VISUAL CRYPTOGRAPHY SCHEME FOR COLOR IMAGES

B. Saichandana
Assistant Professor
Department of Computer Science and Engineering
GIT, GITAM University, Visakhapatnam

Dr. K. Srinivas
Associate Professor
Department of Computer Science and Engineering
Pydah College of Engineering

Dr. Reddi Kiran Kumar
Assistant Professor
Department of Computer Science
Krishna University, Machilipatnam

ABSTRACT:

Visual cryptography is a method for protecting image based secrets that has a computation-free decoding process. In this paper, we propose a new visual cryptography scheme for color images based on CMY model, half toning technique and the traditional binary image sharing scheme. The image shares generated by our method are transmitted to the destination through a network and the image is decrypted by stacking any two transparencies. The image can be in any standard format. This scheme provides an efficient way to hide the natural image among different shares. Furthermore, the size of the shares and the implementation complexity do not depend on the number of colors appearing in the secret image.

I. INTRODUCTION:

Data hiding and visual cryptography are used to introduce confidentiality and security when visual data are transmitted through unsecured channels. Data hiding techniques try to embed data in digital media and transmit it in an imperceptible way. On the other hand, in visual cryptography or visual secret sharing, the original input is shared
between a set of participants by a secret image holder. Based on the sharing policy, only qualifies subsets of participants can recover the original input image.

Visual cryptography [1] is a cryptographic technique which allows visual information (pictures, text, etc) to be encrypted in such a way that the decryption can be performed by the human visual system without the aid of computers. The most traditional visual cryptography scheme is used for black and white images. Recently, some visual cryptography schemes for gray or color images have been proposed. In all the proposed schemes [2, 3, 4], if the number of colors in an image is large, the worse the resolution of the decrypted images.

Two important factors are used to determine the efficiency of any visual cryptography scheme [5], namely: 1) the quality of the reconstructed image and 2) the pixel expansion factor (m). Any loss of information during the reconstruction phase leads to the reduction in the quality of the recovered image. On the other hand pixel expansion refers to the number of sub-pixels in the generated shares that represents a pixel of the original input image. For bandwidth constrained communication channels it is desirable to keep ‘m’ as small as possible. For color images, reducing pixel expansion is of paramount importance since they occupy more space and more bandwidth compared to grey scale and binary images.

The paper is organized as follows: Section II presents the proposed scheme, Section III presents the experimental results and finally section IV makes the conclusions.

II PROPOSED SCHEME:

The proposed color image sharing scheme is based on the CMY model, half toning technique and the traditional binary image sharing scheme.

Firstly, a chromatic image is decomposed into three monochromatic images in tones of cyan, magenta and yellow. The purpose of using a color model is to facilitate the specification of colors in some standard, generally accepted way. In essence, a color model is a specification of a coordinate system and a subspace within that system where each color is represented in a single point. The CMY color model is used in our method. This conversion is performed using the simple operation given in Figure 1.
Secondly, these three monochromatic images (cyan, magenta and yellow) are transformed into binary images by half toning technique. Halftone is a method to display an image in black and white spots. In this paper, we use Floyd-Steinberg algorithm to generate the halftone images.

**FLOYD AND STEINBERG ALGORITHM:**

Assume, \( g \) is the gray value of the image, which location is \( p(x,y) \).

- \( e \) is the difference between the computed value and correct value.
- \( b=0 \).
- \( w=255 \).
- \( t=128 \cdot ((b+w)/2) \)

if \( g > t \) then

print white;

\( e=g-w \);

else

print black;

\( e=g-b \);

\((3/8 \cdot e)\) is added to \( p(x+1,y) \);

\((3/8 \cdot e)\) is added to \( p(x,y+1) \);

\((1/4 \cdot e)\) is added to \( p(x+1,y+1) \)

Endif

Thirdly, we consider every monochromatic image as a secret image and use the traditional binary image sharing scheme to divide it into three secret shares with the same color, and then we can choose any three different colors of which to compose them into three colored shares. We have used (2, 3) visual threshold scheme for natural images [6], for the generation of shares with the matrices shown in Figure 2.

\[
\begin{pmatrix}
C \\
M \\
Y
\end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} R \\ G \\ B \end{pmatrix}
\]

Figure 1 Conversion from RGB to CMY

\[
\begin{pmatrix}
0 & 1 & 1 \\
0 & 1 & 1 \\
0 & 1 & 1
\end{pmatrix} = M_0
\]

\[
\begin{pmatrix}
1 & 0 & 1 \\
1 & 0 & 1 \\
1 & 0 & 1
\end{pmatrix} = M_1
\]

\[
\begin{pmatrix}
1 & 1 & 0 \\
1 & 1 & 0 \\
1 & 1 & 0
\end{pmatrix} = M_2
\]

Figure 2 Matrices used in binary image sharing
Finally, these shares are transmitted through a communication channel to the destination. The original secret information will be visible by stacking any 2 or 3 transparencies, but none secret information will be revealed by only one transparency.

As stated in section I, the efficiency of any visual cryptography scheme depends on two factors i.e; the quality of the reconstructed image and the pixel expansion factor ‘m’. We used the Structural Similarity (SSIM) index [7] 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, generated shares and the recovered image. In our proposed scheme, a) the size of the shares is equal to the size of the original input image, implies that no extra bandwidth is required for transmitting the shares through a communication channel and b) the generated shares perfectly recover the output image with SSIM index near to 1. These are the key advantages of our visual cryptography scheme.

**III EXPERIMENTAL RESULTS:**

This section presents the simulation results illustrating the performance of the proposed Visual cryptographic scheme. The test image employed here is the true color image “flower” with 290×290 pixels. The encryption and decryption algorithm are implemented in Matlab 7.0 in core2duo of 2.66 GHz machine.
e) S3 (share 3)  
f) S1+S2  
f) S2+S3  
g) S1+S3  
h) S1+S2+S3

Figure 3 Simulation results for (2,3) scheme

Figure 3(a) is an original chromatic image. The image is decomposed into three monochromatic images in tones of cyan, magenta and yellow. These three images are transformed into binary images by halftoning technique. If we compose those three monochromatic images, we get figure 3(b). By using the binary image sharing scheme, we divide every monochromatic image into three secret shares with same color, and then, we can choose any three different colors of which to compose them into three colored shares shown in figures 3(c), 3(d) and 3(e). The original information will be visible by stacking any 2 or 3 transparencies as shown in figures 3(e), 3(f), 3(g) and 3(h).

Table 1 shows the quality measures that are calculated between the original image, generated shares and the recovered image by using the SSIM index.

<table>
<thead>
<tr>
<th>Image</th>
<th>SSIM Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original image</td>
<td>1</td>
</tr>
<tr>
<td>S1 (share 1)</td>
<td>0.0041</td>
</tr>
<tr>
<td>S2 (share 2)</td>
<td>0.0032</td>
</tr>
<tr>
<td>S3 (share 3)</td>
<td>0.0036</td>
</tr>
<tr>
<td>S1+S2</td>
<td>0.88</td>
</tr>
<tr>
<td>S2+S3</td>
<td>0.89</td>
</tr>
<tr>
<td>S1+S3</td>
<td>0.87</td>
</tr>
<tr>
<td>S1+S2+S3</td>
<td>0.94</td>
</tr>
</tbody>
</table>

Table 1: SSIM index values for images in Figure 3
CONCLUSION:

In this paper, we have presented a new kind of visual cryptography scheme based on CMY model, half toning and binary secret sharing scheme. The advantages of the proposed method are its pixel expansion factor (the size of the share is same as the size of the original image) and its capability of perfect reconstruction of the secret image. This work is an attempt to make a secured transfer of valuable images between two trusted parties. The confidentiality is maintained and the authentication can be checked by digital signatures. It can be shown that the proposed scheme do not depend on the number of colors appearing in the secret image.

REFERENCES:


