Multimodal Biometrics for authentication using DRM Technique

Sherin Edward[1], S.Sumathi [2] and R.RaniHema Malini[3]

[1]PG ,Sri Sai Ram Engineering College,Chennai-44 E-mail: sherin_ece07@yahoo.co.in,
[2]Research Scholar, Sathyabama University, Chennai-96 E mail: sumathi_ba@rediffmail.com,
[3]Professor& Head, Dept of E&I,St.Peter's University, Chennai-54. E mail: ranihema@yahoo.com,

***Abstract*- Aim of this project is to implement a novel authentication scheme to establish Digital Rights Management (DRM) based on multimodal biometric verification and watermarking technique. Security of biometric system is a major concern. An attack on a biometric system can result in loss of privacy, monetary damage and security breach. Biometric system offer better security then existing approaches. The Highly secure face and iris features are used for multimodal biometric verification. Face image is taken to be the host image and the iris feature is selected as the watermark hidden in the host image. Such that iris feature watermark not only protects face biometric data but also can be used as covert recognition. To evaluate the performance of watermarking for multimodal biometrics - embedding iris feature into a face image. The first process is enrollment of the victim's face and iris features in the available database. Second authentication is done by comparing the features of face image in the data base when it matches, the iris feature is extracted and compared with data base then verify the authentication. This type of biometric system protects the biometric template and improves the security and privacy level of biometric authentication.**

***Index Terms* —Digital Rights Management (DRM); Iris recognition; Face recognition; Watermarking**.

I. INTRODUCTION

Information security has gained more and more attention from researchers because it plays an important role in our daily life. Due to the rapid development of digital technology, internet, mobile and extensive use of multi-media terminal, greatly expanding the scope of the transmission of digital content. With the ease of duplication and sharing of digital content- may it be music, video or documents a need has been felt to provide a mechanism to check unauthorized access to content. The DRM system provides security for digital content distribution, management and operational control authority.

The problem with biometric identification is security and privacy of the biometric data's .If the person's biometric data is stolen, it is not possible to replace it as in case of a credit card, ID. Biometric data provides uniqueness, but it is not secret. So in order to improve the utilization of biometric recognition and to provide biometric security. One of the most stolen attacks is against stored templates. ie, Templates in the database are modified, removed or new templates are added. Another one is the transferred template information is altered in the communication channel.

The watermark embedded in the biometric data provides another line of defense against illegal utilization of the biometric data. It also should eliminate some of attacks to biometric system [1].Due to embedding watermark the inherent characteristics of host image may change .The verification of watermark image should not lead to degrade compared with original non watermark image. Ratha et al proposed a data hiding method for wavelet compressed finger print images [2]. Pantanti and Yeung developed a fragile watermarking for finger print images verification [3]. These works are only on biometric data hiding and only involve the use of face and fingerprint images. In order increase the authentication accuracy, it is required to combine more than two biometric. The technology of combining biometric and watermarking algorithm has been proposed [4-6]. Anil K.J. has proposed a method of hiding fourteen eigenface coefficients in fingerprint images based on digital watermarking [7].There is some disadvantages, first, because of local features such as minutiae are used for conventional fingerprint recognition, finger print images could be easily impaired by the embedded face watermark. Second, watermark on spatial domain has severe weakness against attack such as blurring and cropping.

According to biometric watermarking, iris image also sensitive to watermark embedding, because it uses high frequency components such as fine iris textures for authentication. On the contrary, a face image has the advantage of being embedded with a more robust watermark, because it uses low frequency components for authentication compared to iris and fingerprint image. However, face recognition has an inherent weakness for high security authentication due to its sensibility to pose, expression and lighting variations. So, we use the method of watermarking iris features on face data [5], which hide iris features based on the Fast Fourier Transform (FFT) to a face image by watermarking technique.

In this paper according to Kang et al [5] Research theory and De Song Wang [8], we describe digital rights management using multimodal biometrics which integrates watermarking technique and multimodal biometric system to provide more secure and reliable personal recognition. For describing authentication scheme, two biometric traits have been in consideration: iris feature and face feature. The rest of the paper is organized as follow. The DRM system in section II. Iris feature based watermarking algorithm in section III .Biometrics fusion authentication in section IV. Section V presents the conclusion and future work.

II. DRM SYSTEM

The basic digital rights management system have two main module which is enrollment and authentication. This can be shown in fig 1(a), 1(b).

The enrollment process is done by the following steps

Step 1. Initially, the face of the victim is captured as a photograph which is an high resolution image.

Step 2. Then the iris part is detected from the captured image from this iris region is segmented including removing eyelash, eyelid and Regular and Singular detection .Then we extract iris features in mid and high frequency bands of FFT domain from the segmented iris region.

Step 3 Here iris become the watermark and face is the host image.

Step 4 The Eigen Face of the watermarked Face the Iris feature is obtained and the original images are stored in the database and the victim gets enrolled.

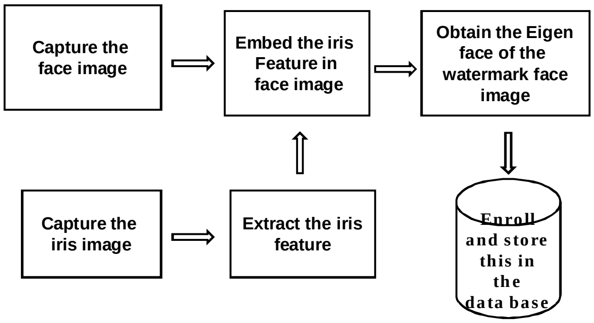

Capture the face image
Embed the iris Feature in face image
Obtain the Eigen face of the watermark face image
Capture the iris image
Extract the iris feature
Enroll and store this in the data base

Figure 1(a) Enrollment

The authentication is done by following steps

Step 1. In this module, the victim's facial image is captured and the eigen face is obtained.

Step 2 Now Compare the facial image with unique features with the collection of images in the database.

Step 3. If the image doesn't match, the person not authenticated. If the image is authenticated (matched), then extract the watermark i.e., Iris is done.

Step 4. The extracted iris feature is compared with the database. This can be the second level of authentication procedure to assure more security to the access of the victim .If it matches with the database the particular person is said to be authenticated. Otherwise the victim is not authenticated.

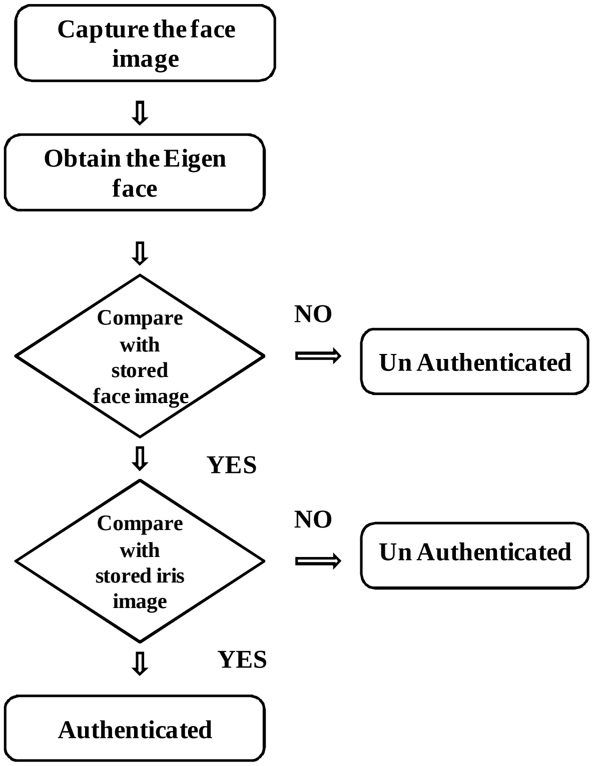


Figure .1(b) Authentication

It is the verification of victim's identity for security issue. As a result of module 1, the captured images and the respective eigen faces are utilized as the reference database.

III. FACE AND IRIS RECOGNITION

For the credibility and the safety ownership identifying we combine the watermarking technique and fusion technique with iris and face recognition. The iris and face recognition is done by DWT.The threshold for authenticate or imposter was determined by trained face data (without watermark) based on Bayesian rules which can minimize both FAR (False Acceptance Rate: error rate of accepting imposter as genuine) and FRR (False Accepting Rate: error rate of rejecting a genuine imposter).

IV. WATERMARK ALOGRITHM

A. Watermark generation

In this the iris image is used as watermark. The iris image have much useless part which can be removed by location and elimination .The iris locating algorithm was proposed by Li and Ma[9] to locate the iris part, eliminate its inner part and outer part and then normalize the iris part

B. Biometric watermark embedding and extraction

In this research, we use iris features as watermarking Information embedded to face image. The Iris features such as Trabecular mesh, furrows, and freckles are converted into 512 bytes and embed this in the face image. After face recognition is finished, we extract the embedded watermark (iris features in frequency domain) from face image and compute the similarity between the extracted iris features and the enrolled one. This is not only a robust authentication method, but it can make the watermarked iris features secure. The watermark embedding and extraction is performed in ridgelet domain.

1. Ridgelet domain

Wavelets are very effective in representing objects with isolated point singularities. Unfortunately, in two dimensions, they act well at isolating the discontinuities across an edge, but cannot see the smoothness along the edge. The ridgelet transform was proposed in order to overcome the problem of the wavelet transform in representing objects with singularities along line. The idea behind the ridgelet transform was to map a line singularity to a point singularity using the radon transform and then use wavelet transform to represent the point singularity in the radon transform effectively

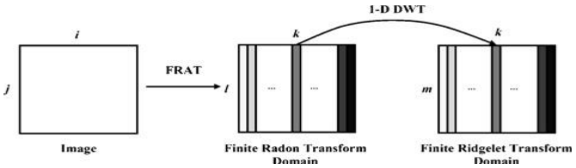

1-D DWT
i
j
k
k
FRAT
l
m
...
...
...
...
Image
Finite Radon Transform Domain
Finite Ridgelet Transform Domain

Fig.2. Two stages in applying FRIT to an image.

At the first stage FART is applied to the image and 1-D wavelet transform is applied on each FART projection where k is fixed this was proposed by Nima Khademi [10].

2. Watermark embedding

The watermark embedding procedure can be summarized in the following steps.

1) The original image is divided into fixed length $N \times N$ non-overlapping blocks.

2) In order to embed the watermark data into the more textured regions, L blocks with high-entropy values are selected for data embedding. This entropy thresholding scheme is carried out so that the invisibility of the watermark insertion is assured.

3) The ridgelet transform is then applied to each of the selected blocks. Thus, $(N + 1)\times(N-1)$ FRIT coefficients (FRITl $[k,m]$, $1 < l \leq L$) are obtained for each block.

4) The most energetic direction for each of the selected blocks is found as follows:

$$d_l = \arg\max_k \left(\frac{1}{N-1}\sum_{m=0}^{N-2}(FRIT_l[k,m])^2\right) \qquad (1)$$

Where m refers to the coefficients of ridgelet transform in each direction.

5) In this step, the watermark data $M=\{m1,\ m2,\ mL\}$ is embedded by modifying the amplitude of the selected coefficients.

$$X_{wl} = \alpha \times X_l, \qquad m_l = 1 \qquad (2)$$

$$X_{wl} = \frac{1}{\alpha} \times X_l \qquad m_l = 0 \qquad (3)$$

Xw is the watermarked ridgelet coefficients vector, and α is the watermark strength factor and has a value larger than one. A larger value for α leads to more robustness and lower transparency, and vice versa.

6) In the final step, the inverse ridgelet transform is applied to the FRIT coefficients and the watermarked image is constructed.

3. Watermark extraction

In this section, the watermark extraction process for the proposed embedding scheme is described. The decoder is optimized under additive white Gaussian noise (AWGN) attack. For this aim, we consider the watermarked image which is contaminated with the zero-mean Gaussian noise. According to [11], for orthogonal FRIT, the noise is still zero-mean Gaussian with the same variance in the ridgelet domain. Thus, we have $R = Xw+N$ where N is the zero-mean Gaussian noise with variance σ_n^2 and independent of Xw. Here in after, for the sake of simplicity, we eliminate the block index l in equations. As mentioned in [12], we cannot make any assumption on the distribution of the ridgelet coefficients. Therefore, a maximum likelihood decoder cannot be derived for the embedding method in the ridgelet transform domain. Thus, we need to have a decoder which works independent of the host signal distribution. The decoder that we propose here extracts the watermark data by the following hypothesis testing:

if $$z = \frac{\sum_{i=1}^{N} (x_{wl} + n_i)^2}{\sum x_i^2} > T, \quad \text{then } \hat{m} = 1 \quad (4)$$

if $$z = \frac{\sum_{i=l}^{N} (x_{wl} + n_i)^2}{\sum_{i=1}^{N} x_i^2} < T, \quad \text{then } \hat{m} = 0 \quad (5)$$

Where $\hat{m}$ is the extracted watermark data, n_i is the white Gaussian noise , x_i are the ridgelet coefficients corresponds to high energetic direction.

Four steps as follows.

1) The watermarked image is divided into $N \times N$ non-overlapping blocks
2) The ridgelet transform is applied to the blocks where the watermark data have been embedded during the watermark embedding process.
3) The coefficients representing the most energetic direction in each block are selected.
4) The watermark data is extracted from the coefficients obtained in step 3.

V. BIOMETRICS AND FUSION AUTHENTICATION

We use the iris feature extracted and the enrolled face feature to fuse together. Then we calculate the correlation value between the fusion features of iris and face and the enrolled fusion features of iris and face. User's authentication is successful when the computed correlation value is greater than predefined threshold. If the correlation value is smaller than the threshold, then the user's authentication is regarded to be unsuccessful.

VI. RESULTS

In this section, some experimental results are demonstrated to show the effectiveness and the robustness of the proposed watermarking algorithm. We see that the watermarked image is not distinguishable from the original image. To evaluate the quality between the watermarked image and the original image, the calculated PSNR value for Watermark image is 45 db. When the PSNR value of a watermarked image is greater than 30 dB, the quality is still acceptable to the human eyes. So we got good response in this method.

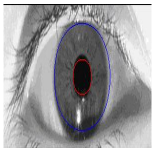


Fig.3 a.Iris pattern

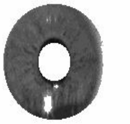
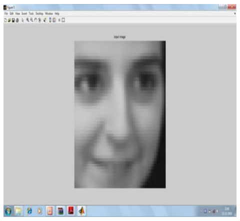
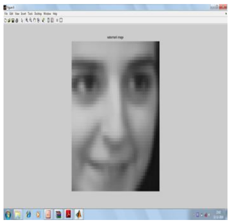


Fig.3b.Isolated boundary



Original Image



Watermark Image

VII. CONCLUSION AND FUTURE WORK

Multimodal biometric systems are expected to be more reliable and able to meet the stringent performance requirement imposed by various applications. However, the security and privacy of the biometric data are important issue. In this paper, we introduce a novel authentication scheme of the DRM system based on multimodal biometric verification and watermarking technique having following four objectives. First, by using watermarked iris features to face data, the multimodal biometric authentication can be possible, which can increase the authentication accuracy. Second, if the saved face data is illegally let out and privacy infringement happens, then we can solve the legal responsibility problem about the outflow of face data by checking the embedded iris feature watermark. Third, Multimodal biometric systems based biometrics fusion authentication not only result in a better improvement in performance but also ensure sufficient population coverage. Fourth, the system provides more security against spoofing because it is difficult for an attacker to simultaneous spoof the multiple characteristics of a genuine user. In future, we will include more features and conduct more tests to validate the performance of the recognition system in real-time application

REFERENCES

[1] Jain A. K., and Uludag U., "Hiding biometric Data", IEEE Trans. on PAMI, Vol.25, No.11, pp.1494-1498, 2003.

[2] Ratha N. K., Connel J. H., and Bolle R. M., "Secure Data Hiding in Wavelet Compressed Fingerprint Images", Proc. ACM Multimedia, pp.127-130, Oct. 2000.

[3] Pankanti S., and Yeung M. M., "Verification Watermarks on Fingerprint Recognition and Retrieval', Proc. SPIE, Vol. 3657, pp.66-78, 1999.

[4] Lin H., and Anil. K. J., "Integrating Faces and Fingerprints for Personal Identification", IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 20, No. 12, pp. 1295-1307, 1998.

[5] Kang Ryoung Park, Dae Sik Jeong, Byung Jun Kang, and Eui Chul Lee, "A Study on Iris Feature Watermarking on Face Data", ICANNGA 2007, Part II, LNCS 4432, pp. 415-423, 2007.

[6] Gui Feng, and Qiwei Lin, "Iris feature based watermarking algorithm for personal identification", Proc. of SPIE, Vol. 6790, pp. 679045, 2007.

[7] Anil K. J., Umut U., and Rein-Lien H., "Hiding a Face in a Fingerprint Image", Proc. of Int. Conf. on Pattern Recognition, Vol. 3, pp. 756-759, 2002.

[8] De-Song Wang, Jian-Ping Li, Yue-Hao Yan "A Novel Authentication scheme of the DRM System based on Multimodal Biometric Verification and Watermarking Technique"IEEE 2008

[9] Qing-rong Li, and Zheng Ma, "An Iris Location System", Journal of UEST of China, Vol. 31, No.1, pp.7-9, 2002.

[10] Seyed Mohammad Ahadi, Nima Khademi Kalantari, "A Robust Image Watermarking in the Ridgelet Domain Using Universally Optimum Decoder" IEEE Transactions on circuits and systems for video technology, Vol 20, NO. 3, March 2010

[11] M. N. Do and M. Vetterli, "The finite ridgelet transform for image representation," IEEE Trans. Image Process., vol. 12, no. 1, pp. 16–28, Jan. 2003.

[12] P. Campisi, D. Kundur, and A. Neri "Robust digital watermarking in the ridgelet domain," *IEEE Signal Process. Lett.*, vol. 11, no. 10, pp. 826–830, Oct. 2004.