduce the time needed for encryption and decryption procedure.

9. REFERENCE

1. www.ijest.info/docs/IJEST10-02-06-83.pdf
2. www.cs.fsu.edu/yasinsac/group/slides/burke2.pdf
3. Naor and A. Shamir,"Visual cryptography", Advances in Cryptology EUROCRYPT "94,M LectureNotes in Computer Science, 1995; 950(7): 1–12.
4. N. Gowdham, S.D. Libin Raja, M. Sornalakshmi, M. Navaneetha Krishnan, "Two Step Share Visual Cryptography Algorithm for Secure Visual Sharing", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, 2(3): 656 – 660.
5. Jyoti Rao, Dr. Vikram Patil," Meaningful Shares Through Visual Cryptography For Better Security Of Images During Transmission", International Journal of Advance Foundation and Research in Computer (IJAFRC) ISSN 2348 – 4853, January 2015; 2: 879.
6. Mr. Rohith S Mr. Vinay G," A Novel Two Stage Binary Image Security System Using (2,2) Visual Cryptography Scheme." International Journal of Computational Engineering Research / ISSN: 2250–3005.
7. P.S.Revenkar, Anisa Anjum, W. Z.Gandhare, "Survey of Visual Cryptography Schemes", International Journal of Security and Its Applications, 4(2); April, 2010.
8. Renu Poriye, Dr S. S Tyagi, "Secret Sharing Using Visual Cryptography", IJRSCSE, ISSN 2349-4840, (Print) & ISSN 2349-4859, August 2014; 1(4): 46-52.
9. Shyamalendu Kandar, Arnab Maiti, Bibhas Chandra Dhara, "Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking", IJCSI International Journal of Computer Science Issues, ISSN (Online): 1694-0814, May 2011; 8(3): 1.

10. Survey of Visual Cryptography Schemes", P.S.Revenkar, Anisa Anjum, W. Z. Gandhare, International Journal of Security and Its Applications, 4(2): April 2010.
11. A New Visual Cryptography Scheme for Color Images", B. SaiChandana, S. Anuradha, International Journal of Engineering Science and Technology, 2010; 2(6): 1997-2000.
12. Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking", Shyamalendu Kandar1, Arnab Maiti2, Bibhas Chandra Dhara3, IJCSI International Journal of Computer Science Issues, ISSN (Online): 1694-0814, May 2011; 8(3): 1.
13. Secret Sharing Using Visual Cryptography", Renu Poriye, Dr S. S Tyagi, International Journal of Research Studies in Computer Science and Engineering (IJRSCSE) ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online), August 2014; 1(4): 46-52.
14. New Visual Cryptography Algorithm For Colored Image", Sozan Abdulla, Journal of Computing, ISSN 2151-9617, April 2010; 2(4).
15. Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity, "IEEE Transactions on Image Processing, April. 2004; 13(4): 600-612.

Authors

Mr. Kalyan is an Assistant Professor in the Information Technology Department, St' Thomas College of Engineering and Technology Kolkata, India.

Ms. Aromita Sen, Department of Computer Science and Engg, St' Thomas College of Engineering and Technology Kolkata, India.

Prof. Samir Kumar Bandyopadhyay, Professor of Computer Science & Engineering, University of Calcutta.