

Recursive Visual Secret Sharing for Biometric Authentication

A. B. Rajendra*

Department of Information Science & Engineering, Vidyavardhaka College of Engineering, Mysuru-570002, Karnataka, India; abrajendra@vvce.ac.in

Abstract

Visual Secret Sharing (VSS) or Visual Cryptography is a single level encryption used to share a secret image in the form of shares among group of users and the image decryption can be done by stacking the shares without the prior knowledge of encryption and with no cryptographic computations. In the Recursive Visual secret Sharing (RVSS), the original image is encrypted into first level, second level, third level shares and so on. For n levels $2n$ shares are generated. In this paper, a new method of Biometric authentication using 2-out-of-2VSS with two levels encryption is proposed, where the output of first level shares becomes the input to the second level shares generation. The security of the Biometric Image (BI) can be improved by increasing the levels of share generation (encryption) and decrypted image is obtained by stacking all level shares.

Keywords: Biometric Authentication, Recursive Visual Secret Sharing (RVSS), Visual Cryptography, Visual Secret Sharing

1. Introduction

The cryptography schemes are used for information security. If copy of encrypted secret information (Cipher) is destroyed, then it is difficult to recover it. Duplicating the secret information will lead intruders to access it. In order to handle information in a secure and reliable way the secret sharing schemes are used. An extension of secret sharing scheme is visual secret sharing¹. Visual Cryptography is a kind of secret image sharing scheme that uses the human eye to perform the decryption. Parakh and Kak^{2,3} proposed recursive threshold visual secret sharing and recursive hiding of secrets in Visual Secret Sharing in network application to reduce the network load. And VSS schemes are proposed for

contrast improvement and access structures⁴⁻⁷.

Biometric refers to identity verification of individuals based on their physical and behavioral characteristics. Physical biometrics (fingerprint, iris, retina, hand geometry, face, etc.) and behavioral biometrics (signature, keystrokes, voice, etc).

Thomas Monoth and Babu Anto P proposed a Tamperproof fingerprint authentication using VSS with single level Encryption^{8,9}.

This paper is organized as follows. Section II introduces the fundamental principles of VSS, based on which our method is proposed. Section III shows our proposed method for constructing the simplest 2-out-of-2RVSS scheme for fingerprint image authentication with two level encryption. Finally, conclusions are drawn in section IV.

* Author for correspondence

2. Visual Secret Sharing

Visual Secret Sharing (VSS) or Visual Cryptography (VC) is mainly used to secure the Secret Image (SI) among group of users, where the SI is encrypted into 'n' shares (dotted black and white images) which individually yield no information. SI comes out only when shares are stacked on one another.

The schemes present in VSS are k-out-of-n and n-out-of-n. In k-out-of-n scheme, by stacking any k ($k \leq n$) of these shares, the original SI can be recovered, but stacking less than k of them will not disclose any information about the SI. In n-out-of-n scheme all n shares have to be stacked to get the SI. The contrast, security and size are the main significant parameters in VSS. The proposed design uses XNOR operation for perfect biometric decryption, multilevel (Recursive) encryption for the biometric security and random basis column selection to encode a binary fingerprint Image into the shares without pixel expansion.

2.1 Basic Model

Considering the image, it will consist of a collection of m black and white pixels; each pixel appears in n shares or transparency. The overall structure of the scheme can be described by an $n \times m$ (No. of shares \times No. of pixels) Boolean basis matrix $B = [B_{ij}]$,

Where,

$B_{ij} = 1$, if and only if the j^{th} sub pixel in the i^{th} share is black.

$B_{ij} = 0$, if and only if the j^{th} sub pixel in the i^{th} share is white.

White basis matrix B_w and black basis matrix B_b should satisfy the following rules holds:

- If set $S = \{i_1, i_2, \dots, i_n\} \in Q$, then OR operation of shares i_1, i_2, \dots, i_n of B_w satisfies the Hamming weight $H(V) \leq k - \alpha.m$, whereas, for B_b satisfies $H(V) \geq k$.

Where Q is qualified set, α is relative Contrast and k is threshold value.

- If $S = \{i_1, i_2, \dots, i_n\} \in F$, then the two $n \times m$ matrices obtained by restricting B_w and B_b to shares i_1, i_2, \dots, i_n are identical up to a column permutation.

The first rule is for contrast and the second rule is for security. The collections C_w and C_b are found by permuting the columns of the basis matrices B_w and B_b in all possible ways.

2.2 Encryption

The Biometric image (BI) is encrypted into exactly two shares and both have to be stacked to get back the BI. Figure 1 represents the division of black and white pixel in this scheme. Encryption process in the 2-out-of-2 VSS scheme with 2 pixel layout using two basis matrices B_w and B_b realization is as shown in Table 1.

An original black pixel is converted into two pixels for two shares, shown in 1st row. After stacking the two shares we will get a perfect black. Similarly we have other combination for two pixels generated shown in 2nd row.

For original white pixel also we have two pixels for each of the two shares, but after stacking the shares we will not get exact white. We have a combination of black and white pixels. This results in the loss of the contrast. Considering the following Figure 1 we can generate the basis matrix:

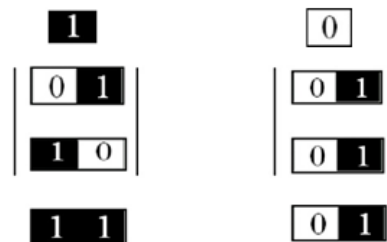


















Figure 1. Basis matrices construction.

Table 1. A 2-out-of-2 VSS Scheme

Pixel color	Original pixel	Encryption		Decryption
		Share 1	Share 2	Share1+Share2
Black				
Black				
White				
White				

The matrix B_w is for encoding white pixels and B_b is for encoding black pixels. The matrices B_w and B_b can be represented as follows:

$$B_w = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \& B_b = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

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

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

So finally,

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

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

Now to share a white pixel, it selects randomly one of the matrices in C_w . To share a black pixel, it selects randomly one of the matrices in C_b . The first row of the chosen matrix is used for share S_A and the second for share S_B . The Figure 2 shows decryption of 2-out-of-2 VSS Scheme for regular size using random basis pixel expansion scheme.

2.3 Decryption in 2 out of 2 VSS Scheme

The Figure 2 shows decryption of 2-out-of-2 VSS

Scheme. Figure 2a shows the biometric image, Figure 2b and 2c are the shares generated from the biometric image using single level encryption. Figure 2d shows the decrypted image after stacking the two shares.

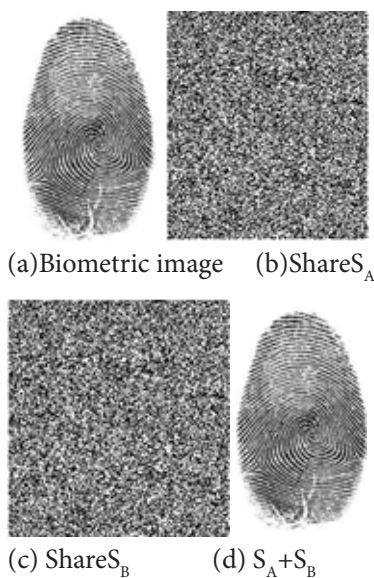


Figure 2. Basis matrices construction.

3. Proposed Method

In the proposed scheme, the Biometric image (BI) is encoded into two first level shares. The each of the two first level shares is further encoded into two second level shares in repetitive manner and so on.

$BI = \{ SA, SB \}$ $SA = \{ SA1, SA2 \}$ & $S_B = \{ SB1, SB2 \}$.
 Where S_A, S_B are the two first level shares generated by Biometric image (BI). Further S_A is encoded into two second level shares S_{A1}, S_{A2} and S_B is encoded into two second level shares S_{B1}, S_{B2} respectively, The proposed model is also represented by using Tree representation (Figure 3).

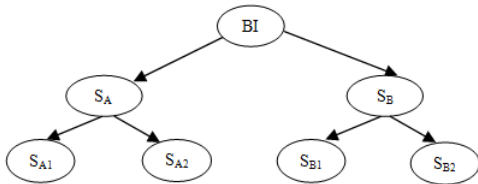


Figure 3. Tree representation of RVSS.

The number of level of encryption used depends on the security and reliability requirements. Increasing the level of encryption will increase the level of security and reliability of the biometric image.

On the decryption process, there are different ways to reconstruct the SI. That is:

$BI = S_A + S_B$
 $BI = S_{A1} + S_{A2} + S_{B1} + S_{B2}$
 Mathematically $k \geq 1$, where k is the level of encryption required.
 If $k = 1$, then $BI = S_A + S_B$
 If $k = 2$, then $BI = S_{A1} + S_{A2} + S_{B1} + S_{B2}$

3.1 The Experimental Results

The proposed scheme is practicable; experiments done using 2-out-of-2VSS with two level of encryptions (i.e. $k= 2$). In the second level of encryption, the shares, S_A & S_B are further encoded into two shares each. That is, S_A is encoded in to S_{A1} and S_{A2} , S_B is encoded in to S_{B1} and S_{B2} respectively. The experimental results are shown in Figure 4.

4. Conclusion

This paper proposes a new method for security using Recursive Visual Secret Sharing mechanism. The experiments were conducted for 2-out-of-

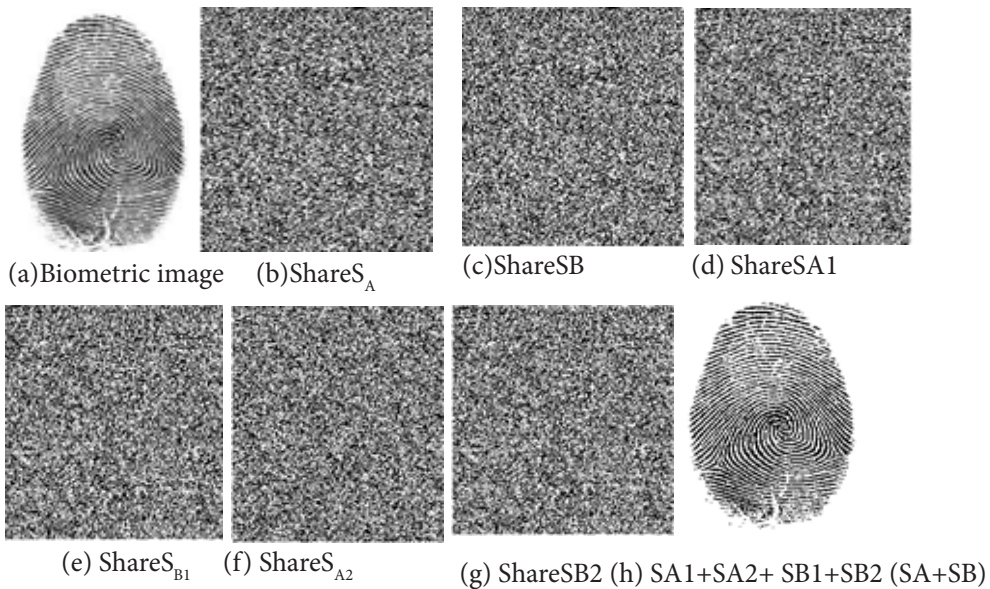


Figure 4. A 2-out-of-2 RVSS Scheme (Two level Encryption)

2RVSS with 2-subpixel layout using random basis column pixel selection. The multilevel encryption is performed for fingerprint image and in decryption the shares are stacked using XNOR operation.

This experiment can be extended to k -out-of- n VSS. The scheme is secure and easy to implement. The major advantage of this method is that the fingerprint reconstruction process could not require any complex algorithm and computations. The proposed method is less complex and fast compared to other cryptosystems.

5. References

1. Naor M, Shamir A. Visual Cryptography. EUROCRYPT. 1994. 950:1–12.
2. Gnanaguruparan M, Kak S. Recursive hiding of secrets in visual cryptography. *Cryptologia*. 2002; 26:68–76.
3. Parakh A, Kak S. A recursive threshold visual cryptography scheme. *Cryptology ePrint Archive*. 2008; 535.
4. Ateniese G, Blundo C, Santis AD, Stinson D. Constructions and bounds for visual cryptography. LNCS. 1996; 1099:416–28.
5. Naor M, Shamir A. Visual Cryptography II: Improving the Contrast Via the Cover Base. *Security in Communication Networks*. 1996; 197–202.
6. Wang D, Yia F, Li X. On general construction for extended visual cryptography schemes. *J Pattern Recognition*. 2009; 42:3071–82.
7. Droste S. New results on visual cryptography. *CRYPTO*. 1996; 1109:401–15.
8. Monoth T, Anto BP. Tamperproof Transmission of Fingerprints Using Visual Cryptography Schemes. Elsevier science direct, *Procedia Computer Science*. 2010; 2:143–8.
9. Rajendra AB, Sheshadri HS. A new approach to analyze visual secret sharing schemes for biometric authentication. *International Journal in Foundations of Computer Science & Technology*. 2013; 3(6):53–60.