Biometric Privacy by Visual Cryptography Using Random Grid Method

Rahna. P. Muhammed
Department of Computer Science, Viswajyothi College of Engineering and Technology, Vazhakulam rahnap2000@gmail.com

Abstract—It is of great importance to preserve the privacy of biometric data stored in the central database server. This paper explores the possibility of using visual cryptography for imparting privacy to biometric data such as fingerprint images, iris codes, and face images. Visual cryptography is a secret sharing scheme where a secret image is encrypted into the shares which independently disclose no information about the original secret image. These two transparencies are stored in separate database servers such that the identity of the private data is not revealed to either server. Here one of the share is in reversible style. Stacking two transparencies after reversing one of them will reveal the original image. Reversing one of the transparencies is to improve security.

Keywords—Visual Cryptography, Random grid, Face, Fingerprint, Iris codes

I. INTRODUCTION

BIOMETRICS is the science of establishing the identity of an individual based on physical or behavioral traits such as face, fingerprints, iris, etc. The working of biometric authentication system is by acquiring raw biometric data from a subject, extracting a feature set from the data, and comparing the feature set against the templates stored in a database in order to identify the subject or to verify a claimed identity. The biometric template is generated during enrollment and is stored in the database. For ensuring the privacy to biometric template stored in the central database, several methods were provided. Here it introduced the concept of visual cryptography for imparting privacy to biometric template. Visual cryptography is a technique which allows visual information to be encrypted in such a way that the decryption can be performed by human visual system, without the aid of computers.

II. RELATED WORKS

For protecting the privacy of an individual enrolled in a biometric database, David et al. [1] and Rath et al. [2] proposed storing a transformed biometric template instead of the original biometric template in the database. Apart from these methods, various image hiding approaches [3–5] have been suggested by researchers to provide anonymity to the stored biometric data. Many visual cryptographic schemes produce shares in which each pixel of the original image is represented by multiple pixels in each share, diminishing the resolution of the decrypted image. Random Grid algorithm proposed by Kafri and Kerem [6] presents algorithms that both do not require pixel expansion.

The principle behind the random grid method is the use of two random grids in which the areas containing information in the two grids are inter correlated. When the two grids are superimposed and viewed together (see Fig. 1) the correlated areas will be resolved from the random background due to the difference in light transmission.

In this paper, the use of visual cryptography using random grid method is explored to preserve the privacy of biometric data by decomposing the original image into two noise images and are stored in two separate data bases in such a way that the original image can be revealed only when both images are simultaneously available; further, the individual component images do not reveal any information about the original image. One of the noise image is in reversible style in order to improve security.

III. VISUAL CRYPTOGRAPHY

The basic visual cryptography scheme was proposed by Naor and Shamir’s [7]. This scheme is referred to as the kout-of-n VCS which is denoted as (k, n)VCS. Given an original binary image, it is encrypted in n images, such that

$$T = S_{h1} \oplus S_{h2} \oplus S_{h3} \oplus \ldots \ldots \ldots \oplus S_{hn}$$

where $\oplus$ is a Boolean operation, $S_h$, $h \in 1, 2, \ldots, k$ is an image which appears as white noise, $k \leq n$, and $n$ is the number of noisy images. It is difficult to decipher the secret image $T$ using individuals $S_h$’s [7]. The encryption is undertaken in such a way that $k$ or more out of the $n$ generated images are necessary for reconstructing the original image $T$. In the case of $(2, 2)$ VCS, each pixel $P$ in the original image is encrypted into two subpixels called shares. For biometric privacy, here 2-out-of-2 scheme is using. In this scheme for sharing a single pixel $p$, in a binary image $Z$ into two shares $A$ and $B$ is illustrated in Table 1. If $p$ is white, one of the first two rows of Table 1 is chosen randomly to encode $A$ and $B$. If $p$...
is black, one of the last two rows in Table I is chosen randomly to encode A and B. Thus, neither A nor B exposes any clue about the binary color of p. When these two shares are superimposed together, two black sub-pixels appear if p is black, while one black sub-pixel and one white sub-pixel appear if p is white as indicated in the rightmost column in Table 1. Based upon the contrast between two kinds of reconstructed pixels can tell whether p is black or white.

### Table I

<table>
<thead>
<tr>
<th>Z</th>
<th>A</th>
<th>B</th>
<th>A(\oplus)B</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
</tr>
<tr>
<td></td>
<td><img src="image4.png" alt="Image" /></td>
<td><img src="image5.png" alt="Image" /></td>
<td><img src="image6.png" alt="Image" /></td>
</tr>
</tbody>
</table>

### IV. VISUAL SECRET SHARING BY RANDOM GRIDS

Random grid is a transparency comprising a two-dimensional array of picture elements (pixels). An important property of random grids is the principle of combination. If we cut out a section from a random grid and replace it with a similar section from a second random grid, the result is yet another random grid. The number of different grids possible is of the order of \(2^N\), where \(N\) is the number of pixels in the array. When two random grids with the same dimensions are placed one on top of the other so that they correspond pixel by pixel, the probability of each superimposed pixel’s being transparent is \(\frac{1}{2}\). Precisely, the binary secret image \(I\) with the size of \(h \times w\) will be encrypted into two cipher-grids \(R_1\) and \(R_2\) with the same size as that of \(I\) as shown in fig 2. Firstly, the cipher-grid \(R_1\) is created by randomly assigning each pixel the color 0 or 1, i.e., white and black. Secondly, the other cipher-grid \(R_2\) will be created by referring both the secret image \(I\) and the cipher-grid \(S_1\) according to one of Kafri and Keren’s algorithms. Algorithm for creating the shares is explained below.

### Algorithm for decomposing into two shares

Input: original image \(I\), where \(I\) is a halftone image and the image size is \(512 \times 512\) pixels

Output: Shares \(S_1\) and \(S_2\)

For \(i=0; i<512; i++\)

For \(j=0; j<512; j++\)

Random assign \(S_1[i][j]\) as white or black

If \(I[i][j]\) is white then

\(S_2[i][j]=S_1[i][j]\);

Else

\(S_2[i][j]=\) complement of \(S_1[i][j]\);

End if

End for

End for

### VI. PROPOSED METHOD

As protecting template in the database securely is one of the challenges in any biometric system. Here visual cryptography using random grids is applied to biometric authentication system [8]. In this system there are two modules: Enrollment module and Authentication module.

#### A. Enrollment

During enrollment process, the biometric data is sent to a trusted third party entity. Once the trusted entity receives it, the biometric data is decomposed into two shares. Among these two shares one of the shares is reversed. And these two shares (one reversed) are stored in separate databases such that the identity of private data is not revealed to either server. Further, cooperation between the two servers is essential in order to reconstruct the original biometric image.

#### Algorithm for decomposing into two shares

Input: original image \(I\), where \(I\) is a halftone image and the image size is \(512 \times 512\) pixels

Output: Share \(S_1\) and reverse share \(S_2\)

For \(i=0; i<512; i++\)

For \(j=0; j<512; j++\)

Random assign \(S_1[i][j]\) with subpixels

If \(I[i][j]\) is white

\(S_2[512-i][j]=S_1[i][j]\);

Else

\(S_2[512-i][j]=\) complement of \(S_1[i][j]\);

End if

End for

End for

#### B. Authentication

Here the trusted entity sends a request to each server and the corresponding sheets are transmitted to it. Stacking these two shares will not reveal the original image, thereby improving the security. Reversing one of the share and stacking with the other will reconstruct the original private image thereby avoiding any complicated decryption and decoding computations. Only the authenticated server knows which one is the reversed share.

#### Algorithm for superimposing two shares

Input: Share \(S_1\) and reverse share \(S_2\)

Output: Original image \(I\)

For \(i=0; i<512; i++\) For \(j=0; j<512; j++\)
if S2 is the reversed share Temp[i][j]=S2[512-i][j]
Superimpose two shares
I[i][j]=S1[i][j] ⊕ Temp[i][j]
End for

For faces, iris and fingerprints, as shown in Fig. 3, the biometric image is decomposed by the visual cryptography scheme and two noise-like images known as sheets are produced. For faces each private face image is decomposed into two independent public host images.

In basic visual cryptographic scheme increasing the pixel expansion factor m can lead to an increase in the storage requirements for the sheets. By using random grid method the encryption is possible without pixel expansion. Further if there is a possibility of getting the secret sheets it is impossible to retain the original image, since one is in reversible form.

VI. CONCLUSIONS

This paper explored the possibility of using visual cryptography by random grid method for imparting privacy to biometric templates. Here, the templates are decomposed into two noise-like images using (2, 2) VCS, and since the spatial arrangement of the pixels in these images varies from block to block, it is impossible to recover the original template without accessing both the shares.

REFERENCES