Biometric authentication and template protection using visual cryptography and watermarking

Dhanya K
Rajagiri School of Engineering and Technology
Cochin, Kerala
Email: dhanyadas63@gmail.com

Uday Babu P
Assistant Professor
Rajagiri School of Engineering and Technology
Cochin, Kerala
Email: udaybabup@gmail.com

Harikrishnan M
Assistant Professor
Rajagiri School of Engineering and Technology
Cochin
Email: krishna86hari@gmail.com

Abstract—Biometric system offer reliable personal identification but there are a lot of vulnerabilities associated with it like template modification, template tampering etc. Normally, biometric data are transmitted through a non secure channel. So the transferred biometric data should be properly authenticated. This paper suggests an entire protection for the iris biometrics in two stages: the primary step is to preserve iris image while the other is for securing the iris template. For preserving the captured iris image in the system, some unique information will be inserted in the middle band frequency of the image as watermark using a watermarking algorithm which works in the concept of Discrete wavelet Transform (DWT). Secondly, to protect the iris template, the binary format of the template will be converted to two parts called shares using some visual cryptographic techniques. And then one share will be stored somewhere in the dataset of the system and the other share will be given to the user. As an additional layer of security, the secure hash function SHA-2 is used to conserve the robustness of the iris template which is stored in both the database and with the user, usually in smart cards. And hence this system ensures the total security to the iris image.

Keywords—Template tampering, Watermark, Iris Template Protection, Discrete wavelet transform, Visual Cryptography, SHA-2.

I. INTRODUCTION

Biometric security devices helps to identify a person’s authenticity. A person’s unique characteristics which will not change over time is called biometrics. These include fingerprints, iris texture etc. The primary scope behind the biometric system is to do automatic action immediate after recognition. Biometric features are pre-stored in a biometric security system, which can be exclusively accessed by the authorized personnel. When an individual attempts to attain access to a system, the device inspect for his/her physical characteristics, which are then matched with the stored records. If a match is discovered, the individual is accorded access. Due to the extensive spread of biometrics technology, it is probable that the biometric details are being transmitted over non secure channels. Hence, for a biometric based system to act correctly, the system must ensure that the biometric data come from an authenticated individual at the time of registration. Several methods are employed to preserve the features of biometric data such as encryption alone, or watermarking along with encryption. However, encryption may put a boundary to the capacity of big scale biometric systems because it is computationally expensive [1]. Also, there is a condition such that the decryption of the templates must happen before the template matching. This condition can also reduce the protection strength. Therefore, the use of watermarking technology has raised. Since watermarking implicates hiding information within the host data, it can provide safety even after decrypting the data. Also the template for matching will be stored as raw form in the database [2] believing that people cannot get details from it. But there are softwares to decode the raw templates. So additionally, visual cryptographic techniques can also be used to secure the templates.

This paper is organized as follows. Section III explains the proposed technique. Experimental design and performance analysis are given in Section IV. Finally, Section V concludes this paper.

II. RELATED WORKS

This section includes the current area including vital findings and different works which are present in this area.

1) Iris image protection using DCT watermarking: As per the concept [3], it aims to protect the authenticity and integrity of the iris image. It uses DCT to embed in the middle band frequency of the image and embed the bio data of that person in the image. It exchanges more than one pair of central band frequencies so as the attacker cannot make change to all of the coefficients. It can withstand JPEG compression, noising at the same time, it won’t affect the image quality.

2) Bio-metric data security using Steganography and Visual Cryptography: In the concept of [4], the image will be divided into two shares in this method and store these shares in two different databases. Without getting these two shares, the retrieval of the image will not happen. Through steganographic techniques, the bio data will be stored in the images.

3) Verification System for the Privacy Protection of Iris Template: The concept in [5] extracts the secure identifiers from both of the irises with the help of pseudo random permutation function and hash function. To get the original image, it requires the user ID and both the templates. Additionally, it will also asks for two biometric traits to add more complexity.

III. WATERMARKING AND VISUAL CRYPTOGRAPHY SCHEMES

The proposed system will go through three stages.
A. Stage one: Binary template creation

Binary template is used to save the details of the authentic owner of the biometric ID. There are different ways to create the biometric ID. Two such important methods are image segmentation and gabor, both of them can be used independently. Image segmentation [8] is the process of dividing a digital image into several fragments. The idea is to unravel the complex representation of image into a more meaningful format for easy analysis. Gabor is a method in which the image is represented as a histogram sequence by adding the histograms of every local regions of every local Gabor magnitude binary pattern map [7]. By using the histogram intersection method, calculate the resemblance of dissimilar LGBP HSS, histograms can be identified.

B. Stage Two: Biometric images watermarking

The data will be set in the image in an invisible format which is called watermarking. Watermarking algorithms are divided according to their embedding domain into transformation domain techniques [8] and spatial domain techniques [9]. In the spatial domain the pixel values are directly modified to embed the watermark using different approaches such as Least Significant Bit (LSB) [10]. Since the spatial domain techniques have high payload and least complexity, they cannot withstand low pass filtering, image compression and basic image processing attacks [11]. Therefore, transform domain watermarking has emerged because it is robust against image manipulations and compression. In the frequency domain, the host image is divided into different frequency chains using several transformations such as DWT or DCT [12], [13]. Then, the watermarked image will be getting by applying the inverse transform. Different methods can be used for watermarking one of which is DWT. Discrete wavelet transform is a multiresolution decomposition of a signal. It hierarchically divides an image. Information regarding edge elements are included in high frequency parts and low frequency parts again divided into a set of low and high frequency wedges. The image is partitioned into four types of sub bands namely LH, HL, HH and LL using DWT. Fine-scale DWT coefficients are represented by LL, sub bands. LL sub band is further divided into four sub bands to obtain next coarser wavelet coefficients [2]. This process is repeated several times.

Fig. 1. Decomposition using DWT watermarking.

C. Stage Three: Visual Cryptography

Template spoofing is the most destructive attack in many biometric systems. Replication of the stored template is also an issue. So this section proposes a technique to tackle such issues and provide integrity to the stored template. Visual cryptographic techniques are used to securely save the templates as shares and the SHA-256 [2] algorithm is used to provide integrity to the stored shares. Hash signature helps to dispense an individual signature to the template and thereby deliver integrity.

IV. PROPOSED SYSTEM

The proposed system comprises of two modules.

1) Enrollment module
2) Authentication Module

A. Enrollment Module

In this module, feature encoding is implemented by convoluting the normalized iris template with a 1-D log-Gabor filter. Using the Daugman method [14], the output of is then phase quantized to four levels, with two bits of data per filter for each phase to form the binary template. Then, the binary template is divided into two shares using (2,2) visual cryptography and the original template is discarded. After that, two 256 bit signatures s1 and s2 are generated as signatures for share1 and share2 respectively using the SHA-256 hash function to prolong the integrity and uniqueness of the iris template. In the enrolment stage, one of the decomposed shares (share1) is stored with the admin along with s2 (signature of share2) while share2 and s1 are given to the user via email or on a smart card. s1 is also used as the private key which selects the watermarking embedding locations. Enrollment module takes up the biometric feature and necessary details. Watermark the unique detail in the binary image (iris or fingerprint) and store somewhere securely. Then using visual cryptography, it can divide the watermarked image into two shares and generate two keys from each of the shares using some hash function. Provide one share and another shares key to the user [2] and save the other share and key in a folder. The result from this module is represented in Fig 2.

Fig. 2. Enrolment Module

B. Authentication Module

Authentication module will accept the share and key from the user, check with the other share and generate the watermarked binary image if authenticated share is the input. Compare both the watermarked images and provide service if authentication is successful. During the authentication process, the system dispatches a request to the database to fetch the corresponding share based on the generated signature (s2) from share2. Then, the obtained share from the database is lade
together with the user's share from the smart card or special storage in order to rebuild the original iris template. Moreover, to ensure that the template in the smart card or the database is not altered, the SHA-256 hash function is generated again and compared with the stored signatures s1 and s2. If the signatures do not match, authorization will not be granted. After that, the inbound users' iris template and the reconstructed iris template from the smart card and the database are compared together to authenticate the user.

Fig. 3. Authentication Module

V. RESULTS AND DISCUSSIONS

1) Homepage will be the page the user will see while getting into the application. An existing user can go for the login option and a new user can go for a registration. Both will redirect to corresponding forms.

2) Enrolment form which would display after the user clicks on the register button. Here user can fill all the details and the details will be saved in the database in an encrypted manner. After entering the details, the user can upload his iris image. Iris images can be uploaded from the dataset using the browse functionality.

3) For converting text file into image, it needs to be converted to first to an 1D matrix and then to image. One condition persists is the image size. It must be equal as foregoing for handling the text into image. Then converted to 1D matrix using reshape command. Then write into text file.

4) Binary template will be created from the uploaded iris image using image segmentation technique or gabor and apply DWT watermarking in it.

5) The binary template is partitioned into two shares using the (2,2) visual cryptographic scheme. A hacker can get into the system only if he/ she has both of the shares. Here one share will be Emailed to the registered email id and the other will be saved in the system for future use.

6) Hashes of both the shares are generated using SHA-256 function and hash of one share will be saved while the other will be sending through email to the user. ie: Hash of share A will save in the system while hash of share B will be emailed to the user.

7) While the authentication phase, the user has to do the normal login procedure with his username and password. After successful login, user can upload the share and the hash key along with the unique id and his iris image to login to the system.

8) The binary image can be reconstructed in the following way.
   - Get the other share from database using hash
   - Merge two of them
   - Add the unknown image
   - Apply watermarking

On successful matching, permission will be granted or else the access will be denied. And finally the iris image will be transformed into two shares after the enrolment module and reversed to the original image during authentication phase.

Fig. 4. Transformations of Iris Image

I have done the comparison between DCT and DWT and reached to a conclusion that DWT provides higher compression ratios. DWT provides good restriction along with localization in both spatial and frequency domains. Alteration of the entire image launches inherent scaling. Better identification of which data is pertinent to human recognition, higher compression ratio and also see that DCT takes more time than DWT. So this method provides good performance rather than in system [2]

Fig. 5. Comparison Study Table.

<table>
<thead>
<tr>
<th>factors</th>
<th>DCT</th>
<th>DWT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compression ratio</td>
<td>20.1763</td>
<td>20.3855</td>
</tr>
<tr>
<td>PSNR</td>
<td>0.0263</td>
<td>38.6309</td>
</tr>
<tr>
<td>MSE</td>
<td>10.38</td>
<td>8.9123</td>
</tr>
<tr>
<td>BER</td>
<td>37.96</td>
<td>0.0259</td>
</tr>
<tr>
<td>TIME</td>
<td>7.4121</td>
<td>3.5139</td>
</tr>
</tbody>
</table>

VI. CONCLUSION

The work proposed in this paper aimed to bring insight into the problem of biometric security. Novel schemes were proposed for iris image and template protection which consist of two security layers. The first layer is a robust watermarking algorithm which was implemented to secure the uniqueness of the biometric image. In particular, a binary text image that accommodates the bio data of the person to be authenticated was embedded inside the biometric image by randomly interchanging four pairs of the DCT middle band coefficients. The embedding locations were randomly selected based on
a private key. Moreover, the proposed strength constant $s$ was included to add more robustness to the watermarking algorithm. The second layer involved using the VC to protect the iris template by decomposing the indigenous iris template into two shares using (2,2) Visual cryptography where one share is given to the user through email or on a smart card and the other will be saved in a database. The proposed VC scheme allows the iris template to be perfectly restored with the same quality and size when the shares are available, and therefore it does not hinder the iris recognition performance. An extra layer of security is added to the iris template because even if any of the shares in the database or the smart card is compromised, the original template cannot be retrieved. Further, the uniqueness of the iris templates, in both the smart card and the database, is also guaranteed with the use of the hash signatures. The generated signature from the hash function is not only beneficial to manage the uniqueness and integrity of the smart card but also it has been used to select the embedding locations for the watermarking algorithm.

VII. FUTURE ENHANCEMENTS

Security enhancement is possible by using $(k,n)$ visual cryptography instead of $(2,2)$ cryptography. This paper can be extended to secure another biometrices such as fingerprint, face recognition etc.

REFERENCES
