International Journal of Research in Engineering, Science and Management
Volume-3, Issue-4, April-2020
www.ijresm.com | ISSN (Online): 2581-5792

Visual Cryptography - A Secure Medium

Aashutosh Sehgal[1], Abhinav Chaudhary[2], Aditya Sangwan[3], Ajay Sharawat[4], Vishal Jayaswal[5]
[1,2,3,4]*Student, Department of Computer Science and Engineering, Meerut Institute of Engineering and Technology, Meerut, India*
[5]*Professor, Department of Computer Science and Engineering, Meerut Institute of Engineering and Technology, Meerut, India*

***Abstract*: Secret information is main topic focused in systems used for communication an effective and secure protection is through encrypting the data. The data must be protected from being tampered by any process going on within the systems. Encryption of data is one of the methods to make sure that integrity and confidentiality of important information is available. The major role of encryption techniques is to prevent exposure of information to unnecessary individuals. Secret image sharing is also an alternative to consider as a solution to problems, especially for long detailed information so called as secret images. Nowadays with the increase in networking industry the transmission of images and other multimedia can be done easily. This use of secret sharing is increased because hackers can find the weak points of a communication system and attack to extract confidential information being transmitted over the network.**

***Keywords*: Visual cryptography, Security, Secretly data sharing, Visual Cryptography.**

1. Introduction

Visual cryptography was firstly discovered by Noar and Shamir in 1994. Encryption of a visual information using the cryptography technique such that the decryption is only possible using proper orientation of images or with the right algorithm for overlapping. Transferring multimedia information using Internet is very common these days. Various techniques and methods have been developed to solve the problem of sharing of secret images and these tools can be used to resolve this problem. The splitting of images should be done such that even hacker is able to make available any share but is not able to get any information out of it. In today's scenario of electronic commerce, the need to solve the issue of sharing information safely considering the fact of using network as medium of sharing information. Regular efforts of hackers to gain secret information are done as a result of which there is an urgent need to make both communication medium as well as communication tools and techniques safe and secure. The scheme of visual secretly sharing of the image is to eventually divide it into 'n' total shares. As all 'n' shares are combined, the secret image is created. The benefit of using this technique is that even if the hacker gets 'n-1' shares they would not be able to get the main secret image as all the 'n' shares are required to generate the secret image.

2. Literature review

The main operation of Visual Cryptography is based on the use of binary inputs. As the binary data is displayed transparent when imprinted on screen that is transparent itself. Smaller blocks are used to divide every pixel of the secret image. Same numbers of black and white blocks are present in the image or the blocks. Only 1 black and 1 white block is there if any of pixel is split into two parts. And so on goes on if pixel gets split in 4 parts, 2 black and 2 white blocks are formed out of it. Fig. 1 shows an example for division into 2x2 blocks and Fig. 2 is superimposed image.

Figure 1: Two 2 × 2 pixel blocks

Figure 2: Superimposed Image

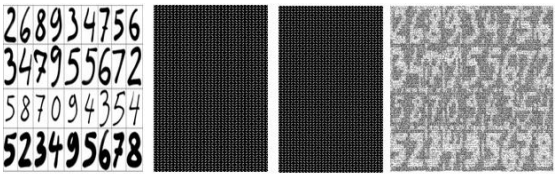

Fig. 3. Example of Visual Cryptography

Visual secret sharing is the most simple out of problems of messages that comprise of black and white pixels and each pixel is handled separately. 'n' modified shares are generated for each original pixel that appears, one for each transparency. 'm' black and white sub-pixels are formed for each share, they are imprinted as close pattern to each other such that visual system create a median of the separate black as well as white versions. Structure that is formed by shares and contribution can be explained by Boolean matrix which is (nxm) and S is expressed [sij], where *sij*->1 and when the jth pixel is black in transparency. The framework is almost similar to the Naor and Shamir whereas the important difference that their framework that divides into 'n' shares of binary secret image. The 'm' sub pixels are used to explain each pixel of image. Black and white schema of visual cryptography is illustrated by a Boolean matrix of the form 2(n x m) where (S0 and S1). Main image i.e.

white pixel image is represented using S0 and but if main image is black then S1 is used instead. Representation of white and black pixel is done by 0 and 1 respectively in the technique of visual cryptography. Various visual cryptography techniques are used eg. 2 / 2, 2 / n, n/n and k/n. The 2/2 is the widely taken in use to explain the Visual Cryptography schema.

The 2/2 Visual Cryptography technique S1 and S0 is expressed as,

$$S0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \quad S1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

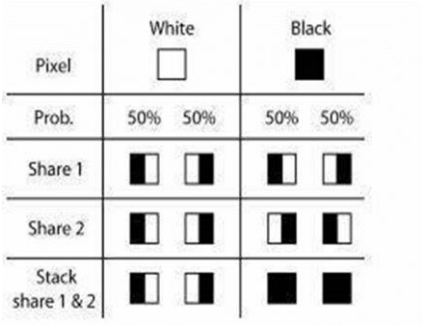

Fig. 4. Formation of 2 by 2 VC schema

Two different Q0 and Q1 matrices. We select the matrix Q0 to give a white pixel and the matrix Q1 is used give a black pixel. The very initial row of selected matrix is for the share S1 and the row after the is for the share S2.

The encoding of every pixel of the main image into two sub pixel is the disadvantage and if main image sized S x S is positioned by share and is sized as S X2S. Due to the distortion present we take 4 sub pixel as design layout. Also the expansion of pixel is 2 by 2 pixels.

$$S0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad S1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

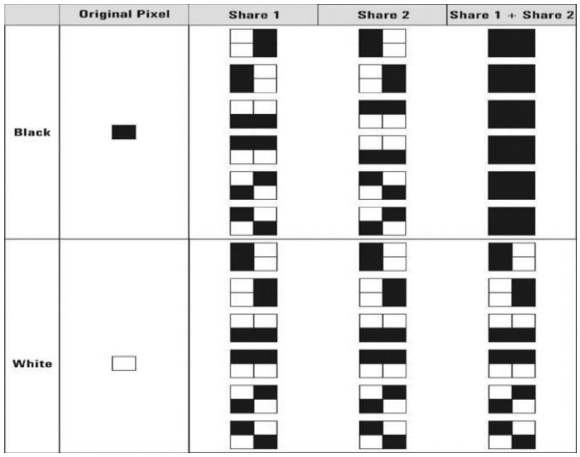

Fig. 5. Illustration of 2 X 2 Visual Cryptography technique using a layout design of 4 sub pixel

3. Proposed algorithm

Our project uses an advance technique of Visual Cryptography where an image is taken and eventually divided as 2 shares. Share 1 also called random share whereas the share 2 is main/key share that contains confidential information. The shares share 1 and share 2 have nothing in common to the secret image. The combination of the shares by XORing generates the secret image. There is no change in the quality of image created and the secret image. This algorithm has efficient recombination property and there is no loss of pixel so far. The use of algorithm is only bound for Black and white images without the loss of pixel.

Algorithm:

Step 1: Generation of random share
Step 2: Generation of key share
Step 3: Combining both the shares to generate secret image

In given step 1: For monochrome image a random share is generated for every pixel that has either 0 or 1 as it's value. So, by picking randomly either 1 or 0 the random share would be created. Share size is same as that of the secret image. Different value is generated for each pixel each time a random share is created. Therefore, 2 randomly generated shares of the original image can never be equivalent.

In given step 2: XORing is the technique used to for key share generation where each and every pixel taken from the share randomly created is XORed with each and every pixel of the secret image. No change in size of original image and share can be seen. As it is seen that no 2 randomly generated shares can be same as a result of which no 2 key shares can be same.

In given step 3: XORing of randomly generated share and key share pixel after pixel is done to find the overlapping or resultant image. The result of which is the generation of the desired secret image.

For Monochromatic Images

```
Algo RaKeOv ( )
 For each pixel j=0 to n
{
      RaSj = Ra (0-1)
      KeSj = DSj ⊕ SIj
}
SI = DS ⊕ JS
 }

/* SI = Secret Image, DS=Random Share, JS=Key Share*/ *
```

4. Results and Discussions

Report of test cases:

The test cases that are discussed above can be seen to have passed.

A. 8-bit Gray Scale Image

Example:

The algorithm has its implementation on gray scale image that is shown in Fig. 6. 2 different shares S1 and S2 as shown in Fig. 7 and Fig. 8 respectively. After overlapping S1 and S2 the resultant image is shown in Fig. 9.

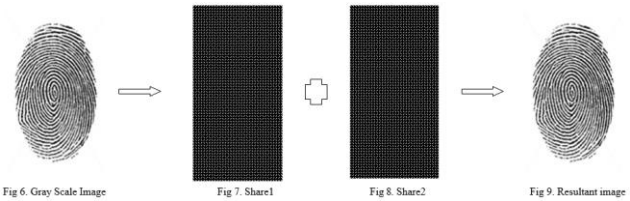

Fig 6. Gray Scale Image Fig 7. Share1 Fig 8. Share2 Fig 9. Resultant image

B. 1-bit Black and White image

Example:

The algorithm is also tested on B & W image as shown in Fig. 10. 2 shares S1 & S2 are shown as Fig. 11 and Fig. 12. After overlapping S1 and S2 the resultant image is shown in Fig. 13.

Fig. 10. Monochromatic message

Fig. 11. Share1

Fig. 12. Share2

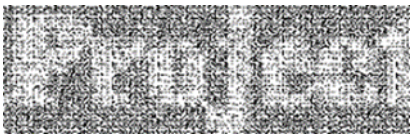

Fig. 13. Resultant image

5. Conclusion

The key logic behind the project is the splitting of the original image into two shared images, a randomly generated image and the other one is the key image and the secret image can be easily get back by performing least computation possible.

This project has the following merits:

a) Retrieval of original image with completeness and integrity.
b) Storage requirement for each share is same as no pixel expansion takes place.
c) No quality change of the image.
d) The logic in project is for gray scale images and B & W images.

Project checks the authentication where access to original image is given only when overlapped using right algorithm and right shares generated for the give image to reveal the original message. The secret image is accessed using combination of both the shares if any one of them is missing then the original or secret cannot be retrieved else if one does not have the right algorithm to overlap the image is not generated.

6. Future scope

Visual Cryptography has a lot of scope in future for encrypting images. The method used in the project produces the exact image similar to the original image or message to be sent. Randomly generated shares are for the i/p image, this technique is improvised by increasing randomness in shares.

References

[1] Moni Naor, Adi Shamir, “Visual Cryptography”, Advances in cryptology, 1995.
[2] M. Naor and A. Shamir,1996. Visual cryptography ii: Improving the contrast via the cover base. Theory of Cryptography Library.
[3] Sandeep Katta, “Visual Secret Sharing Scheme using Grayscale Images”, Department of Computer Science, Oklahoma State University Stillwater
[4] Feng Liu and chuankun Wu. (2011), ‘Embedded Extended Visual Cryptography Schemes’, IEEE *transactions on information forensics and security*, vol. 6, no. 2, pp. 307-322.
[5] Swarnalata Bollavarapu and Ruchita Sharma, “Data Security using Compression and Cryptography Techniques.”
[6] Kulvinder Kaur and Vineeta Khemchandani, “Securing Visual Cryptographic Shares using Public Key Encryption,” 2013 3rd IEEE International Advance Computing Conference (IACC).
[7] https://en.wikipedia.org/wiki/Cryptography
[8] https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf
[9] https://en.wikipedia.org/wiki/Cryptography
[10] Ateniese G, "Extended capabilities for visual cryptography", Theoretical Computer Science.
[11] Ida Christy, V. Seenivasagam. "Construction of color Extended Visual Cryptographic scheme using Back Propagation Network for color images", 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), 2012.
[12] Daisy, Annie, J. Arokia Renjith, P. Mohan Kumar, and L. Selvam, "Achieving Secrecy in Visual Secret Sharing Scheme Using Encrypted Images", Journal of Applied Security Research, 2014.
[13] Feng, J. B, "Visual secret sharing for multiple secrets", Pattern Recognition.