IMPROVED NEW VISUAL CRYPTOGRAPHIC SCHEME USING ONE SHARED IMAGE

Gowramma B.H\textsuperscript{1}, Shyla M.G\textsuperscript{1}, Vivekananda\textsuperscript{2}
\textsuperscript{1}PG Student, \textsuperscript{2}Assistant Professor
Department of Computer Science and Engineering,
Adichunchanagiri Institute of Technology, Chikmagalur, Karnataka, India

ABSTRACT

Visual cryptography scheme is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. The Improved Visual Cryptography Scheme (VCS) differs from any existing visual cryptography schemes; this scheme encodes one binary secret image into one shared image with innocent-looking. The secret image is visually revealed by superimposing the portion of the share and its other portion together. The Improved VCS has the advantages of resisting geometry distortion, easy recognition and management, the size of the revealed image is same size as that of original secret image.

KEYWORDS: Visual cryptography scheme, geometric distortion.

I. INTRODUCTION

Digital information and data are transmitted more often over the Internet now than ever before. The availability and efficiency of global computer networks for the communication of digital information and data have accelerated the popularity of digital media. Digital images, video, and audio have been revolutionized in the way they can be captured, stored, transmitted, and manipulated, and this gives rise to a wide range of applications in education, entertainment, media and military, as well as other fields. Computers and networking facilities are becoming less expensive and more widespread. Creative approaches to storing, accessing and distributing data have generated many benefits for the digital multimedia field, mainly due to properties such as distortion-free transmission, compact storage and easy editing. Visual Cryptography Scheme (VCS) was introduced by Naor and Shamir in 1995. The basic concept of the conventional (k, n)-threshold VCS\cite{1} is that one binary secret image is encoded into n random-looking images called shares or shadows which are then distributed to n corresponding participants. Any k or more participants print their shares on transparencies and superimpose the transparencies together; the secret image is visually reconstructed. However, any k-1 or fewer participants cannot get any information about the secret image.

Many visual cryptography schemes (VCS)\cite{2}\cite{3}\cite{4} have been proposed to meet different requirements. Various k-out-of-n VCS were also proposed by different researchers to support variable threshold numbers, in which the secret image is split into n share images and the secret can be retrieved by the cooperation of at least k of them. If the number of shares stacked is less than k, the original image is not revealed. The other schemes are 2-out-of- n and n-out-of-n VCS. In the 2-out-of-n scheme n shares will be produced to encrypt an image, and any two shares must be stacked to decrypt the image. In the n-out-of-n scheme, n shares will be produced to encrypt an image, and n shares must be stacked to decrypt the image. If the number of shares stacked is less than n, the original image is not revealed. Increasing the number of shares or participants will automatically
increase the level of security of the encrypted message. The researchers also extended visual cryptography schemes to support grayscale images and color images. A novel EVCS [5] using one shared image encodes one secret image into one innocent-looking share. The secret image is visually revealed by copying the share, shifting the copy and superimposing the shifted copy and the original share together.

In this paper, an improved VCS using one shared image is proposed. The proposed scheme encodes one secret image into one innocent-looking share. The secret image is visually revealed by superimposing the portion of the share and its other portion together. The self-decrypt characteristic of the proposed scheme make it more robust against geometry distortion, while conventional VCSs and EVCSs are not.

In section 2, we discuss the related literature with respect to visual cryptography schemes. The section 3 discusses about general access structure. The section 4 discusses about the proposed scheme. The section 5 gives results and discussions of the proposed scheme. The section 6 gives conclusion and future enhancement of the work.

II. LITERATURE SURVEY

Moni Naor and Adi Shamir [1], introduces a new type of cryptographic scheme, which can decode concealed images without any cryptographic computations. The scheme is perfectly secure and very easy to implement. They extend it into a visual variant of the k out of n secret sharing problem, in which a dealer provides a transparency to each one of the n users; any k of them can see the image by stacking their transparencies, but any k - 1 of them gain no information about it. The main results of [1] includes practical implementations of a k out of n visual secret sharing scheme for small values of k and n, as well as efficient asymptotic constructions which can be proven optimal within certain classes of schemes.

P. Tsai and M. Wang [3], proposes an improved (3, 3)-visual secret sharing scheme, which can be used to embed three secret messages into three shares and improve security. First of all, the fist main share image is resulted randomly and other two share images are based on the first share image and the two coding tables designed by them. In the conventional (3, 3)-visual secret sharing scheme, it is usually to embed one confidential messages, the proposed conventional (3, 3)-visual secret sharing scheme has been extended to encrypt three secret images. It is also provides increased security.

Rijmen and Preneel [11] have proposed a visual cryptography approach for color images. In their approach, each pixel of the color secret image is expanded into a 2×2 block to form two sharing images. Each 2×2 block on the sharing image is filled with red, green, blue and white (transparent), respectively, and hence no clue about the secret image can be identified from any one of these two shares alone. Rijman and Preneel claimed that there would be 24 possible combinations according to the permutation of the four colors. Because human eyes cannot detect the color of a very tiny subpixel, the four-pixel colors will be treated as an average color. When stacking the corresponding blocks of the two shares, there would be 242 variations of the resultant color for forming a color image.

L. Duo and D. Yi-Qi [4], they proposed a new scheme on hiding a secret image into single shadow image. It can also be used as a technique of digital watermarking. Differ from any existed methods of visual hiding schemes using one secret image, the new scheme based on the rotation of the shadow image. In this scheme, the single shadow image acted both encoder and decoder function. Therefore the secret image can be recovered by stacking the shadow image and the shadow image after rotated 90 degree anticlockwise. The new method has the property of anti-compression, anti- distortion and anti-shrink. Furthermore, the new scheme can use the shadow image sufficiently.

Xiaotian Wu and Wei Sun [5], they proposed a novel extended visual cryptography scheme using one shared image. Differ from any existing visual cryptography scheme, the proposed scheme encodes one secret image into one shared image with innocent-looking. The secret image is visually revealed by copying the share, shifting the copy and superimposing the shifted copy and the original share together. Extended visual cryptography scheme using one shared image has the advantage of resisting geometry distortion. Comparing to the two existing one share based VCSs [4], the share generated by the proposed scheme is easy to recognize and manage. The innocent-looking of the share make it draw less attention from attackers.
III. GENERAL ACCESS STRUCTURE

An access structure is a rule [6], which defines how to share a secret. The most familiar examples are (n, n) and (t, n) threshold access structures. A (t, n) threshold access structure rules that any t or more out of n participants can cooperate to reveal the secret image and any less than t participants together get nothing about the secret image. Obviously, a (n, n) threshold access structure is one instance of the (t, n) threshold access structure. It demands all participants to cooperate for a secret recovery and hence nothing can be seen even if only one attendee is absent. It is easy to know that a (t, n) threshold access structure is tolerant because the final secret still can be restored from the other t shares even though up to (n−t) shares are corrupted.

However, threshold access structure is only one special case of the so-called general access structure. Usually, a general access structure is denoted as Γ = {A0, A1}, where A0 and A1 are sets of subsets of all participants and A0 ∩ A1 = Ø. Furthermore, A0 denotes a collection of forbidden sets and A1 denotes a collection of qualified sets. It is easily known that stacking all the shares held by the participants of any qualified set can recover the secret image; but stacking all the shares held by the participants of any forbidden set cannot reveal any information about the secret image. For example, in a system with four participants, we let A1 = {{1, 2}, {2, 3}, {3, 4}, {1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}, {1, 2, 3, 4}}, which implies that A0 = {{1}, {2}, {3}, {4}, {1, 3}, {1, 4}, {2, 4}}. Therefore, we can learn that stacking share 1 and share 2 can recover the secret image; however, stacking share 1 and share 4 can reveal nothing about the secret image.

It is easy to know that a general access structure should follow the monotone property: if γ ∈ A1 and γ ⊆ γ′, then γ ′ ∈ A1; if λ ∈ A0 and λ⊇λ′, then λ ′∈ A0. So we can learn that the fact {1, 2} ∈ A1 implies it is truly sure that {1, 2, 3} ∈ A1, {1, 2, 4} ∈ A1 and {1, 2, 3, 4} ∈ A1; the fact {1, 4} ∈ A0 implies that {1} ∈ A0 and {4} ∈ A0. Furthermore, we also can let A1− = {{1, 2}, {2, 3}, {3, 4}} and A0+ = {{1, 3}, {1, 4}, {2, 4}} to represent above mentioned A1 and A0 respectively in terms of the monotone property. In fact, A1− is usually named the family of minimal qualified sets and A0+ is the family of maximal forbidden sets. In many situations, it is more convenient to refer to them instead of A1 and A0.

IV. THE PROPOSED SCHEME

In this section, an improved VCS using one shared image is proposed. The binary secret image is encoded into one share with innocent-looking [5]. The secret image is visually revealed by superimposing the portion of the share and its other portion together. The decryption of the proposed scheme is very simple. By selecting upper most portion of share and lower most portion of the share and superimposing them together gives the revealed secret image and exor-ing the each pixel in blocks of size 2x2 from a revealed secret image to improve the reconstructed image.

4.1. Encryption Process

In encryption process binary image with m x n pixels is considered as the secret image. Then, a cover image with innocent-looking is selected. The cover image has to be larger than the secret image. Here, the size of the cover image is assumed to be M x N, where M >m, N>=n or M >=m, N>n. The encryption of the proposed scheme is divided into two parts. Part 1 of the encryption algorithm encodes Area 1 of the share, Part 2 encodes Area 2. Area 1 and 2 of the share are demonstrated in Figure 1. The share is generated based on the secret image and cover image. Each pixel of secret image is expanded into a 2x2 subpixel block. Therefore, the size of the output share is 2M x2N.

The basis matrices of the proposed scheme used in the encryption are illustrated in Table 1. Matrices used in Area 2 are generated based on the three conditions of EVCS [7]. In the basis matrices, 1 represents black pixel and 0 represents white pixel.
Table 1. Basis matrices of the evc

<table>
<thead>
<tr>
<th>Area Of The Share</th>
<th>Basis Matrices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area 1</td>
<td>$T^w = [0 \ 0 \ 1 \ 1]$</td>
</tr>
<tr>
<td></td>
<td>$T^b = [0 \ 1 \ 1 \ 1]$</td>
</tr>
<tr>
<td>Area 2</td>
<td>$T^{w_w} = [0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0]$</td>
</tr>
<tr>
<td></td>
<td>$T^{w_b} = [0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0]$</td>
</tr>
<tr>
<td></td>
<td>$T^{w_b} = [0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1]$</td>
</tr>
<tr>
<td></td>
<td>$T^{w_b} = [0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0]$</td>
</tr>
<tr>
<td></td>
<td>$T^{b_w} = [1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1]$</td>
</tr>
<tr>
<td></td>
<td>$T^{b_b} = [1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1]$</td>
</tr>
<tr>
<td></td>
<td>$T^{b_w} = [1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1]$</td>
</tr>
<tr>
<td></td>
<td>$T^{b_b} = [0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0]$</td>
</tr>
</tbody>
</table>

In encryption algorithm, step 2-7 encode Area 1 of the share. Step 8-13 encodes Area 2 of the share. Area 1 is firstly encoded, then Area 2. In Area 1, the subpixel block is determined by the corresponding pixel in cover image. But in Area 2, the subpixel block is determined by cover image pixel, secret image pixel and the corresponding subpixel block in Area 1.
Algorithm for encryption process
Input: Secret image S (m x n pixels), cover image C (M x N pixels)
Output: Innocent-looking share SH (2M x 2N pixels)
Step 1: Compute p=M-m and q=N-n.
Step 2: For i=1 to p and for j=1 to N, repeat step 3-4.
Step 3: Obtain the corresponding basis matrix TC(i, j) from Table 1 Area 1 according to C(i,j).
Step 4: Randomly permute the columns of the determined basis matrix and assign the elements of the permuted basis matrix to the pixels SH (2i-1, 2j-1), SH (2i, 2j-1), SH(2i-1,2j), SH(2i,2j) of the share.
Step 5: For i = p+1 to M and for j=q+1 to N, repeat step 9-13.
Step 6: Obtain the corresponding basis matrix TC(i, j) from Table 1 Area 1 according to C(i,j).
Step 7: Randomly permute the columns of the determined basis matrix and assign the elements of the permuted basis matrix to the pixels SH (2i-1, 2j-1), SH (2i, 2j-1), SH(2i-1,2j), SH(2i,2j) of the share.
Step 8: For i =p+1 to M and for j=q+1 to N, repeat step 9-13.
Step 9: Find out the corresponding basis matrices TS(i,j) for all possible. All these basis matrices and their permuted matrices form a matrix set MS.
Step 10: For i =p+1 to M and for j=q+1 to N, repeat step 11 until all the matrices in MS are checked and the candidate vector set CVS is formed.
Step 11: Fetch one matrix from MS. Check the first row of this matrix is equal to SH(2i-1,2j-1), SH(2i,2j-1), SH(2i-1,2j), SH(2i,2j) of the share.
Step 12: If yes, put the second row of this matrix into the candidate vector set CVS. If not, move to the second row and conduct the above processing.
Step 13: Randomly choose one vector in CVS and assign this vector to the pixels SH(2i-1,2j-1), SH(2i,2j-1), SH(2i-1,2j), SH(2i,2j) of the share.
Step 14: Output the innocent-looking share SH.

The vital parts of encryption algorithm are finding the corresponding basis matrices and forming the candidate vector set when Area 2 is encoding. For instance, assume that pixels in C(i, j) and S(i, j) are 1 and 0, respectively. The obtained basis matrices in Table. 1 Area 2 are

\[ T_{bw}^{w} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \]

\[ T_{bw}^{w} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \]

\[ T_{bb}^{w} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \]

If the corresponding four pixels SH(2i-p, 1,2j-q-1), SH(2i-p, 2, j-q-1), SH(2i-p-1,2j-q), SH(2i-p,2, j-q)) in Area 1 of the share are 1, 0, 0, 1, respectively. The formed candidate vector set is \{1011,1101\}.

Then, one vector is randomly selected from the candidate vector set and assigned to the pixels SH(2i-1,2j-1), SH(2i,2j-1), SH(2i-1,2j), SH(2i,2j) of the share.

Let us consider an example
S be secret image of size 2x2 and C be cover image of size 3x3

\[
S = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}
\]
C =

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

The generated share is of size 6x6.

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

**4.2. Decryption Process**

The decryption process of the proposed scheme is very simple. By selecting upper most portion of share and lower most portion of the share and superimposing them together gives the revealed secret image and exor-ing the each pixel in blocks of size 2x2 from a revealed secret image to improve the reconstructed image.

The decryption process of the proposed scheme is illustrated in Figure 2. Superimposing the uppermost portion of the share of size 2mx2n is selected i.e plain area in the below figure and lowermost portion of the share of size 2mx2n is selected i.e shaded area in the below figure reveals the secret image.

![Figure 2: Decryption Process](image-url)

Considering the above mentioned example, the share generated in the encryption process is
The uppermost portion of the share is:

\[
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 \\
\end{array}
\]

The lowermost portion of the share is:

\[
\begin{array}{cccc}
0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 \\
\end{array}
\]

Superimposing the 2 portions of the share reveals the secret image of size 2mx2n and xor-ing the each pixel in blocks of size 2x2 from a revealed secret image and then negating it improves the reconstructed image quality and also reduces its size to original secret image.

\[
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array}
\]

Revealed secret image=

\[
\begin{array}{cc}
1 & 1 \\
1 & 0 \\
1 & 1 \\
\end{array}
\]

Final revealed image=

\[
\begin{array}{cc}
1 & 1 \\
1 & 0 \\
\end{array}
\]

V. RESULTS AND DISCUSSION

To demonstrate the effectiveness of the proposed scheme, examples are illustrated in this section. The secret image with 200x200 pixels is shown in figure 3 and cover image with 249x260 pixels is shown in Figure.4. The innocent-looking share of size 498x520 shown in Figure.5 Figure.6 shows the superimposed image of size 400x400. The final reconstructed image after xor-ing the each pixel in
blocks of size 2x2 is shown in Figure 7. The PSNR value between secret image and reconstructed image is 11.6052 dB and histogram error between secret image and final reconstructed image is 0.00078408. The histogram error of superimposed image and secret image is 0.1185. The histogram error of proposed VCS is smaller than the histogram error of the existing VCS it shows that the proposed scheme gives more similar image of secret image.

![Figure 3. Secret image of size 200x200](image1.png)

![Figure 4. Cover image of size 249x260.](image2.png)

![Figure 5. Share image of size 498x520.](image3.png)
VI. CONCLUSION

In this paper, an Improved VCS using single shared image is presented. The proposed scheme hides one secret image into one innocent-looking share. The secret image is visually revealed by superimposing the portion of the share and its other portion together. The proposed scheme has the advantage of resisting geometry distortion and the revealed secret image size is same as that of original secret image. Comparing to the two existing one share based VCSs, the share generated by the proposed scheme is easy to recognize and manage. The innocent-looking of the share make it draw less attention from attackers and image quality is also improved.

VI. FUTURE ENHANCEMENT

Several future enhancements can be made to this VCS. This proposed scheme can be enhanced by using the morphological operations and using filters to remove the noise in the image. The proposed system is designed to run on single host machine, the work can be extended to run on multiple host machines.

REFERENCES


AUTHORS

Gowramma B H, is currently Pursuing 4th Semester, Master of Technology in Computer Science and Engineering at AIT, Chickmagalur. She has completed her Bachelor of Engineering from PES Institute of Technology and management, Shivamogga. She had published a paper. Her areas of interests include visual cryptography and Information Security.

Shyla M G, is currently Pursuing 4th Semester, Master of Technology in Computer Science and Engineering at AIT, Chickmagalur. She has completed her Bachelor of Engineering from Adichunchanagiri Institute of Technology, Chikmagalur. She had published a paper. Her areas of interests include image processing and Information Security.

Vivekananda is presently working as assistant professor in the Department of Computer Science and Engineering, Adichunchanagiri Institute of Technology, Chikmagalur, Karnataka, India. He had 9 years of teaching experience. He obtained his Master of Technology degree from SJCIE Mysuru under Visveswaraya Technological University, Belgaum. His research interests include Image Stegonography, Visual Cryptography, and Language Processing.