Abstract—Over the past few years, increasing concern over personal information in computer systems has increased interest in data security. This paper reviews and applies visual cryptography, a perfectly secure method of keeping images secret, for possible use in biometric identification and protection. The basic concept of visual cryptography is to divide secret images into random shares. Decryption is performed by superimposing the shares. Hence the process does not require any special software or hardware device for cryptographic computations. In this work, we review some visual cryptography schemes and apply them to biometric data such as fingerprint images for the purpose of user authentication.

I. INTRODUCTION

Increasing access to the Internet and information resources has a great impact in our everyday life and is making humans more dependent on computer systems and networks. This dependency has brought many threats to information security. As a result, reliably secure mechanisms are required to protect computers and important information against vulnerabilities like ID spoofing and unauthorised access to computer resources. Biometric authentication systems are an example of technologies which are widely accepted in various applications such as in identification based systems and access control, ID cards, banking, etc. Therefore its accuracy and confidentiality should be guaranteed.

Biometrics is a science that uses unique physical characteristics (such as fingerprints, iris, retina, face and hand geometry) or behavioural characteristics (such as voice, signatures, and keystrokes) for the purpose of identification and authentication [1]. Using biometric methods has significant advantages over traditional password authentication systems. For example passwords can be forgotten, stolen or shared. Also simple passwords are easy to guess and complex passwords are hard to remember. Hence biometric traits can be more reliable. In addition, it is difficult to forge biometrics because the presence of an eligible user is required for authentication. But, there are some difficulties in biometric authentication. Biometric data is not secret and often this data can be changed according to the physical or emotional conditions of an owner at a time of authentication [1]. Thus, a number of studies have been done by researchers to protect biometric data and templates in a database. Cryptography and data hiding are the well-known methods for protecting data information by writing it in unreadable, secret codes and transmitting in a secure way. Steganography, visual cryptography and watermarking are some data hiding methods that can be used in order to increase the level of information security.

This paper provides an overview of visual cryptography as a technique for achieving data security and discusses its application in biometric authentication. The rest of this paper is organized as follows: in Section 2, visual cryptography is introduced and we review the visual secret sharing schemes proposed by Naor and Shamir [2] and Chen and Wu [3]. Section 3 presents some applications of visual cryptography to biometric security. The experimental results and conclusions are presented in Section 4 and section 5.

II. VISUAL CRYPTOGRAPHY

The visual cryptography scheme (VCS), introduced by Naor and Shamir in 1994 [2] is a type of secret sharing scheme which can split secret information into $n$ shares and recover them by superimposing the shares. In VCS, the secret to be hidden is a black and white image and each share is compromised of groups of $m$ black and white subpixel used to recover a pixel of the secret image. It is assumed that a white pixel in a share is transparent and a black pixel is opaque. It
is impossible to get any information about the secret images from shares individually. The other advantage of VCS is that, unlike other cryptography techniques, this secret recovery does not need difficult computations. The secret information can easily be recovered with enough shares and requires human vision instead of special software or hardware devices.

Naor and Shamir proposed a \( k \) out of \( n \) scheme and assumed that the image or message is a collection of binary 1 and 0 displayed as black and white pixels. According to their algorithm, the secret image is turned into \( n \) shares and the secret is revealed if any \( k \) of them are stacked together. So the image remains hidden if fewer than \( k \) shares are stacked together [5].

Image contrast and the number of subpixels of the shares and recovered image are two main parameters in visual cryptography schemes. The number of subpixels represents expansion of the image and should be as small as possible, while the contrast, which is a relative difference between the maximum value of Hamming weight for a black pixel and the minimum value of Hamming weight for white pixel, needs to be as large as possible [4]. Some researchers have focused on contrast degradation and introduced methods to improve the contrast of the reconstructed secret image [5], [6] while many studies have been done on applying visual cryptography to support grayscale and natural images with meaningful shares. This is known as extended visual cryptography [7], [8], [9], [10].

A. 2-out-of-2 Secret Image Sharing Scheme

The basic idea of visual cryptography can be illustrated with the 2-out-of-2 scheme. In the 2-out-of-2 scheme, every secret pixel of the image is converted into two shares and recovered by simply stacking two shares together. This is equivalent to using the OR operation between the shares. As illustrated in Table 1 [4], 4 subpixels are generated from a pixel of the secret image in a way that 2 subpixels are white and 2 pixels are black. The pixel selection is a random selection from each pattern. For example, when the corresponding pixel is white, one of the first six rows of Table 1 is randomly selected to encode the pixel into 2 shares. It is easy to see that knowing only one share value does not reveal the other share and the secret image pixel. However superimposing all the shares reveals the corresponding binary secret image.

Figure 1 shows an example of applying the 2-out-of-2 with 4-subpixels layout visual secret sharing scheme, where the share images are 2 times larger than the original secret image in each dimension. That is, the share uses 4 subpixel for the original pixel. As illustrated in Figure 1, (a) is the original secret image, (b) and (c) are two random shares, and (d) shows the reconstructed image from superimposing the two shares.

<table>
<thead>
<tr>
<th>Pixel</th>
<th>Probability</th>
<th>Share1</th>
<th>Share2</th>
<th>After Stacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>White</td>
<td>1/6</td>
<td><img src="image1" alt="Share1 White" /></td>
<td><img src="image2" alt="Share2 White" /></td>
<td><img src="image3" alt="After Stacking White" /></td>
</tr>
<tr>
<td>Black</td>
<td>1/6</td>
<td><img src="image4" alt="Share1 Black" /></td>
<td><img src="image5" alt="Share2 Black" /></td>
<td><img src="image6" alt="After Stacking Black" /></td>
</tr>
</tbody>
</table>

Fig. 1. 2-out-of-2 secret sharing scheme
TABLE II
ILLUSTRATION OF VISUAL TWO-SECRET IMAGE SHARING SCHEME

| Pixel of the first secret image | W | W | B | B | W | W | B | B | W | W | B | B |
| Pixel of the second secret image | W | B | B | W | W | B | B | W | W | B | B | W |

| s1          |          |
| s2          |          |
| s3          |          |
| s1 stack s2 |          |
| s3 stack s2 |          |

**B. Multiple Secret Image Sharing Scheme**

In 1998, Chen and Wu developed Naor and Shamir’s schemes and proposed a multiple secret image scheme [3]. One shortcoming of Naor and Shamir’s schemes is that only one secret image can be concealed at a time. So, Chen and Wu proposed a method that could encrypt two secret images at the same time by using a rotation technique in a way that binary images divide into two random, meaningless shares, according to their encoding process. The first secret image becomes visible by stacking the first and second shares and the second secret is revealed by rotating counterclockwise the pixel groups of the first share by $\theta$, ($\theta$ is $90^\circ$, $180^\circ$ or $270^\circ$) and stacking it with the second share. Wu and Chen’s encoding scheme for visual two-secret sharing in two shares is summarized in Table 2 [11]. In this table, the rotation angle is assumed to be $90^\circ$.

As an example, assume that a pixel of the first and a pixel of a second secret image are both black. Four patterns can be assigned to create the first share (s1). If the selected pattern is randomly selected as depicted in Figure 2, the second share should be selected in a way that can reveal black while it stacks with s1 and s3, where s3 is s1 rotated counterclockwise by $90^\circ$. Consequently, four different patterns shown in Figure 3, could satisfy this condition. If s2 is selected as the pattern shown in Figure 3(a), stacking this pattern with what is shown in Figure 2 (a) and (b), will reveal the black subpixels [11].

![Fig. 2. Example of four possible patterns to be assigned in multiple secret sharing scheme for first share](image)

![Fig. 3. Example of four possible patterns to be assigned in multiple secret sharing scheme for second share](image)

**III. APPLICATION OF VISUAL CRYPTOGRAPHY TO BIOMETRIC AUTHENTICATION**

The fingerprint is the most common human biometric characteristic that has been used for personal identification. Results obtained from comparing different biometric traits [1] show that: the fingerprint has a high value in factors like permanence, distinctiveness and performance, and medium value in universality, collectability and acceptability, while the hand-written signature has the lowest value in universality, distinctiveness, permanence and performance. For improving security, reducing fraud and enhancing user convenience, biometric systems require the process of enrollment, verification and identification.
In enrollment, the biometric template will be collected and stored in a database for eligible users. Verification is the process of confirming the authenticity of a biometric sample. Finally, identification is the process in which the identity of a biometric sample in a database is determined [1]. Protecting and securing biometric templates in the database are of great importance to prevent systems from being vulnerable to some attacks. Data hiding techniques, such as visual cryptography can enhance the security by embedding additional information in biometric images. Using the basic scheme of visual cryptography for securing fingerprint authentication is suggested in [4], [12], [13]. For improving the quality, increasing the contrast and simplicity in matching of the reconstructed image, the authors in [13] substituted the OR operator with XOR operator as the process of stacking VCS shares. Figure 4 depicts the encryption and decryption processes of the fingerprint image [14] using 2-out-of-2 VCS based on XOR operation which results in perfect reconstruction of both black and white pixels.

As an example application combining biometrics and data hiding consider the application of an ID card containing a biometric template VCS share. Fingerprint images are considered as a biometric sample and an entrance security system in a company is considered as case study in our approach.

Generally, as discussed in [13], the fingerprint of each eligible person is collected by the system administrator and they are given to the visual cryptography algorithm. Random shares are created from fingerprint images. One of the shares is stored in the database and the other share is given to the eligible person in the form of unique ID card. For verification, the user should insert the ID card into the security system. The corresponding share which is stored in the database is found and stacked with the other random share that is embedded in the ID card. After verification, the system should identify the participant. Hence, the system requests the participant’s new fingerprints to compare with the minutiae extracted from secret fingerprint images obtained from the visual cryptography algorithm. Authentication is accepted if the matching process succeeds.

The drawback of this method is the limitation in the number of biometric samples. The ID card requests one secret share for each biometric template. However, increasing a user’s biometric samples or using different types of biometric samples in a template can lead to increasing the accuracy and security in an authentication system. Moreover, it makes biometric systems spoofing more difficult. Further, fingerprint authentication systems may have thousands of users and it is therefore desirable to minimize the cost and capacity of storing biometric templates in a database.

Using the multiple secret image sharing algorithm is one way to improve the system. As discussed earlier, Chen and Wu’s visual cryptography method needs only two shares to represent secret images (eg. biometric templates). We use this method and consider the same idea for an ID card with two fingerprints belonging to the same person. In this process, two fingerprint images are given to the multiple secret sharing algorithm as secret images. After generating the shares, one of the shares could be embedded in an ID card, and the second share will be kept in the database with the third share being derived by rotation of the share which is stored in the database. So there is no need to store the third share in an ID card or in a database. In authentication, inserting the valid card into the system results in the stacking of corresponding shares and ultimately revealing the two fingerprint images. Entrance will be allowed if the comparison and matching of the newly provided fingerprints stored as the secret images with the physically obtained fingerprints are close together. In this scenario, an unauthorized user does not have access to the system. In addition, if the card is lost or stolen, it cannot be used because of the biometric detection technique. Effectiveness of the proposed method is verified by an experiment.

IV. EXPERIMENTAL RESULT

The result of the proposed experiment is implemented in MATLAB 7.9 running on Windows 7 computer. The size of each of the secret images [15], [16] is 210 × 310 pixels. As it is shown in Figure 5, the images are encrypted into three shares, each with the size of 420 × 620 pixels. For decryption, share A and share B are stacked together and the first secret image restored. The second secret fingerprint image is revealed by rotating the pixel group of share A counterclockwise 90° (share C in Figure 5) and superimposing it on share B.

V. CONCLUSION

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.

In this paper, visual cryptography and some of its schemes are reviewed. Moreover, a method is proposed to store and conceal two fingerprint templates in the database based on Chen and Wu’s multiple secret sharing image scheme. Applying multiple biometric templates for authentication can increase the security and is more efficient in terms of cost of storage, database capacity and bandwidth. In the proposed method, authentication in a security system is achieved by comparing and matching the participant’s fingerprints with secret fingerprint images that are derived from the visual cryptography algorithm.

Although our approach is presented for fingerprint authentication security, it can be easily extended to other biometrics such as facial images. Using grayscale 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.

REFERENCES