Secret Code Authentication Using Enhanced Visual Cryptography

Rajendra Ajjipura Basavegowda and Sheshadri Holalu Seenappa

Abstract Secret code (password) is widely used in many applications like data transfer, sharing data, and login to emails or internet banking. So a big necessity to have a strong authentication to secure all our applications is as possible. In this paper, we present a new approach to authenticate password using Enhanced visual cryptography (EVC). Visual cryptography is a secret sharing scheme in which an image is converted into shares. No information can be revealed by observing any share. The information about the original image will be obtained on after stacking sufficient number of shares. We have a new approach to authentication secret code using our 2-out-of-2 EVC which provides efficient authentication for e-banking and other internet application.

Keywords Authentication · Enhanced visual cryptography (EVC) · Secret code (password) · Shares · Visual secret sharing scheme

1 Introduction

A password is a form of secret authentication of code that is used to controlled access to a resource. The password is kept secret, from those not allowed to access, and those wishing to gain access are tested on whether or not they know the password and are granted or denied access accordingly. To overcome the vulnerabilities of traditional methods, graphical password schemes have been developed for more authentications. Using EVC, we are providing security to

R. Ajjipura Basavegowda (✉) · S. Holalu Seenappa
PET Research Centre, PES College of Engineering, Mandya, Karnataka, India
e-mail: rajendraab@hotmail.com

S. Holalu Seenappa
e-mail: hssheshadri@hotmail.com

V. Sridhar et al. (eds.), *Emerging Research in Electronics, Computer Science and Technology*, Lecture Notes in Electrical Engineering 248,
DOI: 10.1007/978-81-322-1157-0_8,

secret code. Visual cryptography (VC) scheme uses permutation techniques to encode secure code. The idea is to convert the secret code into n shadow images (shares). The decoding only requires selecting some subsets of these n shares, making transparencies of them, and stacking them on top of each other [1, 2]. This paper is organized as follows. Section 2 shows the fundamental principles of 2-out-of-2 VC scheme. Section 3 shows the proposed method to improve the contrast and an approach to secure the secret code. Finally, conclusions are drawn in Sect. 4.

2 Visual Cryptography

VC is a model in which the decryption of the secret image is done by using human visual system without any computational complexity. There are two types of VC schemes: n-out-of-n and k-out-of-n VC schemes [3]. In n-out-of-n VC scheme, image is divided into n shares, and in order to decrypt the image, all n shares are stacked on each other. In k-out-of-n scheme, the shares generated from the image are Xeroxed onto n transparencies and distributed among participants, one for each participant. Any k or more participants can visually reveal the secret image by superimposing any k transparencies together. The secret cannot be decoded by any $k - 1$ or fewer participants, even if infinite computational power is available to them [1], [4]. Following n-out-of-n scheme, we have used 2-out-of-2 scheme. In 2-out-of-2 VC scheme, a secret image is encrypted into two shares such that each share has random binary pattern of pixels. In order to decrypt the image, the two shares need to be overlaid [5].

2.1 Basic Model

Consider a set $Y = \{1, 2 \ldots n\}$ be a set of elements called participants. By applying set theory concept, we have 2^Y as the collection of all subsets of Y. Let $\Gamma_Q \subseteq 2^Y$ and $\Gamma_F \subseteq 2^Y$, $\Gamma_Q \cap \Gamma_F = \theta$ and $\Gamma_Q \, U \, \Gamma_F = 2^Y$, members of Γ_Q are called qualified sets and members of Γ_F are called forbidden sets [4]. The pair (Γ_Q, Γ_F) is called the access structure of the scheme. Γm can be defined as all minimal qualified sets: $\Gamma m = \{A \in \Gamma_Q : A| \notin \Gamma_Q \text{ for all } A| \subset A\}$.

Γ_Q can be considered as the closure of Γ_m, and Γ_m is termed a basis, from which a strong access structure can be derived [1]. 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 subpixels. The overall structure of the scheme can be described by an n x m (No. of shares $\times$ No. of subpixels) Boolean matrix $S = [S_{ij}]$, where

$S_{ij} = 1$, if and only if the jth subpixel in the ith share is black.
$S_{ij} = 0$, if and only if the jth subpixel in the ith share is white.

Following the above terminology, let (Γ_Q, Γ_F) be an access structures on a set of n participants. A $(\Gamma_Q, \Gamma_F, \alpha)$-VCS with the relative difference α and set of thresholds $1 \leq k \leq m$ is realized using the two $n \times m$ basis matrices S_w and S_b, if the following condition holds:

1. If $Y = \{i_1, i_2, \ldots i_p\}$ Γ_Q, then the "or" V of rows $i_1, i_2, \ldots i_p$ of S_w satisfies $H(V) \leq k - \alpha \cdot m$, whereas, for S_b, it results that $H(V) \geq k$.
2. If $Y = \{i_1, i_2, \ldots i_p\}$ Γ_F, then the two $p \times m$ matrices obtained by restricting S_w and S_b to rows $i_1, i_2, \ldots i_p$ are identical up to a column permutation [6, 7].

The first condition is called contrast and the second condition is called security. The 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 [8, 9]. The important parameters of the scheme are as follows:

- m, the number of subpixels in a share. This represents the loss in resolution from the original image to the shared one. The m is computed using the equation:

$$m = 2^{n-1} \tag{1}$$

- α, the relative difference. It determines how well the original image is recognizable. This represents the loss in contrast. The α is to be as large as possible and is calculated using the equation:

$$\alpha = |n_b - n_w|/m \tag{2}$$

where n_b and n_w represent the number of black subpixels generated from the black and white pixels in the original image.

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

$$\beta = \alpha \cdot \mathrm{m} \tag{3}$$

The minimum contrast that is required to ensure that the black and white areas will be distinguishable if $\beta \geq 1$ [3].

2.2 Generation of Shares

In order to generate the shares in the 2-out-of-2 scheme, we have the following mechanism (Table 1).

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

Table 1 Pixel pattern for 2-out-of-2 VC scheme

Pixel color	Original Pixel	Share1	Share2	Share1+ Share2
Black	■	■□	□■	■■
Black	■	□■	■□	■■
White	□	■□	■□	■□
White	□	□■	□■	□■

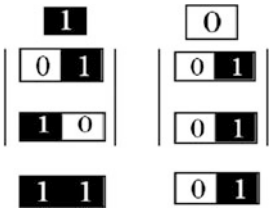

Fig. 1 Basis matrices construction

original white pixel, also we have two subpixels 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 subpixels. This results in the loss of the contrast. Considering the following Fig. 1, we can generate the basis matrix:

The basis matrices for white and black pixels 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 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 $S_w = \{\Theta, \{1, 2\}\}$ 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 $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}\}$

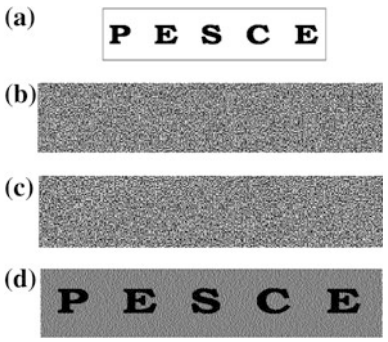

Fig. 2 Visual cryptography scheme. **a** Original image. **b** Share 1. **c** Share 2. **d** Decrypted image

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

So finally, we have,

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

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

Now, to share a white pixel, 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.

2.3 Stacking of Shares

The Fig. 2 shows the stacking of the shares. Figure 2a shows the original image, and Fig. 2b, c are the shares generated from the original image. Figure 2d shows the decrypted image after stacking the two shares. From the Fig. 2d, it can be observed that contrast in the decrypted image is less. In order to improve the contrast, an analysis on the relative contrast value is required.

3 Experimental Results and Discussion

3.1 Proposed Method

Based on the analysis on the relative contrast, we have the following observation:

Table 2 Relative contrast value v/s number of subpixels

Shares n	Subpixels $m = 2^{n-1}$	Relative contrast (α)	Contrast $\beta = \alpha \cdot m$
2	2	0.50	1
3	4	0.25	1
4	8	0.125	1
5	16	0.0625	1
6	32	0.03125	1

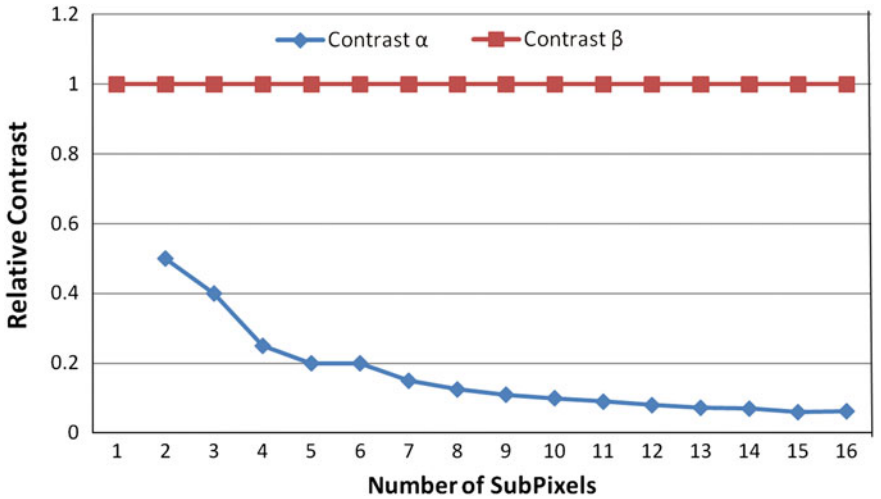

Fig. 3 Relative contrast versus number of subpixels

From the Table 2, we can see that the relative contrast value decreases as the number of subpixels increases. The following Fig. 3 depicts the same.

So considering the same 2-out-of-2 EVC in order to increase the relative contrast value, we have used an additional matrix along with the basis matrices. The additional matrix is used to share the white pixels in the reconstructed secret image. The additional matrix can be formed in the following manner:

Let Y be the set which is given by

$Y = \{i_1, i_2 \ldots i_n\}$ of n elements.
We define an additional matrix AS_w with order n × m such that
$AS_w = [AS_{ij}]$ where
$AS_w = 0$ if and only if $1 \leq i \leq n$ and $j = 1, 2$.

The collection matrices will be obtained in the following manner:

$$C_w = \{\text{Basis Matrix} \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} + \text{Additional Matrix} \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\}$$

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

Now the value of α will be equal to 3/4. This result shows that the relative difference of proposed method is better compare to the existing one.

3.2 Stacking of the Shares

The Fig. 4 shows the stacking of the shares. Figure 4a shows the original image, and Fig. 4b, c are the shares generated from the original image. Figure 4d shows the decrypted image with better contrast. With this better contrast, we can apply our approach in various fields for achieving the security objectives.

In the Fig. 5, the visual secret sharing application will take this secure code and splits the secure code into shares. Our proposed method uses 2-out-2 EVC which improves the contrast. So that after decryption, the image is clearly visible. The shares will be generated which will be in encrypted form. The shares transmitted in different channels in secured way. Authorized persons will receive the shares from different channels, and then, shares are overlaid to get the secret code.

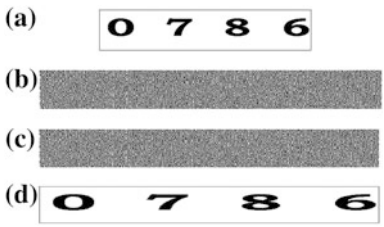

Fig. 4 Enhanced visual cryptography scheme

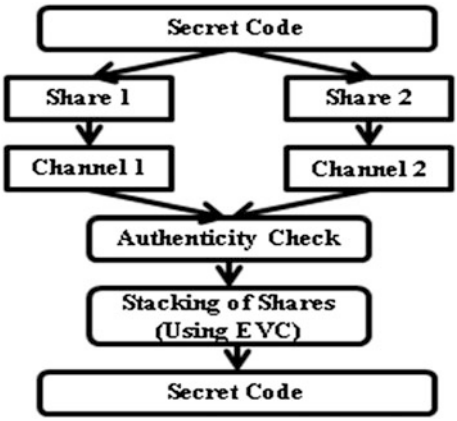

Fig. 5 Software architecture of the proposed method

4 Conclusion

In this paper, a new approach is proposed to transmit secret code. The secret code is divided into two shares using 2-out-of-2 EVC, and it is sent in different channels. Where the contrast of the stacked share (decrypted secret code) is comparatively better than earlier methods, it provides security to devices, to share secret data among the group and split shares in different channels to protect from hackers. This application can also be used for sending secret codes to a customer of the e-banking and in similar highly secured applications.

This is a part of our approach to certain modifications in the methods of encrypting medical data in an image for secured telemedicine. Further the research work is going on graphical password with visual cryptography.

Acknowledgments I thank my guide Dr. H S Sheshadri, professor and dean (research) for supporting to carry out this work.

References

1. Shamir A (1979) How to share a secret. Comm ACM 22(11):612–613
2. Naor M, Shamir A (1995) Visual cryptography. In: Proceedings of advances in cryptology EUROCRYPT' 94, LNCS, Springer, pp 1–12
3. Monoth T, Babu Anto P (2009) Achieving optimal contrast in visual cryptography schemes without pixel expansion. Int J Recent Trends Eng 1(1)
4. Ogiela MR, Ogiela U (2009) Linguistic cryptographic threshold schemes. Int J Future Gener Comm Network 2(1):33–40
5. Rajendra AB, Sheshadri HS (2012) A study on visual secret sharing schemes using biometric authentication techniques. AJCST 1:157–160
6. Manimurugan S, Porkumaran K (2011) A new fast and efficient visual cryptography scheme for medical images with forgery detection. In: Proceedings of IEEE international conference on emerging trends in electrical and computer technology (ICETECT) 2011, pp 594–599
7. Blundo C, University of Salerno, De Santis A, Stinson DR, University of Nebraska-Lincon (1996) On the contrast in visual cryptography scheme
8. Radha N, Karthikeyan S (2010) A study on biometric template security. ICTACT J Soft Comput 01
9. Stinson D (1999) Visual cryptography and threshold schemes. IEEE Potentials 18(1):13–16