Iris Recognition Using Cancelable Biometrics Approach

Bhuvana M
Dept of Computer Science
Atria Institute of Technology

Abstract- *Iris recognition has been implemented successfully in many of the applications over the years. Internal Structure of a human eye consists of complex patterns that offers opportunities for personal identification. Iris recognition is one of the biometrics that offers best reliability and accuracy. This paper has proposed about the integration of iris recognition with cancelable biometrics with non-invertible transformation using encryption and decryption.*

Keywords- cancelable biometrics, Iris recognition, Non-invertible transformation, Support Vector Machine

I. INTRODUCTION

Biometrics is a study on ways to recognize and identify people based on high basis of one or more physical or behavioral characteristics such as fingerprint, retinal pattern and DNA [1]. There are two categories of biometrics namely, physiological and behavioral. Biometrics can provide replacement to username and password. Biometrics is used in applications that needs high level of security. Iris recognition is the most reliable biometrics of all the identification systems [2]. Iris of a human eye has complex patterns that can used for identification. Iris recognition is known for its accuracy and precision.

Iris recognition is been used currently in many real time applications such as border crossing, passenger screening at airports, unlocking a smartphone, e-Government. There is an addition of special feature to the iris recognition biometrics is non-invertible transformation to provide additional security to the system. The main aim of this implementation is to provide an highly secure biometric system.

II. CANCELABLE BIOMETRIC APPROACH

There exists a major disadvantage in biometric identification. Biometric systems sometimes become vulnerable to security threats. Unlike password based system, biometric system cannot be replaced if lost or compromised [3]. To overcome with the issue of security threats of biometrics there are template protection schemes such as cancelable biometrics and biometric cryptosystem.

In this paper the main focus is about cancelable biometric approach. Cancelable biometric is a biometric template protection scheme that intentionally and systematically distorts or alters the original biometric features in a repeated manner. So when the biometric template is compromised the new biometric template can be issued.

Non-invertible transformation is one the criteria for cancelable biometrics. Non-inevitability does not allow creating the original biometric data once it has been transformed. Thus, it helps in keeping biometric data secure.

III. METHODOLOGY

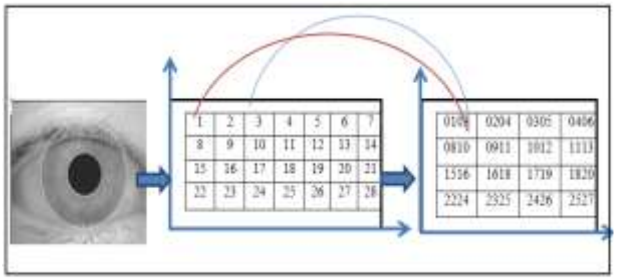
This section will be explaining about proposed cancelable biometric approach. If there is any compromise to any information in the storage, it will be on cancelable biometrics without affecting original biometrics [1].

First, the encryption process is detailed. The pseudo-code for encryption process is given below:

```
START

Read array and get the size;
    Loop {
    For each element in the row; {
Concatenate the first Odd element with next Odd element;
Store the odd value in ‘new array’;
Next; Concatenate the first Even element with the next even element;
Store Even value in ‘new array’;
                Repeat till the end of array; }}
                Output ‘new array’;
END
```

First step is to read the array that contains full size iris image namely {(0,0) – (x-1,y-1)}. Next, concatenate each ‘odd’ element with the next ‘odd’ element starting from left to right array for all ‘odd’ elements. Repeat the same procedure for ‘even’ elements.



1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

0104	0204	0305	0406
0810	0911	1012	1113
1516	1618	1719	1820
2224	2325	2426	2527

Fig. 1 Example of proposed encryption process [1].

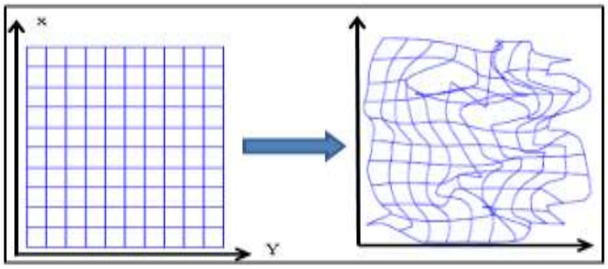


Fig. 2 Visualization upon completion of Encryption (Original array of iris image (left) and iris image encrypted (right))

Figure 1 depicts the example upon encryption while figure 2 shows the visualization upon completion of encryption.

The pseudo-code for the decryption process is as given below:

START

```
Read the ‘new array’ and get the size;
The size for the original array = (New array multiplied by 2)
Loop {
For each element in the row; {
Decoding strings the first Odd element with
next Odd element;
Store first two digits in the first Odd cell then
store second two digits in the next Odd cell;
Next; Decoding strings the first Even
element with next Even element;
Store first two digits in the fist Even cell then
store the second two digits in the next Even
cell;
Repeat till the end of array; }}
Output the ‘Original array’
```

END

In the decryption process, read the size of the array {(0,0) – (x-1, y-1) }. The size the new array will be multiplied by 2 since during encryption the size has been reduced to half. Next the first two digits in the first ‘odd’ cell are stored followed by the second two digits in the next ‘odd’ cell. Similar process is repeated for the ‘even’ element.

Figure 3 depicts the implementation of cancelable biometrics by integrating the module as shown in the shaded block [1]. All the other methods are similar as discussed in [4] except for the integration of cancelable biometrics method.

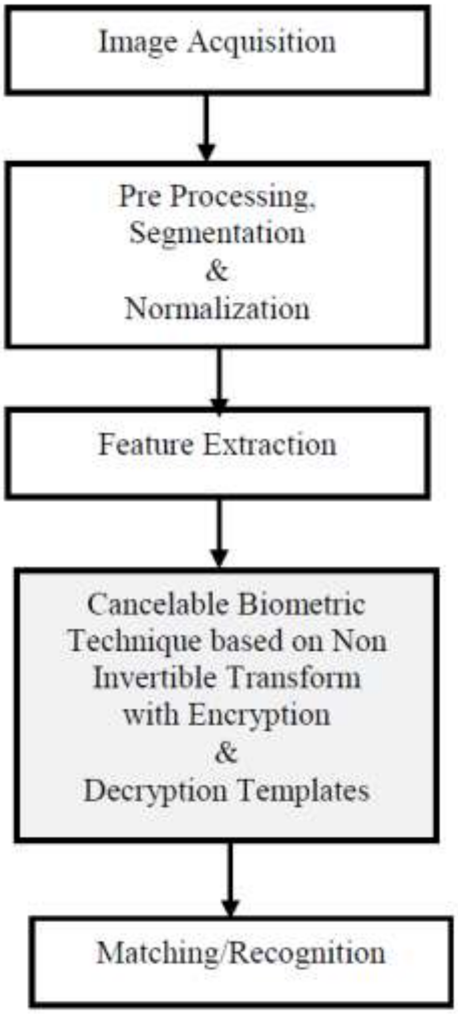


Image Acquisition
Pre Processing, Segmentation & Normalization
Feature Extraction
Cancelable Biometric Technique based on Non Invertible Transform with Encryption & Decryption Templates
Matching/Recognition

Fig. 3 Overview of Block Diagram for an Iris Recognition System

In a normal iris recognition system, the biometric templates are directly stored in the database and extracted for comparison. Hence the templates stored in the database is exposed to danger of any type of security breach.

IV. RESULTS

The results obtained by the implementation of cancelable biometrics is has been discussed in this section. Bath-A dataset comprising of iris images developed by the Department of Electronic and Electrical Engineering at the University of Bath U.K. Bath- A dataset consists of 20 images from each eye of 800 subjects. The majority of the database consists of iris images of students that are represented over 100 countries and staffs from university of Bath.

Totally 1000 samples of iris images are used, 500 images for training and another 500 images for testing. The performance of the biometric system is measured based in terms of False Acceptance Rate (FAR) and False Rejection Rate (FRR). Figure 4 and 5 shows the results for without cancelable biometrics and with cancelable biometrics. The two results have a difference in accuracy of 0.001% . The performance is tabulated in Table 1.

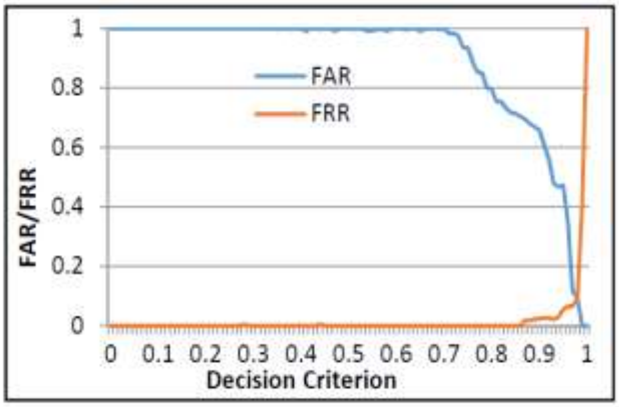


Fig. 4. FAR/FRR without Cancelable biometrics with iris Bath-A

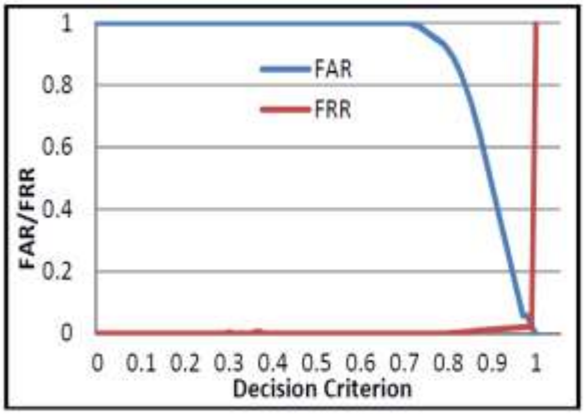


Fig. 5. FAR/FRR with Cancelable biometrics for Bath-A

Table 1. Performance measure based on FAR, FRR & RR with and without Cancelable biometrics

Category	Processing Time	Decision criterion	FAR	FRR	RR
Without	0.8 ms	0.77	0.29	0.29	99.41
With	0.9 ms	0.97	0.09	0.09	99.90

V. CONCLUSION

Cancelable biometrics helps in increasing the security of the biometric system. The performance of biometric system with and without cancelable biometrics is compared. It is worthy to integrate cancelable biometrics approach since it protects the biometric database and overall system.

VI. ACKNOWLEDGEMENT

I would like to express my sincere gratitude to the respected principal Dr. K.V. Narayanaswamy**,** for providing a congenial environment to work in. I also like to express my sincere gratitude to Dr. Aishwarya.P**,** Head of Department, Computer Science, for her continuous support and encouragement.

I am indeed indebted to Mrs. Pallavi Ncoordinator and Mrs .Hemalatha K N guide for their continued support, advice and valuable inputs during the course of this seminar work.

REFERENCES

[1] Musab A. M. Ali, Nooritawati Md Tahir, “Cancelable Biometrics for Iris Recognition”, https://ieeexplore.ieee.org/document/8405512

[2] C Raghavendra, A. Kumaravel, S. Sivasubramaniam, “Iris Technology: A Review on Iris Based Biometric Systems For Unique Human Identification”, https://ieeexplore.ieee.org/document/8186679

[3] Bismita Choudhury, Patrick Then, Biju Isaac, Valliappan Raman, Manas Kumar Haldar, “A Survey on Cancelable Biometrics Systems”, https://www.worldscientific.com/doi/10.1142/S0219467818500067

[4] Ali, M. A. M & Tahir, N.M, “Enhancement of pupil detection and performance comparison based on different Iris patterns”, https://ieeexplore.ieee.org/document/6738992