International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-6, August 2020

Secured Biometric Authentication of Iris Image using Visual Cryptography

Shafiqua Noorain, Mala L Muddannavar

Abstract: ***In the modern era of information technology security violation and attacks are increasing day by day . So, in order to manage this issues the number of ways of providing security to the systems are introduced .In which the most promising one is to improve the security by identifying or verifying the person using some technique. So, the basic idea is to use the identity of a person which can improve the security. Thus, the proposed work focuses on the security architecture for protecting integrity of iris images using watermarking and visual cryptography (VC). First, for protecting the iris image, a watermark text image which carries personal information is embedded in the middle frequency band region of the iris image which randomly interchanges multiple middle band pairs of discrete cosine transform(DCT). Second, for iris template protection, the watermarked image is further processed to generate a template using Gabor filter, the template is gone through another security protection scheme VC. Here the template is divided into two shares this is enrollment module. For the authentication module both shares are overlapped and template is generated. This generated template and the template from Gabor filter are matched using canny edge detection authentication is provided. Otherwise, the person is unauthenticated. This paper is implemented using Matlab.***

Keywords: Biometrics, Watermarking, Discrete Cosine Transform, Template Matching, Visual Cryptography.

I. INTRODUCTION

The growing need for security in recent year has resulted in the development of personal biometric identification systems. Biometrics is science of establishing human identity using physical or behavioral traits. The advantages of personal identification using biometrics features are numerous, such as fraud prevention and secure access control. Biometric techniques play major role in laying the foundation of a comprehensive series of highly secure identification method and designing of individual verification systems. Biometrics is the detailed measurement of human body. Biometrics deals with a method of identification a person or verifying the identity of person based on physiological or behavioral characteristics. There are various applications where personal identification is required such as passports, control, computer login control, secure electronic banking, bank ATM, credit cards, airport, mobile phone, health and social services etc. Many biometrics techniques are available such as finger print, face, retina, Iris, palm print, voice and signature. Among those Iris recognition is one of the most promising approach because of stability and uniqueness[1].

Revised Manuscript Received on July 22, 2020.
* Correspondence Author
Shafiqua Noorain*, M.Tech student, Department of Electronics and communication Engineering at SDM College of Engineering and Technology, Dharwad, Karnataka, India.. E-mail: shafiquanoorain09@gmail.com
Mala L Muddannavar, Assistant Professor, Department of Electronics and communication Engineering at SDM College of Engineering and Technology, Dharwad, Karnataka, India. E-mail: shivallimala97@gmail.com

II. PRELIMINARIES

Biometric systems is a system which allows the recognition of certain characteristics of an individual using mathematical algorithms and biometric data. There are several uses of biometric systems that requires enrollment upstream of users and authentication of data.

A. Watermarking

In this paper we use watermarking technique which is based on Discrete Cosine Transform (DCT). The Iris image is taken and DCT is applied on the image and image is divided into blocks where each block is (8x8). The watermark image which contains person details such as name, place etc is embedded into original iris images and watermarked image is obtained.

B. Template Generation

The obtained watermarked image is converted into binary form. The canny edge detection is used to generate gradient and orientation of the image. The edge detected image under goes Gabor convolve to generate polar array or the Template.

C. Visual cryptography

Visual Cryptography is secret sharing scheme. Here, the template is divided into two share i.e. share 1 and share 2 which does not reveal any information. The secret information can be revealed if they are stacked together. The two shares are overlapped together using XOR operation and thus the template is generated back.

D. Template Matching

The Two dimensional correlation is performed for template matching. Here, the template generated from enrollment module and authentication module are matched. Thus, if both template are matched authenticated is displayed and person authorized and if it is not matched the unauthenticated is displayed and person is declared as unauthorized person.

III. METHODOLOGY

The Proposed work is divided into two sub modules such as Enrollment and Authentication Module:

A. Enrollment module

Firstly, Original Iris image is considered as a input image and watermark text image which contains the person details such as name,

place and Identification number etc is embedded into the original Iris image using Discrete cosine transform(DCT). Where each DCT block consists of three frequency bands low, high and middle frequency bands in which we embed watermark data into middle frequency band and the Watermarked image is generated.

The Log Gabor filter is used to generate a polar array. The polar array is convolved with 1D Gabor filter and quantization is done to generate a template.

The generated template is divided into two shares using Visual Cryptography technique in which a share1 is with the user and another share 2 is stored in data base. Figure 1. shows block diagram of Enrollment module.

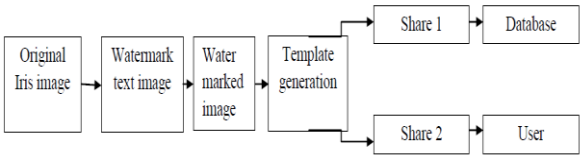

Figure 1: Enrollment module

B. Authentication module

The shares generated in the enrollment module are overlapped together using XOR operation to generate another template . Figure 2. shows the block diagram of Authentication module.

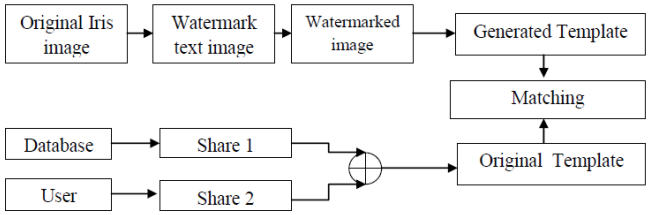

Figure 2: Authentication module

IV. RESULTS AND ANALYSIS

A. Input and Watermarked image

The original iris image is taken as input image and conversion of RBG to grayscale image as shown in Figure 3 . Then the watermark text image which contains person detail such as name, place and user id etc as shown in Figure 4 is embedded into original iris image using DCT as shown in Figure 5. The dct block consists of three frequency band into high frequency band, low frequency band and middle frequency band as shown in Figure 6 and 7. The middle band coefficients are used to embed the data and the watermarked image is obtained as shown in Figure 8.

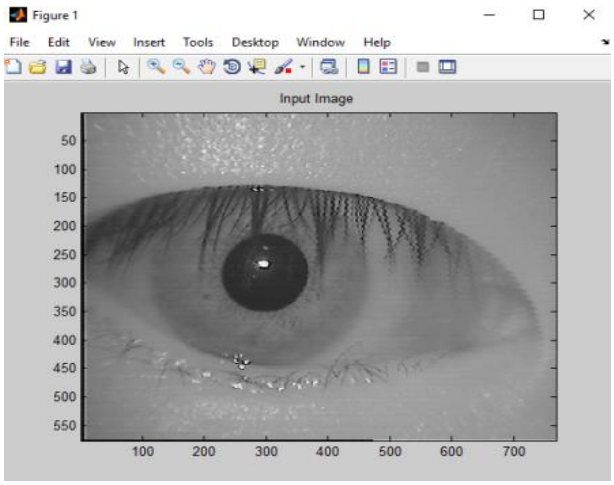

Figure 3: Original Image

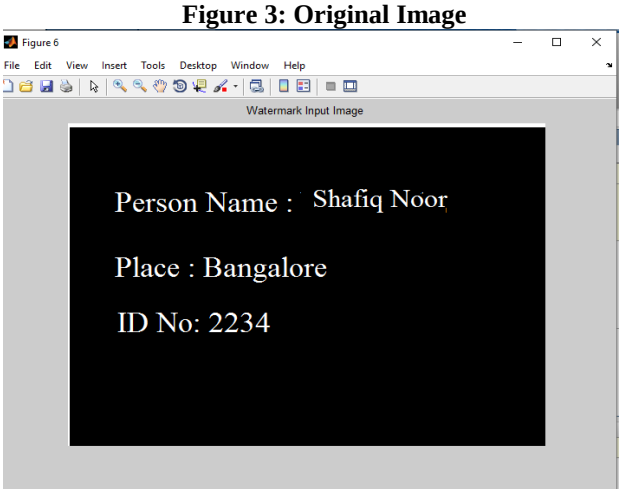

Figure 4: Watermark

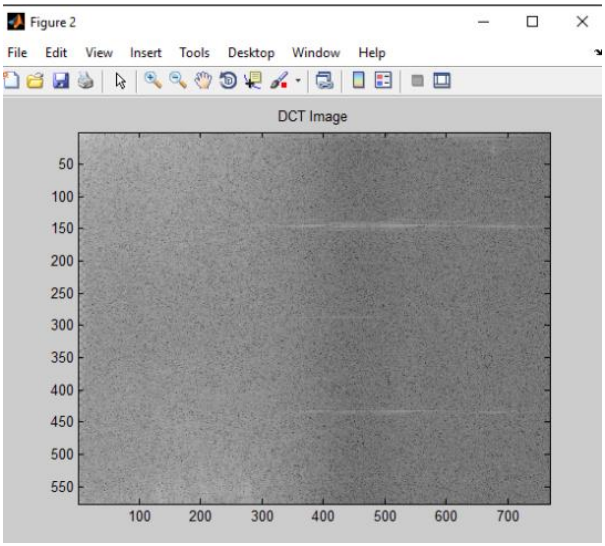

Figure 5: DCT Output

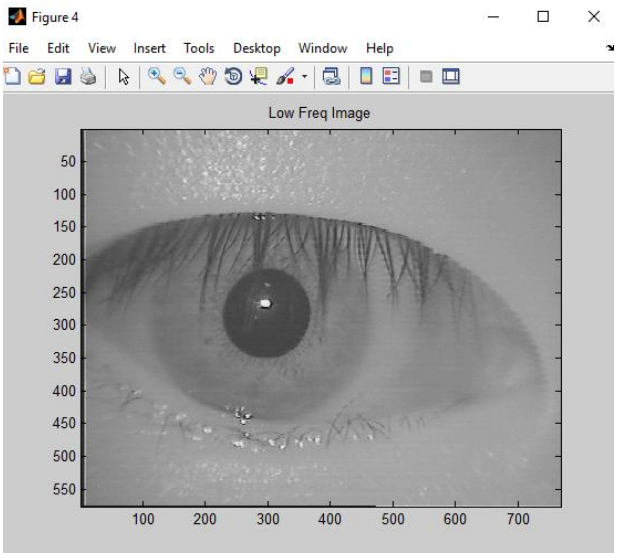

Figure 6: Low Frequency Image

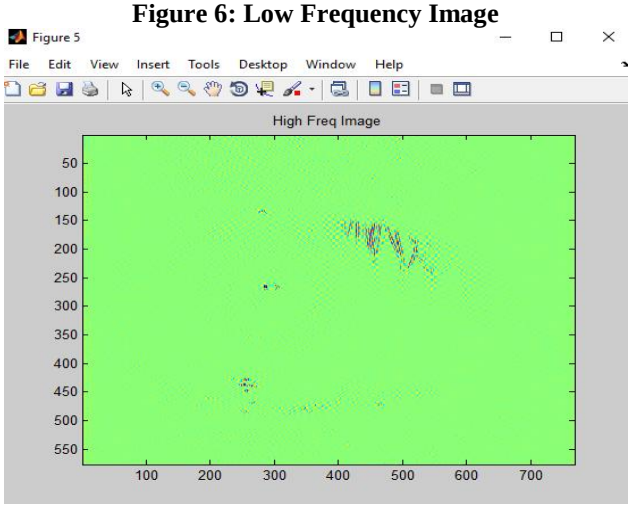

Figure 7: High Frequency Image

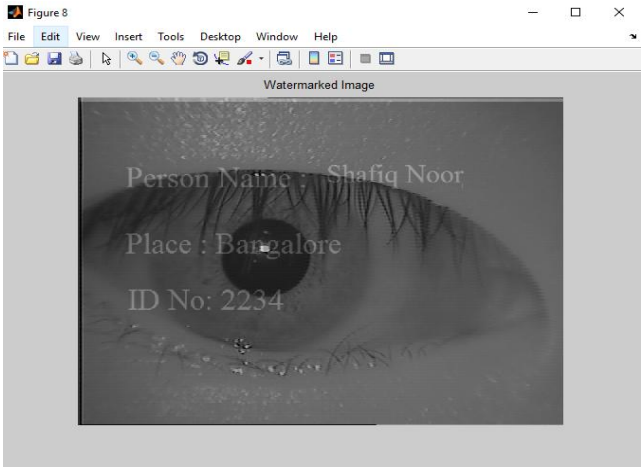

Figure 8 : Watermarked Image

B. Template Generation

The watermarked Image is converted into binary form as shown in Figure 9. The canny edge detection technique is used to generate gradient and orientation of the iris image as shown in Figure 10. For the edge detected image under goes Gabor convolve to generate polar array or the Template as shown in Figure 11.

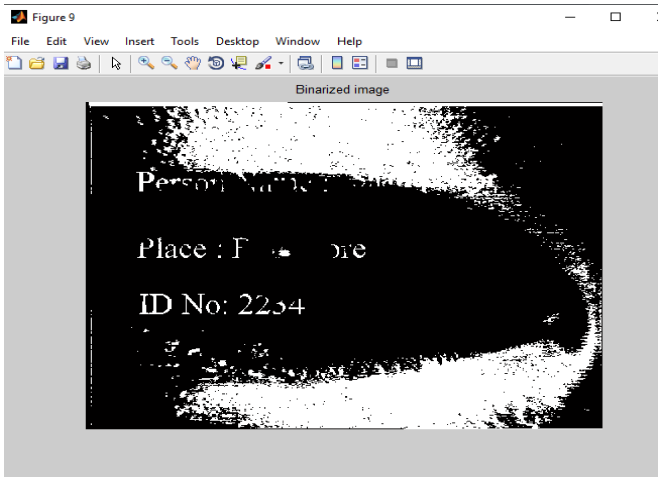

Figure 9: Binarized Image

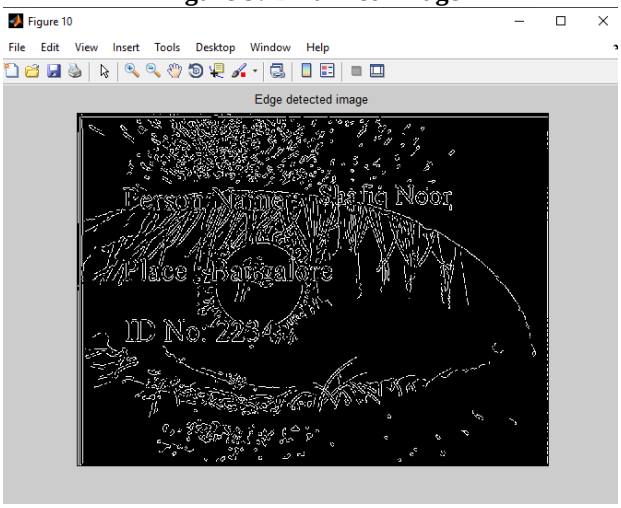

Figure 10: Edge Detected Image

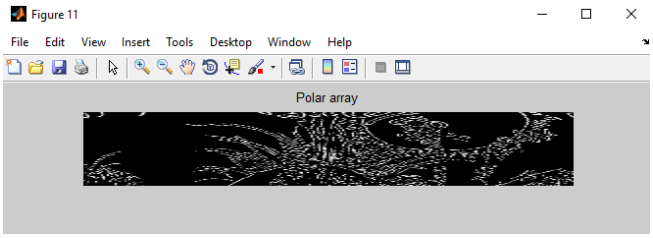

Figure 11: polar Array Or Template

C. Visual Cryptography

Visual Cryptography is a scheme where hidden messages are shared. Here, the template is divided into two share that is share 1 and share 2 which does not reveal any information as shown in Figure 12 and 13.The secret information can be revealed if they are stacked together. The two shares are overlapped together using Exclusive-OR (XOR) operation and thus the template is generated back as shown in Figure 14.

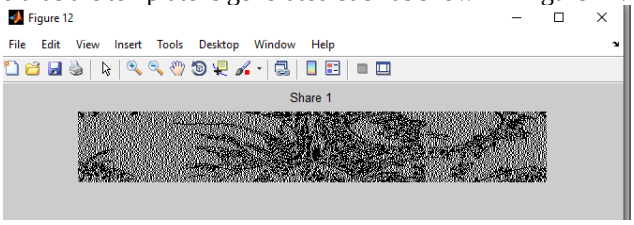

Figure 12: Represents Share 1

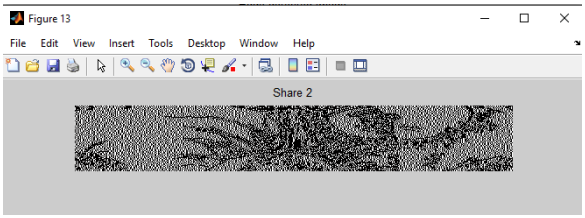

Figure 13: Represents Share 2

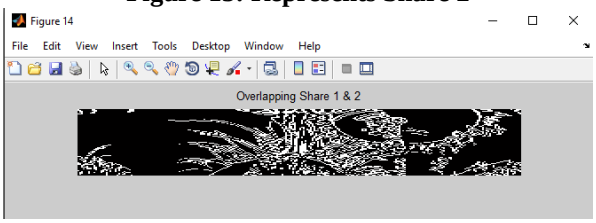

Figure 14: Represent the Overlapping of Two Shares

D. Template Matching

The Two dimensional correlation is performed for template matching. Here, a template generated from enrollment module and authentication module are matched. Thus, if both template are matched authenticated is displayed as shown in Figure 15 and person authorized and if it is not matched the unauthenticated is displayed as shown in Figure 16 and person is declared as unauthorized person.

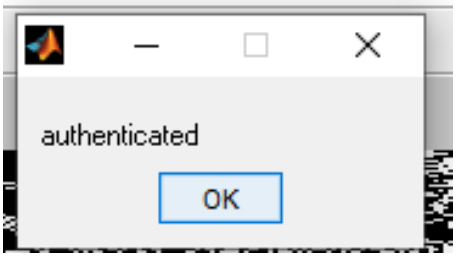

Figure 15: Authentication Displayed

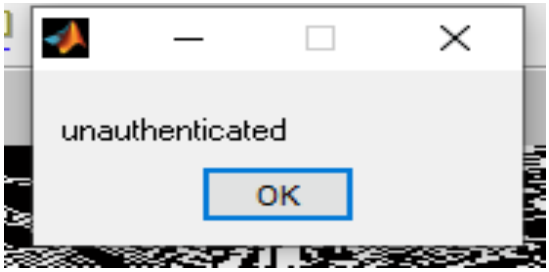

Figure 16: Unauthentication displayed

V.CONCLUSION

The proposed work present a novel schemes for the security of iris image and template protection and to solve the problem of biometric security. The first step is watermarking which is implemented to protect the integrity of biometric images. In particular, a watermark text image which accommodates the bio data of the person to be authenticated is embedded in the iris image by interchanging the middle band coefficients using DCT. Experimental results also illustrate that the DCT block are visually imperceptible and maintain the iris recognition performance. The proposed watermarking scheme is beneficial for the biometric system in number of ways. For example, the biometric traits and the bio information of an individual are usually stored in independent databases.

The second step achieved using Visual Cryptography (VC) technique to protect the iris template by decomposing the original iris template into two shares .An extra layer of security is provided to the iris template so that even if the share in the database or with the user is compromised, the original template cannot be retrieved. Hence, Authenticity of system is achieved.

REFERENCES

1. Cryptographic and Information Security Approaches for Image and Videos by S. Ramakrishnan 2019 by Taylor & Francis Group, LLC, CRC Press is an imprint of Taylor & Francis Group, an Information business, International Standard Book Number-13: 978-1-1385-6384-1.
2. Mohammed A. M. Abdullah, Satnam S. Dlay "A Framework for Iris Biometrics Protection: A Marriage Between Watermarking and Visual Cryptography" IEEE Transaction and content Mining, Volume 04 January 27, Year 2017.
3. Mohammed A. M. Abdullah, S.S. Dlay, W. L. Woo "Securing the Iris Image with robust Watermarking Algorithm based on Discrete Cosine Transform" IEEE International Conference on Computer Vision Theory and Application(VISAPP), Year 2015.
4. Mehran Andalibi, Damon M. Chandler "Digital Image Watermarking Via Adaptive Logo Texturization" IEEE International Transaction on Image Processing, Year 2015.
5. Xinpeng Zhang, Yanli Ren "Compressing Encrypted Image with Auxiliary Information" IEEE Transaction on multimedia, Year 2013.
6. Blossom Kaur, Amandeep Kaur " Steganographic Approach for Hiding Image in Discrete Cosine Transform Domain" International Journal of Advances in Engineering and Technology, July Year 2011.
7. B Swathi, T Madhavi Kumari "Iris Biometrics Security using Watermarking and Visual Cryptography" IEEE International Conference on Power, Control, Signal and Instrumentation Engineering (ICPCSI), Year 2018.

AUTHORS PROFILE

Shafiqua Noorain, is a M.Tech student in the department of Electronics and Communication Engineering at SDM College of Engineering and Technology, Dharwad, Karnataka, India. She obtained her Bachelor of Electronics and Communication Engineering from Anjuman Institute of Technology and Management, Bhatkal, Karnataka, India. She is pursuing Masters in Digital Electronics from SDMCET and has scored 8.34 CGPA till third semester.

Prof. Mala L Muddannavar is a assistant Professor in the department of Electronics and Communication Engineering at SDM College of Engineering and Technology, Dharwad, Karnataka, India. She obtained her Bachelor of Electronics and Communication Engineering from Government B D T Engineering College Davangere, Karnataka. Masters degree in Power Electronics from PDA College Gulbarga. She guided 50 U.G. and 08 P.G. students and published 02 papers at International Journal and 03 at National Conferences and life member of ISTE and IETE.