Iris Biometric Security using Watermarking and Visual Cryptography

B Swathi
Department of Electronics and
Communication Engineering
JNTUH College Of Engineering Hyderabad
Kukatpally,Hyderabad-500085
Email: bswathireddy06@gmail.com

Mrs.T Madhavi kumari
Associate professor
Department of Electronics and Communication Engineering
JNTUH College Of Engineering Hyderabad
Kukatpally,Hyderabad-500085
Email: thoomati@jntuh.ac.in

***Abstract*—This paper presents a novel security architecture which protects the iris using watermarking and visual cryptography techniques.The iris region is protected using watermarking technique where we are using DCT to embedd the watermarked text image into the iris image in the low frequency band.After performing watermarking ,the watermarked image is furthur processed to generate a template using Daugmans method and Gabor filter.The generated template is then gone through another security protection scheme using visual cryptography.Here the template is divided into two shares where one is present with the user and other in the data base.This is the enrollment module.Now for the Authentication module the user share and the data base share are overlapped and then the template is generated.Now the generated template is matched with the template which was already generated using Daugmans method.If both the templates are matched authentication is provided otherwise the person is unauthenticated.This paper is implemented using Matlab**

Keywords—Iris recognition,security,watermarking,visual cryptography,template matching.

I. INTRODUCTION

The Iris biometric security is one of the most secured system as the patterns of the iris remains unchanged throughout the persons life,hence providing a security to this kind of biometric is advantageous.Since we are providing three stage protection ,chances are very less for tampering the information. The proposed method for protection consists of three stages .The first stage is the watermarking algorithm which protects the iris image by using DCT which embedd the watermarking text which contains the details of the person in the form of image and which is embedded into the iris image of the person.The second stage is the template generation which uses Daugmans method.The watermarked image is segmented,normalized and then feature encoded to generate a template using Gabor filter and Daugmans method.The third stage is the visual cryptography scheme where the template is divided into two shares using the visual cryptography ,where one is stored in the database and other will be with the user.

A. WATERMARKING ALGORITHM

Here in this paper we are using watermarking algorithm based on discrete cosine transform.First the iris image is taken and dct2 is applied on the image and then it is divided into blocks where each block size is (8x8).The watermarked image is the text image which contains the details of the person for eg.name,date of birth etc.The watermarked image is converted into binary form and then embedded into the iris image in the low frequency band.Each dct block consists of three frequency bands low frequency,middle frequency and high frequency band.Here we are embedding the watermarked image into the low frequency band.

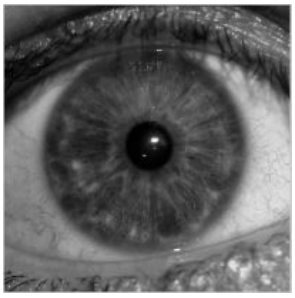

Fig. 1. Iris image

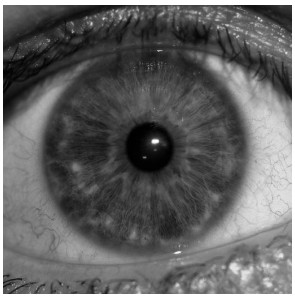

Fig. 2. watermarked iris image

B. TEMPLATE GENERATION

After the watermarked image is generated ,canny edge detection is used to generate the gradient and orientation of the image. Hough Transform and Log Gabor Filter is used to segment the iris boundary and the pupil boundary.Now the Daugmans rubber sheet model is used to generate the polar array and the noise array from the segmented image.Noise array contains the extra part like eyelashes and eyelids.Now the polar array is convolved with 1D Gabor filter and quantized to generate a template.

978-1-5386-0814-2/17/$31.00 ©2017 IEEE

Fig. 3. Generating a template

C. VISUAL CRYPTOGRAPHY

Visual cryptography is a secret sharing scheme.Here the template which is generated is divided into two random shares which doesnt reveal any information.The secret image can be reconstructed by stacking together the two shares.Here we are superimposing the two shares using XOR operation and thus the template is generated back.

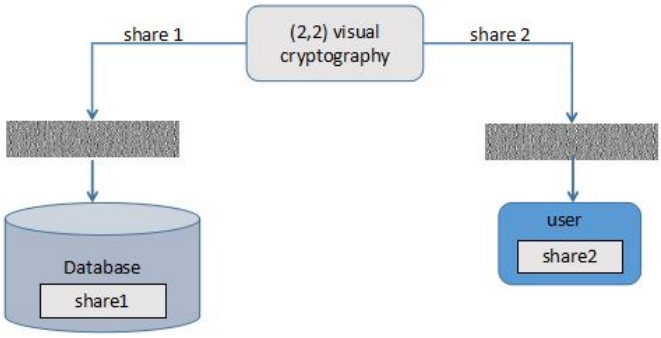

Fig. 4. visual cryptography

D. TEMPLATE MATCHING

For template matching we are using canny edge detection for detecting edges of two templates,one which is generated in enrollment module and other which is generated in authentication module by combining two shares after visual cryptography.After detecting the edges,bit by bit matching is done and total matched percentage is calculated.

II. PROPOSED TECHNIQUE

This represents the procedure for enrollment of a person and authenticating the person for security purpose.

A. ENROLLMENT MODULE

First the person iris image is stored,then the details of the person is watermarked inside the iris image.The watermarked image is generated then template is generated for the watermarked image.The template is undergone through visual cryptography and divided into two shares.One share is with the user and other is stored in the data base.

B. AUTHENTICATION MODULE

The share which is there with the user and the share which is in the data base are overlapped together to generate a template.Now this template and the template which was generated in the enrollment module is matched.If the person is the same person then authentication is displayed otherwise unauthentication is displayed.

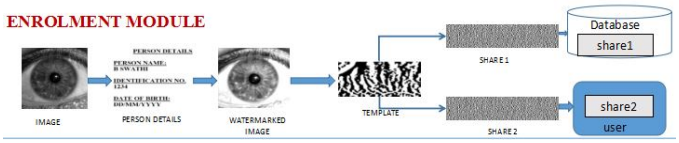

Fig. 5. Enrollment module of the proposed method

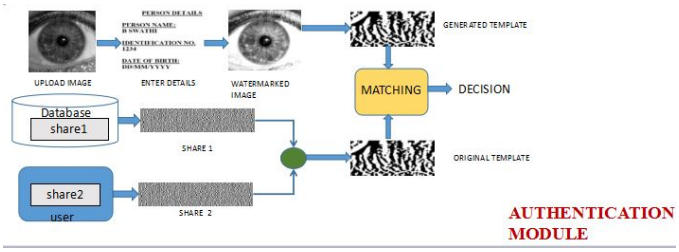

Fig. 6. Authentication module of the proposed method

III. RESULTS AND DISCUSSIONS

A. INPUT AND WATERMARKED IMAGE

Fig. 7. watermarked output

Here the grey image of iris is taken of size(512x512) and the watermarking text image of size(32x32).The watermarked output image is thus formed.

B. UNWRAPPING WATERMARKED IRIS

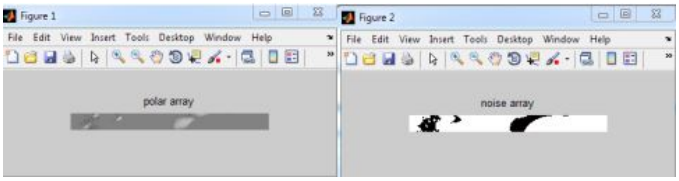

Fig. 8. unwrapped normalized iris

Daugman's rubber sheet model is used to normalize the iris into polar array and noise array.

C. WATERMARKED IRIS TEMPLATE

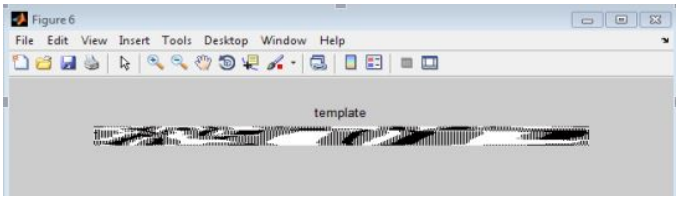

Fig. 9. watermarked iris template

We convolve polar array with the 1D gabor wavelet and real and imaginary are resulted which is quantized.If the acquired result value is zero ,a black pixel is stored otherwise white pixel is stored.Once all the columns of the image are filtered and quantized ,we can form the template by putting all columns side by side.

D. SHARE1 AND SHARE2

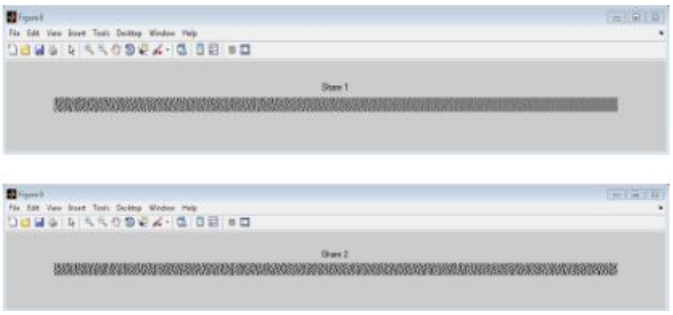

Fig. 10. share1 and share2 is generated after visual cryptography is applied

After the template is generated visual cryptography is applied to generate two shares share1 and share2.

E. TEMPLATE GENRATED

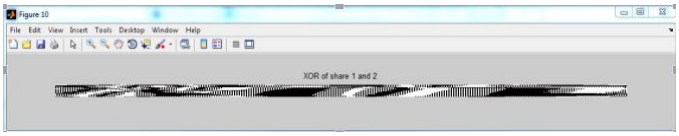

Fig. 11. share1 and share2 is overlapped to generate template

Share1 and Share2 is overlapped using XOR operation to generate a template.

F. FINAL GUI

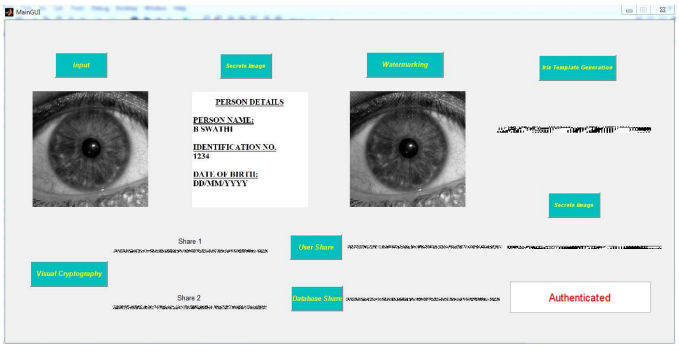

Fig. 12. GUI implementation of the proposed method

This is the final GUI implementation where the authentication deauthentication is displayed after template matching.

IV. CONCLUSION AND FUTURE SCOPE

Paper is aimed to bring insight into the problem of biometric security.The first layer is a watermarking algorithm which protects the integrity of the iris image.The second layer involves visual cryptography to protect the iris template by decomposing the original iris template into two shares.Finally the template matching is done for authentication.

The future scope of this project is cloud based biometric iris security where the cloud stores the data on a remote sensor which can be easily accessed through the internet instead of storing the template data in database.We can access data in real time from any computer which is having internet.Data is secured and can be stored for lifetime.

REFERENCES

[1] Mohammed A. M. Abdullah; Satnam S. Dlay; Wai L. Woo; Jonathon A. Chambers, *A Framework for Iris Biometrics Protection: A Marriage Between Watermarking and Visual Cryptography*. .

[2] M. Paunwala and S. Patnaik, *"Biometric template protection with DCTbased watermarking,"*. mach. Vis. Appl., vol. 25, no. 1, pp. 263_x0015_275, 2014.

[3] M. A. M. Abdullah, S. S. Dlay, andW. L.Woo, *"Securing iris images with a robust watermarking algorithm based on discrete cosine ransform,"*. in Proc. 10th Int. Conf. Comput. Vis. Theory Appl., vol. 3. 2015, pp. 108_x0015_114.

[4] F. Hao, R. Anderson, and J. Daugman,*"Combining crypto with biometrics effectively,"*. IEEE Trans. Comput., vol. 55, no. 9, pp. 1081_x0015_1088,Sep. 2006.