A NEW APPROACH TO ANALYZE VISUAL SECRET SHARING SCHEMES FOR BIOMETRIC AUTHENTICATION-A SURVEY

Rajendra A B[1] and Sheshadri H S[2]

[1]Research student, PET Research Centre, E & C Department, Mandya, Karnataka, India,
[2] Professor and Dean (PET Research) PES College of Engineering, Mandya, Karnataka, India

ABSTRACT

Secret sharing schemes are the methods for sharing secret data over a class of users. Shares are randomly distributed to all users of the secret data. The secret data can be obtained only when all the shares are joined together. Visual cryptography (VC) or Visual Secret sharing Scheme (VSSS) is one such method which implements secret sharing for images. Biometric characteristics provide a unique natural signature of a person and it is widely accepted. Each biometric technique has its advantages and disadvantages VSSS and biometrics have been identified as the two most important aspects of digital security. Based on this study, a new method to analyze VSSS for biometric authentication is given in this paper.

KEYWORDS

Secret sharing scheme, Visual Cryptography (VC), Visual Secret Sharing Scheme (VSSS), Biometrics.

1. INTRODUCTION

Sensitive, individual, private information is being deposited and communicated using networks every day and new threats and computer crimes are also increasing. Duplicating important information will leads intruders to access it. On the other hand, having only one copy of this information means that if this copy is destroyed there is no way to retrieve it. Thus, there is a great need to handle information in a secure and reliable way. The idea of sharing a secret was invented by Adi Shamir in 1979[1].

Secret information needs to be kept by a set of participants in such a way that only a qualified set is able to reconstruct the secret. 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 needs for secret sharing arise if the storage system is not reliable and secure [2]. Secret sharing is also useful if the owner of the secret does not trust any single person. This concept was first applied to numbers, but in the 1994 researchers extended this concept to images. Visual cryptography (VC) or Visual Secret sharing Scheme (VSSS) is one such method which implements secret sharing for images [3].

The biometrics technology brings a new dimension to individual identity verification. .For Biometrics, if it makes use of VSSS it will provide more security. This paper is organized as follows. Section II introduces fundamentals of VSSS. Section III introduces the biometrics.

Section IV shows the architecture of the proposed VSSS for biometric authentication .Finally, conclusions are drawn in section V.

2. VISUAL SECRET SHARING SCHEMES

VSSS proposed by Naor and Shamir in 1994, is one of the cryptographic methods to share secret images. The VSSS describes the way in which an image is encrypted and decrypted. There are different types of VSSS.For example, there is the k-out-of-n scheme that says n shares will have to be produced to encrypt an image, and k shares must be stacked to decrypt the image [4]. 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 VSSS. 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. In this section; 2-out of-2 scheme for black and white Image is analyzed with its model, generation of shares and staking of shares.

3.1. The model

In visual Cryptography (VC), we have various schemes like k-out of-n, 2-out of-n & n-out of-n VSSS. Let $Y = \{1, 2 \ldots n\}$ be a set of participants and let 2^Y denote the collection of all subsets of Y.

- Let Qualified set $Q \subseteq 2^Y$ and Forbidden set $F \subseteq 2^Y$, where $Q \cap F = \theta$ (null set).
- The access structure of the scheme is pair(Q,F).
- Define M which consist of all minimal qualified sets:

$$M = \{A \in Q: A` \notin Q \text{ for all } A` \subset A\}$$

The existing model for black-and-white visual cryptography schemes has been developed by Naor and Shamir. In this model, both the original secret image and the share images contain only black and white pixels. Each pixel in the original image is subdivided into a set of m black and white subpixels in each of the n share images.

The set of subpixels can be represented by an n x m Boolean matrix $S = [S_{ij}]$, where

$S_{ij} = 1 \Leftrightarrow$ the j^{th} subpixel in the i^{th} share is black (S_b)
$S_{ij} = 0 \Leftrightarrow$ the j^{th}sub pixel in the i^{th} share is white ($S_{w)}$

To distinguish between black and white pixels in the recovered image, we define a fixed threshold parameter d, where $1 \leq d \leq m$. If $H(V) \geq d$, then the subpixels are interpreted as black, and if $H(V) \leq d - \alpha .m$,then the subpixels are interpreted as white, where H(V) is the Hamming weight (the number of one's) of the 'or' ed m-vector V. Where d is the threshold parameter for the point at which black areas are distinct from white. The 'm' denotes the pixel expansion. This represents the loss of resolution from the original image to the share image, which is to be as small as possible. The parameter $\alpha > 0$ is called the relative contrast difference of the scheme. It is desirable to have a relative contrast difference as large as possible to minimize the loss of contrast in the recovered image. The value $\alpha.m$ is the contrast, which is greater than or equal to 1 and

hence ensures that the black and white areas will be distinguishable [5]. The formal definition for black-and-white visual cryptography schemes by Naor and Shamir is:

Definition 1.2: A solution to the k-out of-n visual cryptography scheme consists of two collections of n x m Boolean matrices C_w and C_b.To share a white pixel, the dealer randomly chooses one of the matrices in C_w and to share a black pixel, the dealer randomly chooses one of the matrices in C_b. The chosen matrix defines the color of the m subpixels in each one of the n transparencies.

The solution is considered valid if the following three conditions are fulfilled:

1. For any $S \in C_w$, the OR m-vector V of any k of the n rows in S satisfies $H(V) \leq d - \alpha .m$.

2. For any $S \in C_b$, the OR m-vector V of any k of the n rows in S satisfies $H(V) \geq d$.

3. For any subset $\{r_1, r_2 \ldots r_t\} \subset \{1,2,\ldots,n\}$ with $t < k$, the two collections of t x m matrices obtained by restricting each n x m matrices in C_w and C_b to rows $r_1, r_2 \ldots r_t$, are Indistinguishable in the sense that they contain the same matrices with the same frequencies.

For a visual cryptography scheme to be valid, these three conditions must be satisfied. The first two conditions ensure that some contrast in the scheme is maintained, and the third condition ensures that security in the scheme is maintained. The third condition states that no information can be obtained if less than k shares are stacked together.

To encrypt a white pixel of the original image, a matrix is randomly chosen from C_w and is used to create the shares. A black pixel is encrypted by randomly choosing a matrix from C_b. At least two matrices in each collection are needed so that the dealer can randomly choose one of them. If the matrix is chosen randomly, a cryptanalyst, examining less than k shares, will not be able to predict the color of the pixel in the original secret image based on the pixel positions, since each matrix in the collection is equally likely to have been chosen [6].

The important parameters of the existing system are:

• **m**, the number of subpixel in a share. The m should be as small as possible. The m is computed using the equation:

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

• **α**, the relative difference. This represents the loss in contrast. The α should be as large as possible. The relative difference α is given by

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

Where, n_b and n_w are the number of the black subpixels which are generated from black and white pixels from the original image, respectively.

• **β**, the contrast. The value β is to be as large as possible. The minimum contrast that is required to ensure that the black and white areas will be distinguishable is $\beta \geq 1$. The contrast β is given by

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

3.2 Generation of shares

In order to generate the shares in the 2-out-of-2 scheme we have the following mechanism:

Table 1. Pixel Pattern For 2-out-of-2 VC Scheme

Pixel colour	Original pixel	Share1	Share2	Decrypted pixels= Share1+ Share2
Black	■	■□	□■	■■
Black	■	□■	■□	■■
White	□	■□	■□	■□
White	□	□■	□■	□■

An original black pixel is converted into two sub-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 sub-pixels generated shown in 2nd row. For original white pixel also we have two sub-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 sub-pixels. This results in the loss of the contrast. Considering the following Fig. 1 we can generate the basis matrix:

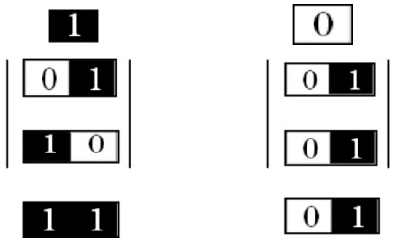


Fig. 1. Basis Matrices Construction.

The basis matrices are given as:

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

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

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 $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ }

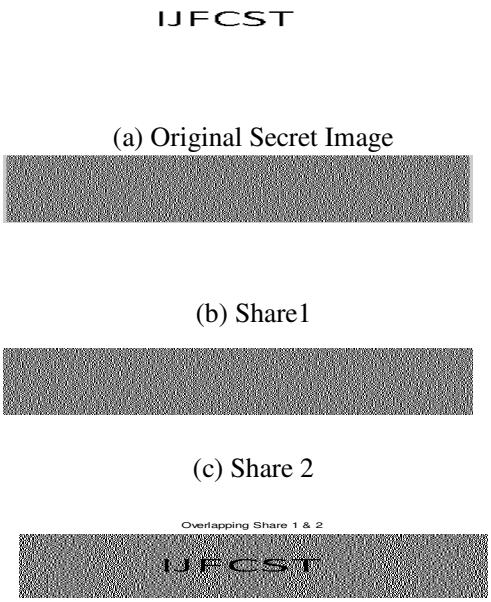
So finally we have,

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

$C_b = \{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ 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 1 and the second for share 2.

3.3 Stacking of shares



(a) Original Secret Image

(b) Share1

(c) Share 2

(d) Retrieved Image (share1 +share2)

Fig.2. 2-out of -2 VC with 2 sub pixel layout

The Fig.2 shows 2-out of -2 VSSS with 2 sub pixel layout. Where original secret image(Fig.2a), which is encoded in to two shares: share 1(Fig.2b) and share 2 (Fig.2c).The Fig. 2d is the result of laying share 1 over share 2 in the '2 out of 2' VSSS scheme.

Table 2.Comparison for major VSSS

	Scheme	**Contrast**	**Security**	**Applications**
Moni Noar & Adi Shamir[3]	2 out of 2 scheme 2 out of n scheme k out of n scheme	Clarity of the decrypted image is poor	No information can be revealed from any of the share alone	Encryption of writing material(picture, text etc)

A Avishek & Bimol Roy[4]	2 out of n scheme	Smaller pixel expansion for contrast improving	No information can be revealed from any of the share alone	Less memory space required to implement this scheme in a computer
Thomas M & B Anto P [5]	2 out of 2 Scheme 2 out of n Scheme K out of n scheme	Additional Basis Matrix(ABM) is used for contrast improvement	Recursive and hybrid Approach for information security	Secure transmission of fingerprint Images and Tamperproof preparation and transmission of online question papers
FengLiu & Chuankun [6]	2 out of 2 scheme	Reduces the noise in the cover images	A secret image is hidden into two meaningful cover images.	This scheme achieves lossless recovery without adding any computational complexity

4. BIOMETRIC TECHNIQUES

Biometric characteristics provide a unique natural signature of a person and it is widely accepted. Each biometric technique has its advantages and disadvantages [7]. No single biometric can meet the entire requirement (e.g. accuracy, cost, practicality, etc.)[8].A brief comparison of biometric techniques based on different factors is provided in Table 3. [10].

Biometrics can operate in one of two modes: the identification mode, in which the identity of an unknown user is determined, and the verification mode, in which a claimed identity is either accepted or rejected. Using biometric characteristics in cryptography has significant advantages over traditional cryptographic methods in the case of authentication. As an example, biometric characteristics of an individual are difficult to lose, steal or forge. However, biometric systems are vulnerable to attacks and break-ins by hackers. To address this issue, some methods are suggested by researchers to provide the security, accuracy and integrity of biometric templates in a biometric authentication system.

Table 3. Comparison of various biometric technologies

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Medium	Low	Low	Medium	Low	High	Low
F. Thermo-grams	High	High	Low	High	Medium	High	High

Although our approach is presented for biometric authentication security using for black and white visual cryptography. Using gray scale and natural images such as the face and iris, and also using more biometric samples with meaningful shares in an authentication security system can be considered as a future work in this area[14].

5. ARCHITECTURE OF THE PROPOSED SYSTEM

The systems of our application have following objectives.

- **Encryption:** Splitting the secret image into shares (cipher texts) using selected VSSS or EVC (Enhanced visual Cryptography).
- **Transmission:** Transmission of shares through different Channels.
- **Decryption:** Stacking the shares to get the secret image (Plaintext).
- **Authentication**: Checking the authenticity of authorized participant.

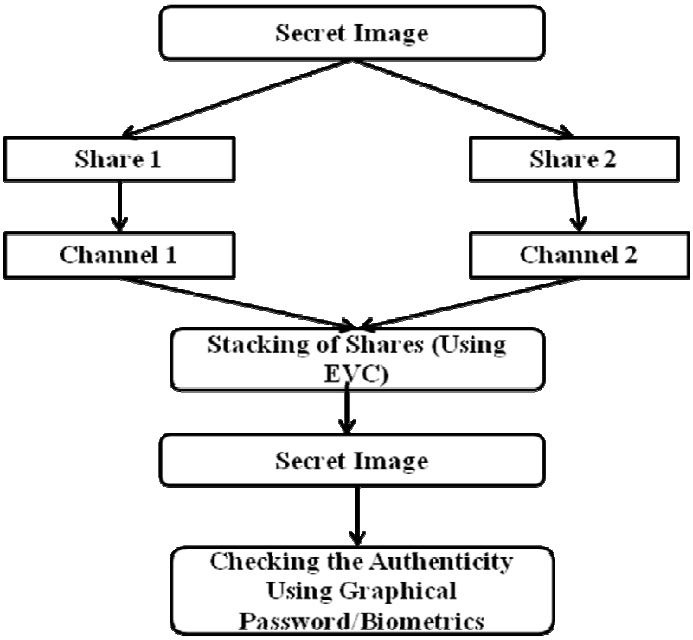


Fig.3 .Architecture of the proposed system

6. CONCLUSION

Even though considerable advancement has been made in security enhancement of Visual Cryptography & biometrics over the past decade, the methods have their own drawbacks. By using the Visual Cryptography for biometric authentication technique avoids data theft.

This is an overview about the application of secret sharing scheme .The method suggested is widely applicable for information sharing and is more secured .Also it cover the intelligent information management which is now being used in telemedicine.

REFERENCES

[1] Adi Shamir (1979) "How to share a Secret", Communications of the ACM, pp 612-613.
[2] Marek R. Ogiela, Urszula Ogiela (2009), "Linguistic Cryptographic Threshold Schemes", International Journal of Future Generation Communication and Networking.Vol.2, No.1, March 2009.pp 33-40.
[3] M. Naor and A. Shamir (1995) "Visual Cryptography", Advances in Cryptology-Euro crypt '94 Proceeding, LNCS vol. 950, Springer-Verlag, pp. 1-12.

[4] Adhikari Avishek and Bimol Roy (2007). "Applications of Partially Balanced Incomplete Block Designs in Developing (2, n) Visual Cryptographic Schemes". IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences Vol.E90-A No.5 pp.949-951

[5] Thomas Monoth, Babu Anto P (2009), "Achieving optimal Contrast in Visual Cryptography schemes without pixel expansion". International Journal of Recent Trends in Engineering, Vol 1, No 1, May 2009, pp.468-471.

[6] A B Rajendra & H S Sheshadri (2013), "Enhanced visual secret sharing for graphical password authentication" Proc. SPIE 8768, International Conference on Graphic and Image Processing (ICGIP 2012), 876835, doi:10.1117/12.2010934

[7] Seifedine Kadry,Aziz Barbar, (2009) "Design of Secure Mobile Communication using Fingerprint", European Journal of Scientific Research.Vol 30,No.1,pp.138-145

[8] Thomas Monoth, Babu Anto P (2010), "Tamperproof Transmission of Fingerprints Using Visual Cryptography Schemes", Elsevier science direct, Procedia Computer Science 2, pp 143–148.

[9] Rajendra Basavegowda & Sheshadri Seenappa (2013)," 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.

[10] N.Radha and S.Karthikeyan (2010), "A study on biometric template security", ICTACT journal of soft computing, Issue 01, pp. 37-41.

[11] Sudheesh K.V. Chandrasekhar M Patil(2012), "An Approach of Cryptographic Algorithm for Estimating the Impact of Fingerprint for Biometric", IEEE, pp 167-171, 2012

[12] Thomas Monoth & Babu Anto P (2007), "Recursive Visual Cryptography Using Random Basis Column Pixel Expansion", Proc. of the IEEE International Conference on Information Technology (ICIT '07), pp. 41-43.

[13] Nazanin Askari, Cecilia Moloney, Howard M. Heys, "Application of Visual Cryptography to Biometric Authentication".

[14] Sonali Patil, Kapil Tajane, Janhavi Sirdeshpande (2013), "Secret Sharing Schemes for Secure biometric authentication", International Journal of a scientific & Engineering, Volume 4, Issue 6, pp. 2890- 2895.

[15] Rajendra Ajjipura Basavegowda & Sheshadri Holalu Seenappa (2013),"Secret Code Authentication Using Enhanced Visual Cryptography",ICERECT -12,volume 248,pp 69-76.

Authors

Rajendra A B Studied BE in E&C (Kuvempu University), M.Tech in Computer Network Engineering (VTU, Belgaum). He has 13 years of teaching experience at VVCE since 2000 and actively perusing PhD course in the area of Visual Cryptography under the guidance of Dr.H S Sheshadri.He is a life member of IE (India), IETE, ISTE, CRSI. Attended in various national and International conferences and has presented papers in various international conferences in India and abroad. Visited countries UK and Singapore.

Dr. H.S. Sheshadri Obtained his B.E. from University of Mysore during 1979 in E& C Engg, M.E (Applied Electronics) from Bharathiar University, Coimbatore during 1989 and Ph.D from Anna University Madras during 2008.He is serving this institution since 1982 and presently he is a professor in the Dept of Electronics &Communication Engg. His field of interest is Medical Image processing and embedded systems. He has published 12 papers in national journals and 21 papers in International journals. Also guiding 6 research candidates for Ph.D programme under university of Mysore, Two candidates under VTU, Belgaum. Has conducted several short term courses and conferences and actively participate in the student and staff activities at the college.

He is a life member of IE (India), IETE, ISTE, SSI, and has participated in various national and international conferences and seminars in India and abroad.