Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 90 (2016) 37395-37397

ISSN: 2229-712X

A Simple and Efficient Visual Cryptography scheme for Sharing Secret Image

Kalyan Das[1] and Samir Kumar Bandyopadhyay[2]

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

[2]Lincoln University, Malaysia

ARTICLE INFO

Article history:

Received: 18 November 2015;

Received in revised form:

25 December 2015;

Accepted: 1 January 2016;

Keywords

Visual Cryptography,
Visual cryptographic scheme,
Symmetric key,
Encryption.

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.

Introduction

In network technology, multimedia information is transmitted over the Internet. Confidential data such as military maps and commercial identifications are transmitted over the Internet. For transmitting secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want .To deal with this security problems of secret images or confidential data, various encryption algorithms are available but it needs a large computing for encryption as well as for decryption. One possible technique is cryptography where information is encrypted using key and same key is used to decrypt the information. Model proposed by Naor and Shamir is based on threshold scheme where a binary secret image is encrypted into multiple shares. In our scheme we have used palindrome number concept to encrypt the secret image which is a simple and efficient way for cryptography.

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.

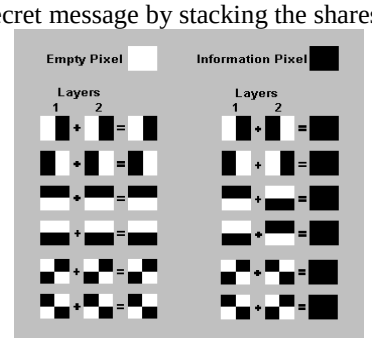

Figure 1

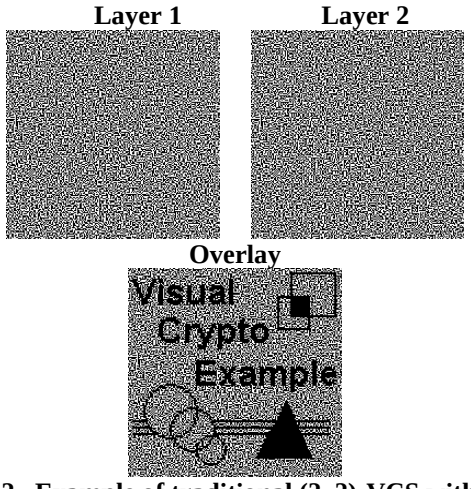

Figure 2. Example of traditional (2, 2)-VCS with image size 128x128

Tele:

E-mail addresses: kalyan.das@outlook.in

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 lossless retrieval, security as well as decrypted images are of same size as original. The scheme is divided into several parts:

Pre-processing

- Read any Random Color Image (Base Image) to hide the message.
- Read all the pixels in the base image as 3 digit decimal numbers ranging from 0 to 255 (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 the Secret Image (Message).
- 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 message in 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).

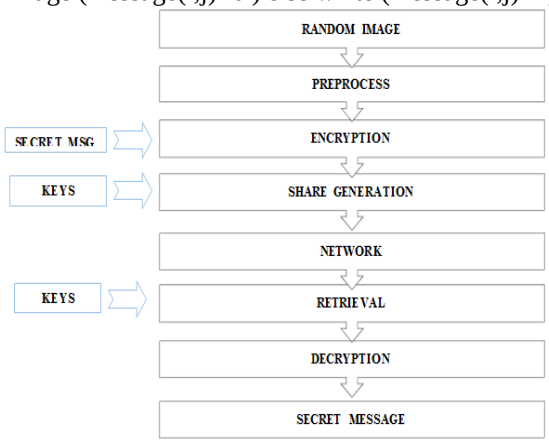

Figure 3. Flow chart representation of the proposed scheme

Experimental Result

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 don'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".

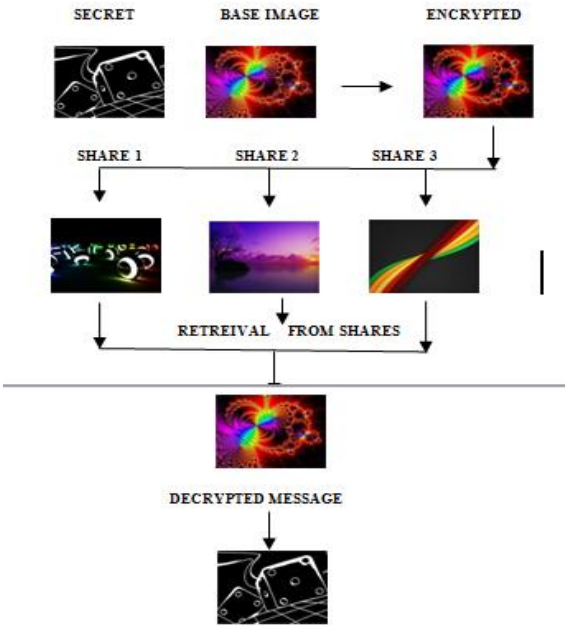

Figure 4. Output of The Proposed Scheme

Conclusion

As conclusion it can be said that; visual information where size and security is more concerned and the proposed visual cryptography has a simpl, lossless implementation module. In this paper, we have presented a new visual cryptographic system which can be used to hide the original image into color images in encrypted from. 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 20.41 seconds and at the receiver side it takes 1.0001 seconds for 640*480 sized message image). The algorithm encryption and decryption of an image uses symmetric key, which allow users to have confidentiality and security in transmission of the image based data. The key is of 24bit. This scheme is best suitable for pictures having secret in the form of binary image.

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.

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 Lecture Notes in Computer Science, vol.950,no.7, pp.1–12, 1995

[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 656 – 660 Volume: 2 Issue:3

[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) Volume 2, Special Issue (NCRTIT 2015), January 2015. ISSN 2348 – 4853 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 Vol. 4, No. 2, April, 2010

[8] Renu Poriye, Dr S. S Tyagi, "Secret Sharing Using Visual Cryptography", IJRSCSE Volume 1, Issue 4, August 2014, PP 46-52 ISSN 2349-4840 (Print) & ISSN 2349-4859

[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, Vol. 8, Issue 3, No. 1, May 2011 ISSN (Online): 1694-0814