Visual Cryptography using Image Thresholding

Daisy Das

M.tech, Computer Science and Engineering, GIMT, Assam, India

---***---

Abstract - *This paper proposes a novel visual cryptographic algorithm using image thresholding. The technique used simple image thresholding to generate a keyless scheme with a minimal computational load. The approach creates two shares of images from the original secret image. The shares are produced by thresholding the secret image such that the individual share do not reveal any information about the secret image. Most visual cryptography algorithms result in a wrong reconstruction of original image restricting the use of the scheme. In this method, the original image could be formed by Oring the pixel value of the shares with the threshold value without any loss of information or image quality. At such the secrecy, accuracy and confidentiality of the secret image is maintained while sharing over a medium.*

Key Words: Visual cryptography; shares; keyless; image; computational complexity, accuracy; secrecy; thresholding; algorithm

1.INTRODUCTION

With an exponential increase in technology, the internet has become a prominent medium for sharing of multimedia information over the network. Many cryptographic methods have been developed in the recent past for sharing of secret information over the network. This gave dimension to a new cryptographic technique known as visual cryptography. Visual cryptography was first introduced in 1994 by Naor and Shamir [1]. The visual information encrypted using Visual cryptography can be decoded using a standard human visual system, without the aid of computers by a layman. Visual cryptography scheme does not require complex computation in decryption process, and overlapping operation can regenerate the secret images. It does not need any particular cryptographic knowledge to implement. Most of the technique concentrates on binary images; however few of them proposed methods for processing gray-level and color images[2]. The methods used for color images have a poor reconstruction of an original image with quality and information loss of the recovered image.

This paper describes a technique of visual cryptography using image thresholding. Two shares are generated in this scheme from the original secret image by thresholding the secret image with some defined threshold value. One share contains the image information for which pixel value is less than the threshold value, and the other provides information for which pixel value is greater than the threshold value. The original image is obtained by Oring the pixel value of the shares depending on the threshold value. This method is a keyless technique and implies no loss of pixel information from the original reconstructed image with less computational complexity. In this paper global threshold is used however adaptive and local threshold can also be applied according to users choice.

2. LITERATURE REVIEW

2.1 Thresholding

Thresholding is replacing each pixel with black if the pixel intensity value of the image is less than some fixed constant T , or a white pixel if the image intensity value is greater than that constant. Colour images can also be thresholded by thresholding each RGB component separately. Automatic thresholding requires the computer to select the threshold automatically. Sezgin and Sankur categorize thresholding methods into the following six groups based on the information the algorithm manipulates[9]

Histogram shape-histogram based method analyzed the peak-valley and curvature of the histogram.

Clustering-based thresholding clusters image into two groups as background and foreground.

Entropy-based methods use algorithms to find the degree of randomness of foreground and background pixels and separate them accordingly.

Object Attribute-based methods measure the similarity between background and foreground using algorithms of fuzzy shape similarity, edge coincidence, etc. to group the image into separate background and foreground image.

Spatial methods uses higher-order probability distribution algorithms and or measures the correlation between pixels

Local methods find threshold of each image pixel based on local area thresholding of the image using pixel connectivity between pixels.The thresholding values may differ depending on the intensity values of pixels locally.

2.2 Visual Cryptography

Visual cryptography is splitting an image into n shares such that no individual share gives any information of the image only when a subset of the shares is stacked on another it reveals the secret image. Table I provides a comparison of six such techniques[3].

Sr.	No.	Number of Secret Images	Pixel Expansion	Image Format	Type of Share generated
1.	Naor and Shamir [1]	1	4	Binary	Random
2.	Wu and Chen [4]	2	4	Binary	Random
3.	Chin-Chen Chang et al [5]	1	4	Binary	Meaningful
4.	Liguo Fang et al [6]	1	2	Binary	Random
5.	S. J. Shyu et al [7]	n(n>=2)	2n	Binary	Random
6.	W. P. Fang [8]	2	9	Binary	Random

3.PROPOSED METHOD

The proposed method uses visual cryptography with image thresholding property to provide accuracy, secrecy, and confidentiality of the secret image. Here in this algorithm global thresholding with predefined image threshold value is used.However one can also use adaptive or local threshold method according to requirement. An RGB image consists of the red, green and blue pixel plane. In the encryption phase, the scheme separates all the three planes and threshold each plane on a predefined threshold value. Each share conveys no information of the original image. While decrypting it, the original image planes are reconstructed by bitwise Oring the pixel value of these shares. Finally, the RGB planes are overlapped to form the original image. The method is used for color image and also could be used for gray scale image. The reconstructed image has no information loss and correctly recover the original image with minimal computational cost without any key management.

3.1 The algorithm

The proposed method involves four steps:

- Step 1 : Separation of an image into its constituent red, blue , green planes.
- Step 2 : Shares generation of each plane according to the predefined threshold value.
- Step 3 : **O**verlapping the two shares of each plane to reconstruct the planes.
- Step 4 : Finally the three planes are stacked to form the original secret image.

In step 1 the secret image is divided into its constituent RGB plane. In additive model or RGB model the image in made up of different RED, GREEN, and BLUE plane stack over each other to define a particular intensity value.The value of each plane range between 0-255.

In step 2 the threshold value is determined, and each separate RGB plane of the colored image is a limit based on this threshold value. Hence one share contains image information having pixel values greater than the threshold value and the other includes image data having pixel values less than the threshold value. In total, the three RGB planes have two shares each resulting in 6 shares.

In step 3 the shares obtained in step 2 are overlapped by Oring the value of pixel information depending on the pixel value from the two shares to a third image reconstructing the desired RGB plane. This step is repeated for each RGB plane restoring the three planes.

In step 4 the RGB planes obtained in step 3 are joined to form the required color image.

Algorithm ( )

```
{
Red plane = Image(Redvalue(0-255))
Green plane = Image(Greenvalue(0-255))
Blue plane = Image(Bluevalue(0-255))
Th=threshold value
 For each Red,Green,Blue Plane
{
        For every pixel i=0 to n
         {
                If(pixel value<th)
                {
                Share 1=pixel value
                }
                Else
                {
                Share2 =pixel value
                }
        }
        For every pixel i=0 to n

        {
                If(pixel value<th)
                {
                Reconstructed Image value=share1 OR
        share2
                }

}
```

3.2 Implementation details

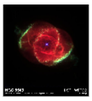
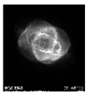
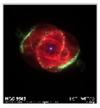
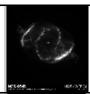
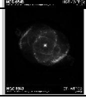
The algorithm was implemented using Matlab on Windows XP where two functions encrypt and decrypt were used. encrypt encrypts the image by creating the two shares by comparing it with the threshold value. decrypt decrypts the image by Oring the shares pixel value with the defined threshold value into the third image reconstructing the original image. This functions works for color images and can be extended to gray scale images as well. In our proposed technique the cost incurred for encryption and decryption are less since the majority operations are comparison and OR operations. In the proposed scheme there are no keys involved, and hence there is no key management.

4. EXPERIMENTAL RESULTS

4.1 Color Image

The method was implemented on a color image with the threshold value (th=231) in Matlab showed in Table 2. The two shares of the picture formed are share1 and share2 shown in column 3 and column 4 respectively. The original image and resultant image which is reconstructed after overlapping the three planes are shown in column 1 and column 6 respectively. Column 5 represents the reconstructed planes after overlapping both share1 and share2.

Table 2 Algorithm implementation for Colored Image

Original image	plane	Share 1>th	Share 2<th	overlapped Plane	Recovered Image
	Red				
	Green				
	Blue				

5. RESULTS AND DISCUSSIONS

The method gives a replica of the original image without any loss of information. The results were validated using Normalized Correlation (NC)[3]. NC is used to calculate the correlation between both the encoded and decoded image

$$NC=\sum_{i=1}^{w} \sum_{j=1}^{h}(S_{ij} \oplus R_{ij})/w \times h$$

S represents the secret image and R the recovered image. w, h represents the width/height of the photographs and represents the exclusive OR operator. The algorithm was repeated for a test over multiple images, the NC for all the recovered images was 1.000. Table 3 gives a detailed feature set of our algorithm

Table 3: Feature set of the algorithm

Features	Thresholding
Noise Correlation	Always 1.00
Image transparency Delivery	Depends on threshold value
Additional Data Structure	no
Key Management	no
Pixel expansion	no

3. CONCLUSIONS

In this paper, a novel hybrid Visual Cryptography technique with image thresholding is presented. It is a hybrid approach of the conventional Visual Cryptographic Scheme and the traditional image encryption schemes together with image thresholding method. A secret colored image is split into its constituent RGB planes, and two shares from each plane are generated, one share image has pixel value greater than a predefined threshold, and another shared image has pixel value lesser than the specified threshold, and with minimum calculation, the original secret image can be reconstructed. The proposed algorithm has the following advantages (a) There is no information loss when the original image is restored back. (b) The storage requirement is same as the original image as the exact original image is replicated (c) It is a keyless encryption method (d) It can counter attacks such as guessing, brute force attacks and shouldering. (e) The same technique can be extended to grayscale images. (f) The individual shares reveal no information about the secret image thus can be sent via an unsecured network. The proposed scheme is suited for entity authentication based application where authentication can be done by overlapping the shares over one another to reveal the secret information. If the hidden image matches the original image, then access is granted else denied

REFERENCES

[1]Moni Naor and Adi Shamir, "Visual Cryptography," Advances in cryptology– Eurocrypt, pp 1-12,1995.
[2] Y. C. Hou, "Visual cryptography for color images," Pattern Recognition, vol. 36, pp. 1619-1629, 2003.
[3] Ms. Moushmee Kuri, Dr. Tanuja Sarode, "RKO Technique for Color Visual Cryptography," in : IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 89-93

[4] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography," Master Thesis, Institute of Computer and
[5] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin, "Sharing A Secret Two-Tone Image In Two Gray-Level
[6] Liguo Fang, BinYu, “Research On Pixel Expansion Of (2,n) Visual Threshold Scheme”, 1st International
[7] S. J. Shyu, S. Y. Huanga, Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual
[8] Wen-Pinn Fang, “Visual Cryptography In Reversible Style," IEEE Proceeding on the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2007), Kaohsiung, Taiwan, R.O.C, 2007.
[9] Mehmet Sezgin and Bulent Sankur, Survey over image thresholding techniques and quantitative performance evaluation, Journal of Electronic Imaging 13(1), 146–165 (January 2004).