ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 7, September 2012

Secret Sharing Image Between End Users by using Cryptography Technique

SRINIVASA RAJESH KUMAR D.

M.Tech Scholar

Department of CSE ,
B V C Engineering college,
Odalarevu

P.MARESWARAMMA

Associate Professor

Department of CSE,
B V C Engineering college,
Odalarevu

Abstract:

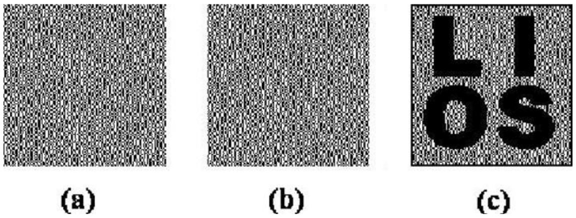
In this Secret Sharing Image(SSI) we are divide the complete image into n shares distributed to n participants. Only authorized persons access the secret image without any cryptography knowledge and the end user will decrypt the original image. In this secret image no users can share. Now a days developed different technique for recover the exact image without image loss in addition they are using the cryptography techniques.

1) Introduction:

Secret Sharing Image is user's Cryptographic technique. In this technique the image will be split into the two random shares (printed on transparencies), which will tell that there is no other image in the visual image, but internally there is a secret image. In this SSI the original image is taking as input and output will be n shares it satisfies the two conditions:

- Authorized (qualified) persons subset can recover the secret image
- Un authorized (forbidden) subset of cannot access the secret image other than the size of secret image

Observe an example of (2, 2) image in Fig 1, where generally speaking a (k, n) – means any out n of shares could recover the secret image. In the scheme of Fig. 1, shares (a) and (b) are distributed to two participants secretly, and each participant cannot get any information about the secret image, but after stacking shares (a) and (b), the secret image can be observed visually by the participants



This technique used in the military order to soldiers. Who may have no cryptographic knowledge and computation device in better field? Other application is watermarking and transmitting password.

In this we use the color pixels, for constructions of threshold SSI with perfect reconstruction of the black pixels. And white is used to specified whiteness levels of the recovered pixels [1]SSI is treated as steganography. One application is to avoid custom inspections. Because shared images is meaningful the other persons may be modifies it may be suspected and detected.

Shares were simply generated by replacing the white and black sub pixels in a traditional SSI share with transparent pixels and pixels from the cover images, respectively. The halftoning technique contains visual information of image.

- The first SSI is share of complementary to cover the visual information of the shares as the way of proposed in [2].
- Second important is cover the visual information of the share by black pixel.

Limitation of the SSI:

There are some limitation are there.

- The first limitation is the pixel expansion is large
- The second limitation is bad visual quality of both shares and recovered images
- Third one is pair of complementary images are required for each qualified subset and the participants are required to take more than one shares for some access structures.

The SSI is simply but not satisfied constraint condition. Human eyes did not recognize the secret image.

2) Main Action:

In this section we will discus the some results about the halftoning techniques by using the dithering matrix.

a) Normal SSI

Secret sharing scheme for all participants are V = { 0,1,….n-1 }. All qualified and forbidden subsets of participants constitute an access structure $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$. where $\Gamma_{\mathrm{Qual}}$is the superset of qualified subsets, and Γ_{Forb} is the superset of forbidden subsets, and Γ_{Qual} ∩ Γ_{Forb} = Ǿ and Γ_{Qual} ∪ Γ_{Forb} = 2^{v}.

$$\Gamma_m = \{A \in \Gamma_{\mathrm{Qual}} : \forall B \subsetneq A \Rightarrow B \notin \Gamma_{\mathrm{Qual}}\}$$

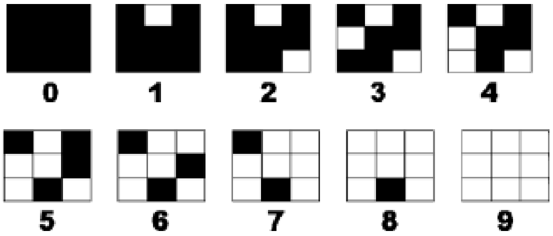
and

$$\Gamma_M = \{A \in \Gamma_{\mathrm{Forb}} : \forall B \supsetneq A \Rightarrow B \notin \Gamma_{\mathrm{Forb}}\}.$$

Then Γ_m is called the minimal qualified access structure and Γ_M is called the maximal forbidden access structure. In this paper we black and white. White pixel denoted by 0 and the black pixel is denoted by 1. The matrix is in the format of (C0,C1).

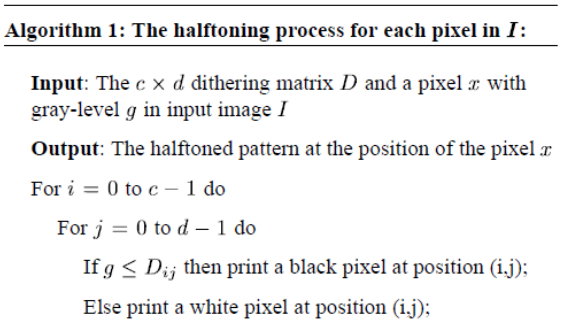
b) Halftoing Technique:

The draw back of the previous method is used gray scale image MacPherson [3] proposed. However, it has large pixel expansion c x m, where the number of the gray-levels and m is is the pixel expansion of the corresponding black and white SSI. Halftoning is introduced by [4][5][6]. Halftoning is converting the gray scale image to binary image. This method will give effective output.



Halftoned patterns of the dithering matrix

The dithering makes use of a certain percentage of black and white pixels, often called patterns, to achieve a sense of gray scale in the overall point of view. The halftone technique process the gray scale image in to certain no of black pixels. The halftoned image is a binary image.



Algorithm 1: The halftoning process for each pixel in I:

```
Input: The $c \times d$ dithering matrix $D$ and a pixel $x$ with gray-level $g$ in input image $I$
Output: The halftoned pattern at the position of the pixel $x$
For $i = 0$ to $c - 1$ do
    For $j = 0$ to $d - 1$ do
        If $g \leq D_{ij}$ then print a black pixel at position (i,j);
        Else print a white pixel at position (i,j);
```

3) The SSI's Main Idea :

In this M0 and M1 are the basic matrix of traditional SSI with access structure $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$. and pixel expansion m. They will take original image as input and convert into n gray scale image subpixels. There are two conditions are there

i) Qualified people may recover the subpixel.

ii) Qualified persons can access only part of original image.

The first condition ensures that the secret image can be visually observed by stacking a qualified subset of shares. The second condition ensures that the shares are all meaningful in the sense that parts of the information of the original share images are preserved.

The idea of our embedded EVCS contains two main steps:
1) Generate n covering shares, denoted as ; s0,s1….sn-1
2) Generate the embedded shares by embedding the corresponding
SSI into n the covering shares, denoted as

4) Covering the image using Dithering Matrices:

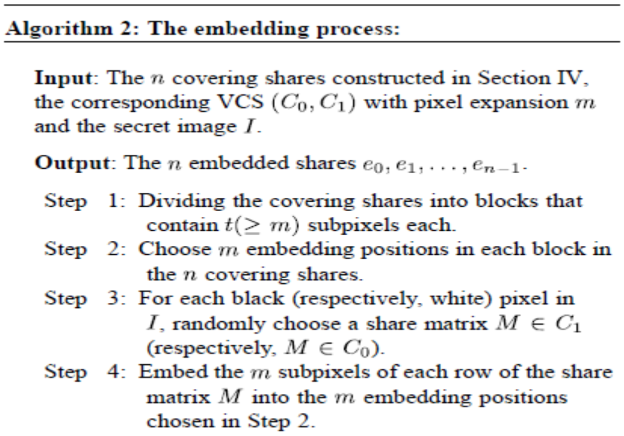
Covering shares S_0,S_1……S_{n-1}. by using the n input original shares images I_0,I_1….I_{n-1}

$$D_1 = \begin{array}{|c|c|c|}\hline 1 & 8 & 3 \\ \hline 6 & 4 & 2 \\ \hline 5 & 0 & 7 \\ \hline \end{array}$$

Dithering matrix is D_0 Let, Gray levels of the pixels in the image I_0 are smaller than 4, where D_{ij}^{0} is the entry in the i th row and j th column of D_0 . If I_1 is gray levels pixel small then 5, Then we get D_{01}^{1} , D_{10}^{1} , D_{20}^{1} and D_{22}^{1} are pixels in the image, I_1^{1} always black stack images I_0^{1} , I_0^{1} and I_1^{1} are covering shares.

Generally, Construct the covering shares S_0, S_1,…. S_{n-1}. for general access structure Γ_m . The dithering matrix D_0, $D_{1,...}$ $D_{n-1.}$ we get the covering shares S_0, $S_{1,...}$ $S_{n-1.}$ Satisfying that the stacking results of the qualified covering shares are all black images[7]

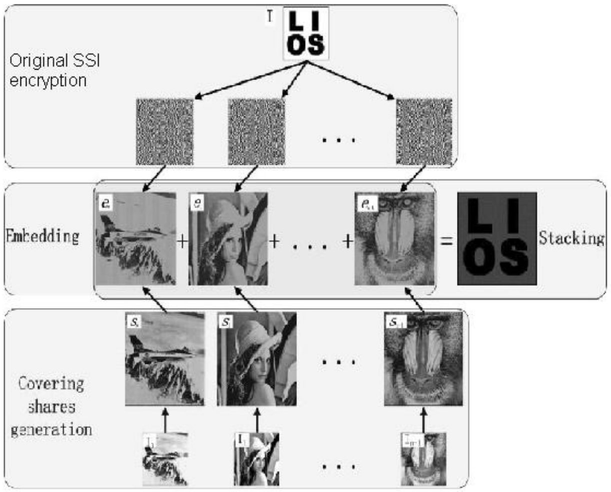
5) SSI into the covering shares :



```
Algorithm 2: The embedding process:

Input: The $n$ covering shares constructed in Section IV, the corresponding VCS $(C_0, C_1)$ with pixel expansion $m$ and the secret image $I$.
Output: The $n$ embedded shares $e_0, e_1, \ldots, e_{n-1}$.
Step 1: Dividing the covering shares into blocks that
        contain $t(\geq m)$ subpixels each.
Step 2: Choose $m$ embedding positions in each block in
        the $n$ covering shares.
Step 3: For each black (respectively, white) pixel in
        $I$, randomly choose a share matrix $M \in C_1$
        (respectively, $M \in C_0$).
Step 4: Embed the $m$ subpixels of each row of the share
        matrix $M$ into the $m$ embedding positions
        chosen in Step 2.
```

p x q is covering share, each covering share divide into (pq)/t blocks each block contain t sub pixels , where t>=m, chose m positions in each t sub pixels to embedded the m sub pixels of M. At this point t-m subpixels that have not embedded by secret subpixel are always black.



m subpixels in the share matrix corresponding to one secret image , m subpixels are position into t – positions in the n covering. The secret image pixel expansion is t in our constructions.

6) Image Visual Quality Improving:

If we reduce black ratio, then it will enhance the visual quality shares, there are two ways to improve visual quality first s = t, and $s \neq t$, s is the share pixel , t is the secret image pixel expansion.

i) s = t :

Here Ai is the block ratio requires gray levels of all the pixels in the original input image Ii[8], to be no large s-|Ai| It will satisfies the same requires .If the black ratio is high then the dark image produces will decrease the visual quality of the covering share, so black ratio will small recall that for t sub pixels. This will reduce the block ratio.

ii) $s \neq t$

The construction of the dithering Matrices for each input original share image for

1) Concatenate starting dithering matrices with entries, and divide these starting dithering matrices into blocks.
2) Choose the embedding positions in each block.
3) Concatenate the blocks, and divide the Minot dithering matrices.
4) For each dithering matrix, remove the embedding positions, and the rest of the positions in each dithering matrix constitute the universal set for this dithering matrix.
5) Generate the dithering matrixes according to Construction

.

Conclusion:

In this paper we proposed to send an image by using cryptographic technique, that image accessed by qualified persons, Forbidden persons not access that image. We will get exact image without losing any quality.

References:

[1] P. A. Eisen and D. R. Stinson, Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," *Designs, Codes and Cryptography*, vol. 25, pp. 15–61, 2002

[2] Z. Zhou, G. R. Arce, and G. Di rescenzo, "Halftone visual cryptography,"*IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453,Aug. 2006.

[3] L. A. MacPherson, "Grey Level Visual Cryptography for General Access Structures,"Master Thesis, University ofWaterloo,Waterloo, ON, Canada, 2002.

[4] Y. C. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 1773, pp. 1–11, 2003.

[5] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," in *Proc. WSCG Conf. 2002*, 2002, pp. 303–412.

[6] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognit. Lett.*, vol. 24, no. 1-3, pp.349–358, 2003.

[7] S. Droste, "New results on visual cryptography," in *Proc. CRYPTO'96*, 1996, vol. 1109, pp. 401–415, Springer-Verlag Berlin LNCS.

[8] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *ACM Theoretical Comput. Sci.*, vol. 250, no. 1–2, pp. 143–161, 2001.

About the Authors:

Srinivasa Rajesh Kumar Duvvakula is currently pursuing his M.Tech in Computer Science and Engineering at BVC Engineering College Odalarevu.

P Mareswaramma is currently working as an Associate Professor in Computer Science and Engineering department, BVC Engineering College Odalarevu. His research interests include data mining, web mining.