Integrated Intelligent Research (IIR)

International Journal of Computing Algorithm
Volume: 03, Issue: 01 June 2014, Pages: 97-100
ISSN: 2278-2397

Visual Secret Sharing for Secure Biometric Authentication using Steganography

A B Rajendra[1], H S Sheshadri[2]
[1]Research Scholar, PES College of Engineering, Mandya, Karnataka, India
[2]Professor &Dean (Research), E & C Department, PES College of Engineering, Mandya, Karnataka, India
Email: rajendraab@hotmail.com, hssheshadri@hotmail.com

Abstract- Visual secret sharing (VSS) is a kind of encryption, where secret image can be decoded directly by the human visual system without any computation for decryption. Secret image is reconstructed by simply stacking the shares together. Steganography using visual secret sharing (SVSS) is an improved version of visual secret sharing where it embeds the random patterns into meaningful images. One of the applications of SVSS is to avoid the custom inspections, because the shares of SVSS are meaningful images, hence there are fewer chances for the shares to be suspected and detected. The disadvantage of VSS is that the interceptors are able to identify that the secret image has been encrypted. Therefore we propose a method so that it is difficult for the interceptors to know about the presence of the shares. In this Paper, The secret image is encrypted by the corresponding VSS, and then we embed its shares into the covering shares.
Keywords-component;Visual secret sharing (VSS), Steganography using visual secret sharing SVSS, Visual cryptography (VC)

I. INTRODUCTION

Secret sharing is to divide the information into pieces, so that qualified subsets of these shares can be used to recover the secret. Intruders need to get access to several shares to retrieve the complete information. Similarly, they need to destroy several shares to destroy the whole information. The concept of secret sharing was independently introduced by Shamir [1]. An example of such a scheme is a *k-out-of-n* threshold secret sharing in which there are *n* participants holding their shares of the secret and every *k* ($k \leq n$) participants can collectively recreate the secret while any *k-1* participants cannot get any information about the secret.

The need for secret sharing arises if the storage system is not reliable and secure. Secret sharing is also useful if the owner of the secret does not trust any single person [2-4]. Visual secret sharing is one such method which implements secret sharing for images [5]. This technique was introduced by the Naor and Shamir in 1994.Visual Secret Sharing is a field of cryptography in which a secret image is encrypted into *n* shares such that stacking a sufficient number of shares reveals the secret image[6]. In VSS the shares generated contains only black and white pixels which make it to difficult to gain any information about the secret image by viewing only one share.The secret image is revealed only by stacking sufficient number of shares. There are different types of visual secret sharing schemes, like *2-out-of-n*, *n-out-of-n* and *k-out-of-n*.In *n-out-of-n* scheme *n* shares will be generated from the original image and in order to decrypt the secret image all *n* shares are needed to be stacked[7-10]. In this paper,when we refer to a corresponding VSS of an SVSS, we mean a VSS that have the same access structure with the SVSS. Generally, an SVSS takes a secret image and *2* original share images as inputs and *n* outputs.There have been many SVSSs proposed in the literature. Visual secret sharing & biometrics methods have their own drawbacks. By using the Visual Cryptography for biometric authentication technique avoids data theft [11-12].

This paper is organized as follows. Section II introduces the fundamental principles of VSS, based on which our method is proposed. Section III explains about proposed SVSS.Section IV shows our proposed method of steganography using VSS. Finally, conclusions are drawn in section V.

II. VISUAL SECRET SHARING SCHEMES

Basic Model

Consider a set Y = {1, 2 . . .n} be a set of elements called participants. By applying set theory concept we have 2^Y as the collection subsets of Y.

Let $\Gamma_Q \subseteq 2^Y$ and $\Gamma_F \subseteq 2^Y$, where $\Gamma_Q \cap \Gamma_F = \theta$ and $\Gamma_Q \cup \Gamma_F = 2^Y$, members of Γ_Q are called qualified sets and members of Γ_F are called forbidden sets. The pair (Γ_Q, Γ_F) is called the access structure of the scheme.

Γ_O can be defined as all minimal qualified sets:
$\Gamma_{O=} \{A \in \Gamma_Q : A^1 \notin \Gamma_{Q\ for}$ all $A^1 \subset A\}$
Γ_Q can be considered as the closure of Γ_O. Γ_O is termed a basis, from which a strong access structure can be derived. Considering the image, it will consist of a collection of black and white pixels. Each pixel appears in *n*shares, one for each transparency or participant. Each share is a collection of *m* black and white sub-pixels. The overall structure of the scheme can be described by an n x m (No. of shares x No. of subpixels).Boolean matrix $S = [S_{ij}]$, where S_{ij}= 1 if and only if the j^{th}subpixel in the i^{th} share is black.

S_{ij}= 0 if and only if the j^{th}subpixel in the i^{th} share is white.
Following the above terminology, let (Γ_Q, Γ_F) be an access structures on a set of *n*participants. A (Γ_Q , Γ_F, α)- VSS with the relative difference α and set of thresholds $1 \leq k \leq m$ is realized using the two n x m basis matrices S_W and $S_b$if the following condition holds[14]:

1. If $X = \{ i_1, i_2, \ldots\ldots i_p \} \in \Gamma_Q$, then the "or" V of rows i_1, i_2, ……i_p of $S_w$satisfies $H(V) \leq k - \alpha.m$, whereas, for S_b it results that $H(V) \geq k$.
2. If $X = \{ i_1, i_2, \ldots\ldots i_p \} \in \Gamma_F$, then the two p x m matrices obtained by restricting $S_w$and S_b to rows i_1,i_2, ……i_p are identical up to a column permutation.The first condition is called contrast and the second condition is called security. The

International Journal of Computing Algorithm
Volume: 03, Issue: 01 June 2014, Pages: 97-100
ISSN: 2278-2397

collections C_w and C_b are obtained by permuting the columns of the basis matrices S_W and S_b in all possible ways. The important parameters of the scheme are:

1. *m*, the number of sub pixels in a share.i.e blowing factor (pixel expansion). This represents the loss in resolution from the original image to the shared one. The m is computed using the equation:

$$m = 2^{n-1} \quad (1)$$

2. α, the relative difference, it determines how well the original image is recognizable.The α to be large as possible. The relative difference α is calculated using the equation:

$$\alpha = | n_b - n_w | / m \quad (2)$$

where$n_b$and $n_w$represents the number of black sub pixels generated from the black and white pixels in the original image.

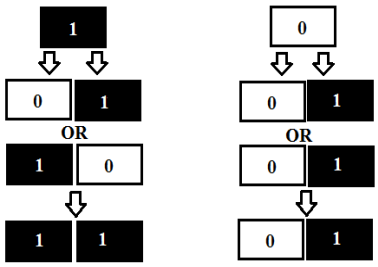
3. β, the contrast. The value β is to be as large as possible. The contrast β is computed using the equation:

$$\beta = \alpha.m \quad (3)$$

The minimum contrast that is required to ensure that the black and white areas will be distinguishable if $\beta \geq 1$.

Encryption of shares

In order to generate the shares in the *2-out-of*-2 scheme. Considering the following Fig. 1 we can generate the basis matrix



Basis Matrices Consruction.

The basis matrices are given as:

$$S_w = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } S_b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

In general if we have Y= {1, 2} as set of number of participants, then for a creating the basis matrices S_w and S_b we have to apply the odd and even cardinality concept of set theory. For $S_w$we will consider the even cardinality and we will get ES_w = {Θ, {1, 2}} and for S_b we have the odd cardinality OS_b = {{1}, {2}}. In order to encode the black and white pixels, we have collection matrices which are given as:

C_w = {Matrices obtained by performing permutation on the columns of $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$}

C_b = {Matrices obtained by performing permutation on the columns of $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ }

So finally we have,

$$C_w = \{ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \text{and} \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \}$$

$$C_b = \{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \}$$

Now to share a white pixel, randomly select one of the matrices in C_w, and to share a black pixel, randomly select one of the matrices in C_b. The first row of the chosen matrix is used for share S_1 and the second for share S_2.

Decryption of shares

Fig 2(a) Original image

Fig 2(b) Share 1

Fig 2(c) Share 2

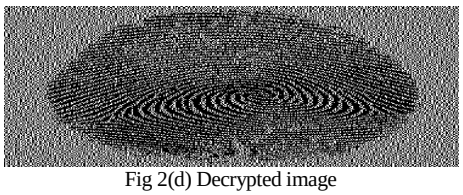


Fig 2(d) Decrypted image

VSS Scheme:

The Fig. 2 shows the stacking of the shares. Fig 2(a) shows the original image, Fig 2(b) and Fig 2(c) are the shares generated from the original image. Fig 2(d) shows the decrypted image after stacking the two shares. From the Fig 2(d) Decrypted Image.

III. STEGANOGRAPY USING VISUAL CRYPOGRAPHY

Generating covering shares using Halftoning

In order to deal with the gray-scale images, the halftoning technique was introduced into the visual secret sharing. The halftoning technique (or dithering technique) is used to convert the gray-scale image into the binary image. This technique has been extensively used in printing applications which has been proved to be very effective. Once we have the binary image, the SVSS can be applied directly.

The halftoning process is to map the gray-scale pixels from the original image into the patterns with certain percentage of black pixels. The halftoned image is a binary image. However, in order to store the binary images one needs a large amount of memory. A more efficient way is by using the dithering matrix. The dithering matrix is a integer matrix, denoted as *D*. The entries, denoted as $D_{i,j}$ of the dithering matrix are integers which stand for the gray-levels in the dithering matrix.We take n gray-scale original share images, denoted as $I_1, I_2, \ldots\ldots, I_n$, as the inputs, and output n binary meaningful shares $s_1, s_2, \ldots\ldots, s_n$, where the stacking results of the qualified shares are all black images, i.e., the information of the original share images are all covered.

International Journal of Computing Algorithm
Volume: 03, Issue: 01 June 2014, Pages: 97-100
ISSN: 2278-2397

Generating Embedding transparencies in to covering shares
Suppose the size of each covering share is *p*q*. We first divide each covering share into *(pq)/t* blocks with each block containing *t* subpixels, where *t>=m* . In case *pq* is not a multiple of *t*, then some simple padding can be applied. We choose *m* positions in each *t* subpixels to embed the m subpixels of *m*. In this project, we call the chosen m positions that are used to embed the secret information the embedding positions. In order to correctly decode the secret image only by stacking the shares, the embedding positions of all the covering shares should be the same. At this point, by stacking the embedded shares, the *(t-m*) subpixels that have not been embedded by secret subpixels are always black, and the *m* subpixels that are embedded by the secret subpixels recover the secret image as the corresponding VSS does. Hence the secret image appears.

IV. PROPOSED METHOD

Results

Fig3 (a) Original Image

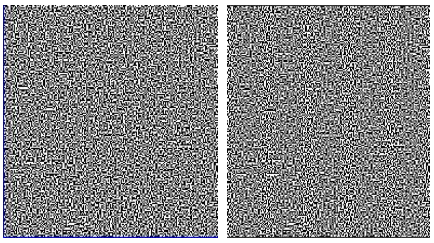


Fig3 (b) Encrypted Shares using VSS

Fig (c) Covering shares

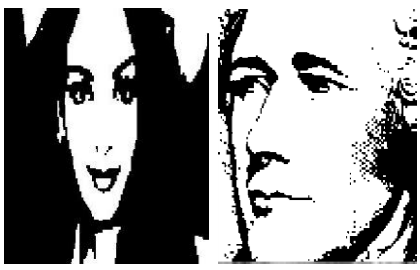


Fig (d) Shares (obtained from VSS) are embedded into the Covering images (Halftone Images)

Fig3 (e) Decrypted Image using SVSS

Streganography using VSS:

Analysis of the results
Original image, Fig 3(b) shows encrypted shares using VSS, Fig 3(c) shows meaning full images used as covering shares, Fig 3(d) shows haftoned Images of fig 3(c) which are embedded with Fig 3(b) and Fig 3(d) shows decrypted Image using.Meaningfull shares are trasmitted instead of dotted black and white shares in SVSS .

Compared to Fig.2 the shares and decrypted image size are same as original image size and XOR operation is used to recover the secret image instead of OR operation.

Algorithm of the Proposed Method Encryption

Load the image
Create M_0 ,M_1
for each pixel p in SI:
{
if (p is black)
r = a random permutation of the columns of M_1
else
r = a random permutation of the columns of M_0
for each participant i:
{
where pixels j if ($r_{i,j}$ = =1)
subpixel=black
else
subpixel= white. }
}

Generating covering shares
Dithering matrix D of size (c*d)
for i=0 to c-1 do&
for j=0 to d-1 do
if g<=Dij
then print black pixel at position(i,j)
else
print white pixel at position (i,j)

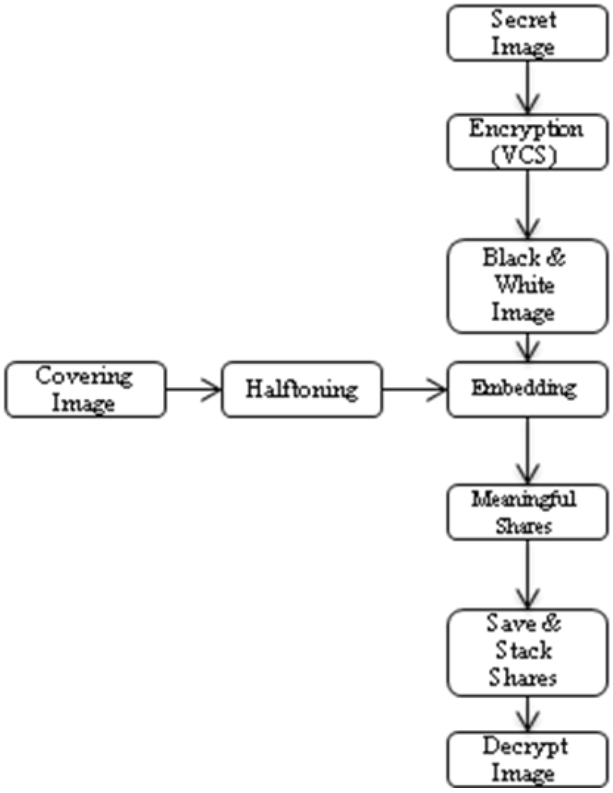
Embedding
Step 1: Divide the covering shares into blocks thatcontain t sub pixels each.
Step 2: Choose m embedding positions in each block in the n covering shares.
Step 3: For each black pixel in SI, randomly choose a share matrix $M_1 \varepsilon C_1$.
Step 4: For each white pixel in secret image, randomly choose another matrix $M_0 \varepsilon C_0$

International Journal of Computing Algorithm
Volume: 03, Issue: 01 June 2014, Pages: 97-100
ISSN: 2278-2397

Step 5: Embed the m sub pixels of each row of the share matrix M into the m embedding positions chosen in Step 2

Decryption
Load the Shares.
if (share file==Null)
print ("No file")
else if (Image==Null)
print ("Image not present")
else
{
Set the dimensions combine the shares
}

Architecture of the proposed method



Architecture of the proposed method

V. CONCLUSION

In this paper ,we presented a new approach where the input is the secret image to be shared and the output is *n* shares to be shared among *n* participants. These shares are random black and white patterns which reveal no information about the original secret image. Secret image is covered with *n* meaningful images and output are *n* covering shares. These shares are binary images.The shares (obtained from VSS) are embedded into the meaningful images to obtain covering shares. To get back the secret images at least *k-out-of-n*shares are stacked one upon the other.Construction of SVSS which was realized by embedding the random shares into the meaningful covering shares. The shares of the proposed scheme are meaningful images and the stacking of a qualified subset of shares will recover the secret image visually. SVSS technique can be used for secure iris authentication , face privacy,etc.

REFERENCES

[1] M.Naor & A.Shamir, "Visual secret sharing", Proc.Advances in Cryptology EUROCRYPT '94, LNCS, Springer-Verlag, pp.1-12,1995.
[2] Stinson, "Visual secret sharing and threshold schemes", Potentials, IEEE, Vol. 18 Issue: 1, pp. 13 -16, 1999.
[3] A B Rajendra & H S Sheshadri, "Enhanced visual secret sharing for graphical password authentication" Proc. SPIE 8768, International Conference on Graphic and Image Processing , 876835, doi:10.1117/12.2010934,2012.
[4] Rajendra Basavegowda & Sheshadri Seenappa, "Electronic Medical Report Security Using Visual Secret Sharing Scheme", Proc. of the IEEE International Conference on Computer Modelling and Simulation, Cambridge, UK, pp.78-83.2013.
[5] S.Droste, "New results on visual secret sharing" in Proc. CRYPTO'96, vol. 1109, pp. 401–415, Springer-Verlag Berlin LNCS.1996.
[6] G.Ateniese, C. Blundo, A. De Santis and D.R.Stinson,"Extended capabilities for visual secret sharing," ACM Theoretical Computer. Sci., vol. 250, no. 1–2, pp. 143–161, 2001.
[7] M. Nakajima and Y. Yamaguchi, "Extended visual secret sharing for natural images," in Proc. WSCG Conf.2002pp. 303–412, 2002.
[8] Rajendra A B, Sheshadri H S , "Visual Cryptography in Internet Voting System", Proc. of the IEEE International Conference on Innovative Computing Technology, London, UK, pp.60-64,2013.
[9] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.
[10] R A Basavegowda, S H Seenappa,"Secret Code Authentication Using Enhanced Visual Cryptography", Emerging Research in Electronics, Computer Science and Technology, LN EE248, Springer book chapter, pp 69-76.2014.
[11] Thomas Monoth, Babu Anto P (2010), "Tamperproof Transmission of Fingerprints Using VisualCryptography Schemes", Elsevier science direct, Procedia Computer Science 2, pp 143–148.
[12] Rajendra A B & Sheshadri H S , "A new approach to analyze visual secret sharing schemes for biometric authentication" International Journal in Foundations of Computer Science & Technology (IJFCST), Vol. 3,No.6, pp 53-60.November 2013