

School of Computing, Engineering
& Physical Sciences

**Computing and Information
Systems Journal**

Vol 22, No 3, 2018

Edited by Abel Usoro



© University of the West of Scotland, 2018

All authors of articles published in this journal are entitled to copy or republish their own work in other journals or conferences. Permission is hereby granted to others for the publication of attributed extracts, quotations and citations of material from this journal. No other mode of publication or copying of any part of this publication is permitted without the explicit permission of the University.

Computing and Information Systems is published normally three times per year, in February, May, and October, by the University of the West of Scotland.

The editorial address is Dr Abel Usoro, School of Computing, Engineering & Physical Sciences, University of the West of Scotland, High Street, Paisley PA1 2BE, UK.

Tel (+44) 141 848 3959; fax (+44) 141 848 3542, e-mail: cis@uws.ac.uk or abel.usoro@uws.ac.uk

Editorial Policy

Computing and Information Systems offers an opportunity for the development of novel approaches, and the reinterpretation and further development of traditional methodologies taking into account the rate of change in computing technology, and its usage and impact in organisations.

Computing and Information Systems welcomes articles and short communications in a range of disciplines:

- Organisational Information Systems
- Computational Intelligence
- E-Business
- Knowledge and Information Management
- Interactive and Strategic Systems
- Engineering
- E-Learning
- Cloud Computing
- Computing Science

The website for Computing and Information Systems is <http://cis.uws.ac.uk>

[An Improved Image Scrambling Algorithm Using \$\{2n-1, 2n, 2n+1\}\$](#)

Damilare Peter Oyinloye and Kazeem Alagbe Gbolagade 1

[Development of Iris Biometric Template Security Using Steganography](#)

Saheed Y. Kayode, Abdulsalam S. Olaniyi, Arowolo M. Olaolu and Akinbowale N. Babatunde 8

[Skin Diseases Predictive Model Using Individual Base and Ensemble Base Approach](#)

Tinuke Omolewa Oladele, Taye Oladele Aro and Adebisi Samuel Segun 18

[RSA Cryptosystem Encryption Based on Three Moduli Set With Common Factor \$\{2n+2, 2n+1, 2n\}\$](#)

Saheed Y. Kayode and Gbolagade K. Alagbe 27

Development of Iris Biometric Template Security Using Steganography

¹Saheed Y. Kayode, ²Abdulsalam S. Olaniyi, ³Arowolo M. Olaolu,
⁴Akinbowale N. Babatunde

¹Department of Computer Science, Al-Hikmah University, Ilorin, Nigeria.

¹yksaheed@alhikmah.edu.ng

^{2,3,4} Department of Computer Science, Kwara State University Malete, Nigeria.

suleiman.abdulsalam@kwasu.edu.ng, olliray2002@yahoo.com and akinbowale.nathaniel@kwasu.edu.ng

ABSTRACT

Purpose: Traditional iris segmentation methods and strategies regularly contain an exhaustive search of a large parameter space, which is sensitive to noise, time-consuming and no longer secured enough. To address these challenges, this paper proposes a secured iris template.

Approach: This paper proposes a technique to secure the iris template using steganography. The experimental analysis was carried out on matrix laboratory (MATLABR2015A) environment. The segmented iris region was normalized to decrease the dimensional inconsistencies between iris region areas with the aid of the usage of Hough transform (HT). The features of the iris were encoded by convolving the normalized iris region with 1D Log-Gabor filters in order to generate a bit-wise biometric template. Then, least significant bit (LSB) was used to secure the iris template. The Hamming distance was chosen as a matching metric, which gives the measure of how many bits disagreed between the templates of the iris.

Findings: The system operated at a very good training time and high level of conditional testing signifying high optimization with recognition accuracy of 92% and error of 1.7%. The proposed system is reliable, secure and efficient with the computational complexity significantly reduced.

Originality/value: The proposed technique provides an efficient approach for securing the iris template.

Keywords: Biometric, Iris Recognition System (IRS), Least significant bit (LSB), Hough Transform, 1D Log-Gabor filters.

Paper type: Research paper.

1 Introduction

Biometric techniques have come to be an outstanding option and secured means of authentication and successfully sustaining the emerging and rising ubiquitous computing (Saheed, Hambali, Adeniji and Kadri, 2017). Biometric recognition techniques have unfolded as a promising option for securing valuable information (Hambali and Jimoh, 2015). Instead of requiring identification cards, passwords or keys, biometrics are capable of identifying face, fingerprints, signatures, iris or retinas of an individual for convenient and easy verification (Simranjitkaur and Jasmeen, 2014).

First developed by Dr. John Daugman in the 1990s (Daugman, 1991), who got the idea from Flom and Safir's patented theoretical design, Iris Biometric identification systems have successfully been implemented and can be found in important applications around the world, ranging from offices to log entry in systems, to airports and passport offices (to associate visa details).

A lot of research effort on iris recognition has been done in the last few decades (Daugman, 1991; Iris recognition and identification, n.d, Daugman, 1993).

Boddeti and Kumar (2010) investigated the use of wave front-coded imagery for iris recognition. Daugman (2003) used a multi-scale quadrature approach to extract the texture phase structure information of the iris to produce 2,048-bit (256 bytes) iris code and used Hamming distance for matching. Wildes et al. (1996) presented a Laplacian pyramid for investigating the iris image, by applying normalized correlation and Fisher's linear discriminant for matching the iris. This paper proposes a method for iris template security using steganography technique.

The rest of this paper is organized in sections. Section 2 presents the material and methods.

Section 3 is the proposed system. In section 4, the results and discussion is presented; while in section 5, the conclusion is discussed.

2 Material and methods

2.1 Iris Dataset

The system will make use of the CASIA database as a total of 50 subjects will be administered with three (3) images for training and one (1) for testing the effectiveness of the system.

2.1.1 Segmentation

This stage is performed to eliminate the iris template from the eye image. The HT, a standard computer vision algorithm is employed here to get the centre coordinates and radius of the pupil and iris region.

2.1.2 Normalization

This is carried out to remap each pixel within the iris region to a pair of polar coordinates. It is performed based on the Daugman's rubber sheet model. Here, the centre of the pupil is regarded as the radial vector-circle and reference point via the iris region.

2.1.3 Feature extraction and selection

The iris biometric can be examined in several approaches to get its digital template T. In all cases, solutions depend on iris texture filtering, but they can vary significantly. The phase-based approach proposed by Daugman, will be used in this paper to extract relevant and important features.

2.1.4 Training

At this stage the extracted features will be used to train the system so as to formulate a machine based knowledge discovery for the iris pattern.

2.1.5 VC Module

This phase generates a secured iris template.

2.1.6 Least significant bit security

The extracted iris template is saved in the database and the use of built in pixel data, a random number is produced and is saved in the database as the extracted template image's title by the use of a steganography algorithm LSB to encode. This number is now given as input to the VC module that produced two shares, out of which one of the share is save in the database and the other share is save on the user ID card. This process ends the enrollment module.

3 System Architecture

Below is the application flowchart.

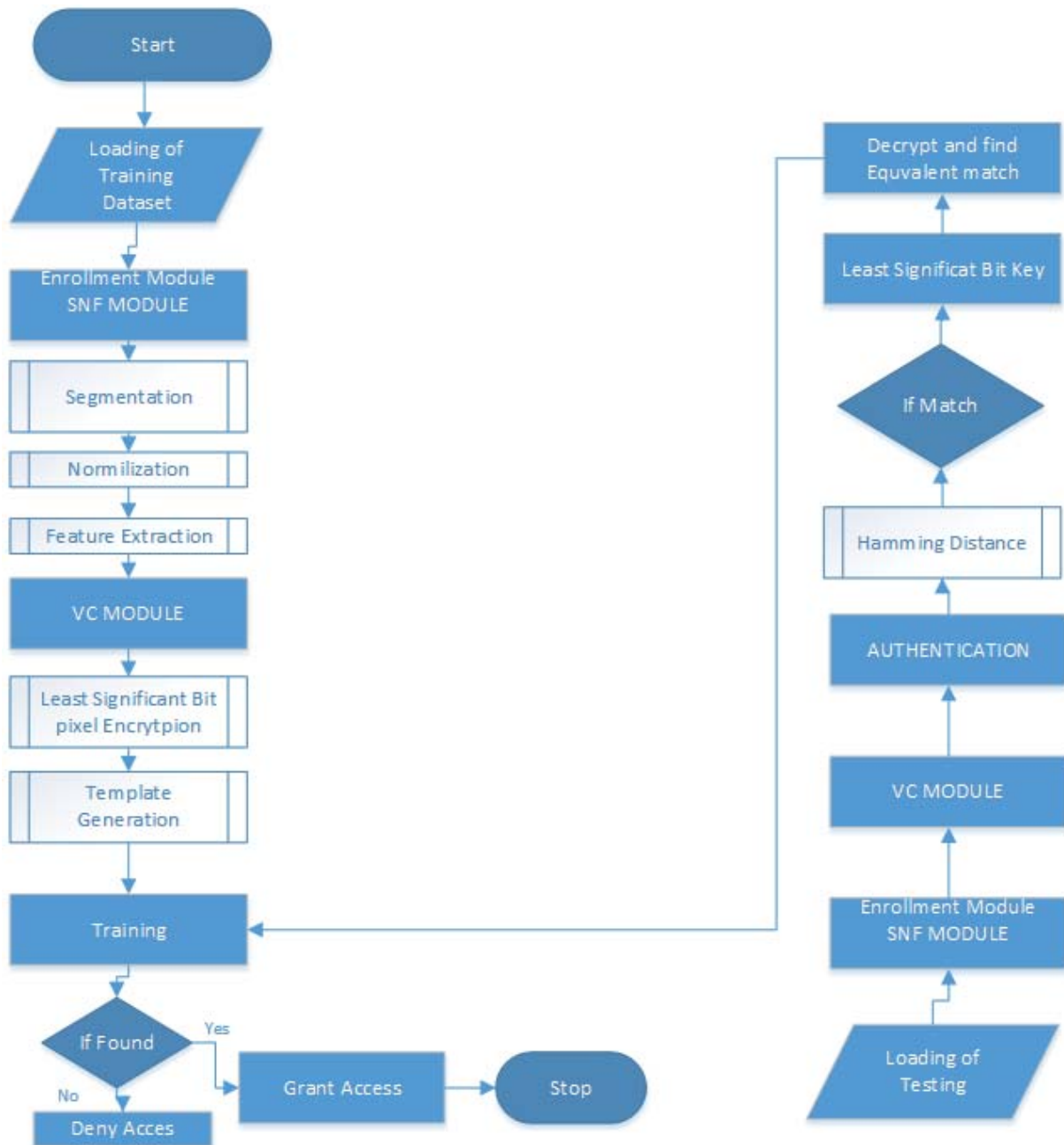


Figure 3.1 System Flow Chart

3.1 Authentication

For matching, hamming distance is the metric chosen for recognition. The result obtained is used as the goodness of match, with smaller values indicating better matches. If two patterns are

obtained from the same iris, the hamming distance between them will be close to 0 due to high correlation

3.2 Proposed System

The developed iris recognition system was tested with five databases from the Chinese Academy of Sciences' Institute of Automation (CASIA) Database. Four of the databases contain five samples with a grouping of three for training and two for testing. The fifth database contains two samples to show the response of the system when the selected sample has not been loaded to the system. The system was developed with respect to five Iris samples per class, three of the iris datasets are passed into the training set so as to build an experimental knowledge process for future query. Two subjects of each class was used to test the accuracy of the model as the two subjects are not passed into the training database but set aside for recognition modules.

Table 3.1 Database Parameter Settings

Parameters	Value
Number of training sets	60
Number of Testing Sets	24
Iris Per subject	6
Total Number of Class	10
Training Iris Per Class	6
Testing Iris Per Subject	2
Imposter	4
Total Iris Images	88

For each individual, we make use of six data sets for training, and two data sets which comprises of the left and right iris for testing. The total number of training sets is sixty; testing sets is 24 and it consists of 10 classes. Four of the testing images were imposter that is, the images were not found in the database.

4.0 Results and Discussion

4.1 Feature Extraction

The feature extraction is the generation of matrix that represents each iris image. This stage obtained the following image processing result.

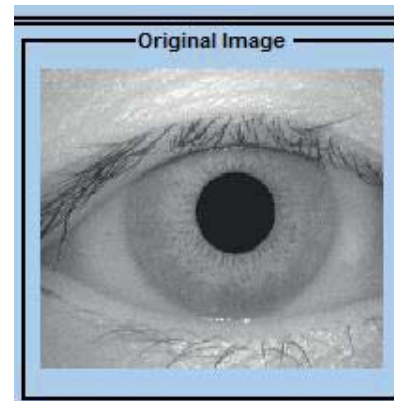


Figure 4.1 Fetching of Original Iris

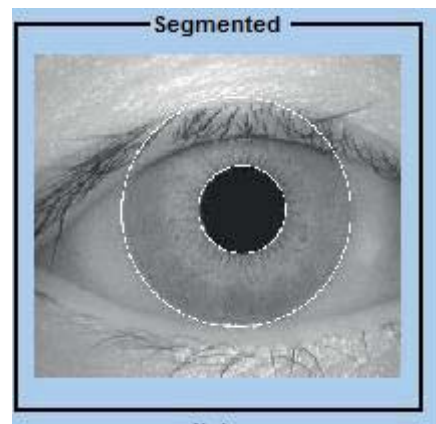


Figure 4.2 Iris Localization

The stage obtained a polarized normalized arrangement as well as reducing noise.

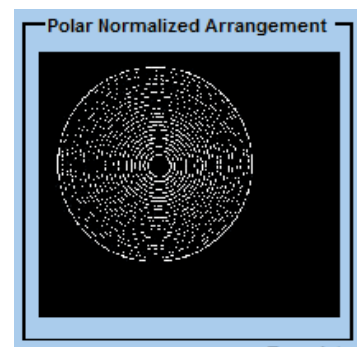


Figure 4.3 Polar Normalized Arrangement

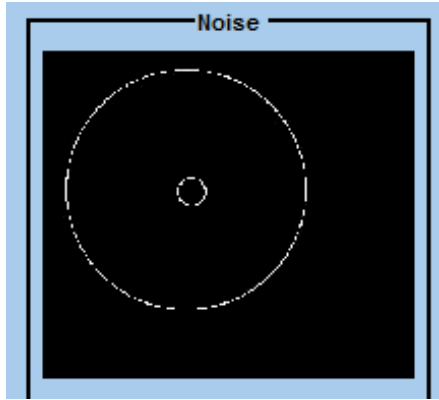


Figure 4.4 Polar Normalized Arrangement



Figure 4.5 Extracted feature template



Figure 4.6 Mask

The template and the mask are the last stage of feature extracted by the doughman integro operator algorithm. The template is encoded to be the cover message and the mask as the message image. The Hamming encoding works on the template and the mask to obtain a unique distance for each of the iris template for the purpose of recognition.

The page shows the different extraction processes, the segmentation, the normalization and the iris template. It shows the processes of feature extraction, the segmentation process, the polar normalization process, the noise removal process and the template of the iris generated.

4.2 LSB Steganography

The Least Significant bit helps to generate a secure template by taking the template image as the cover message and the mask as the message image there by creating a template that encodes the pixel value of the extracted feature. The results of this, is shown in the figure below:

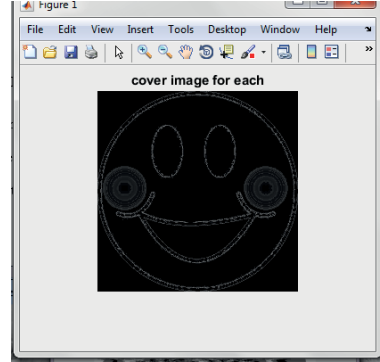


Figure 4.7 Stego Image

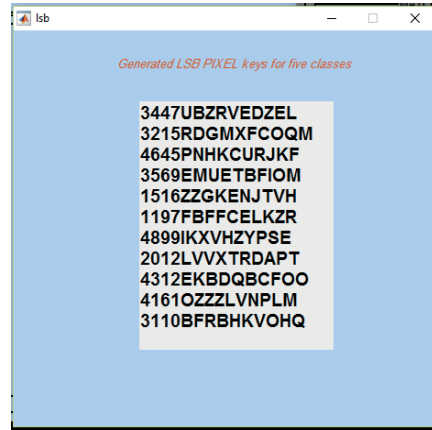


Figure 4.8 LSB Secured Keys

4.3 Trained Samples

The image was trained with the templates generated by the least significant bit cryptography so as to store up a template pattern for a particular iris thereby making it easy to recognize iris from one individual to the other.

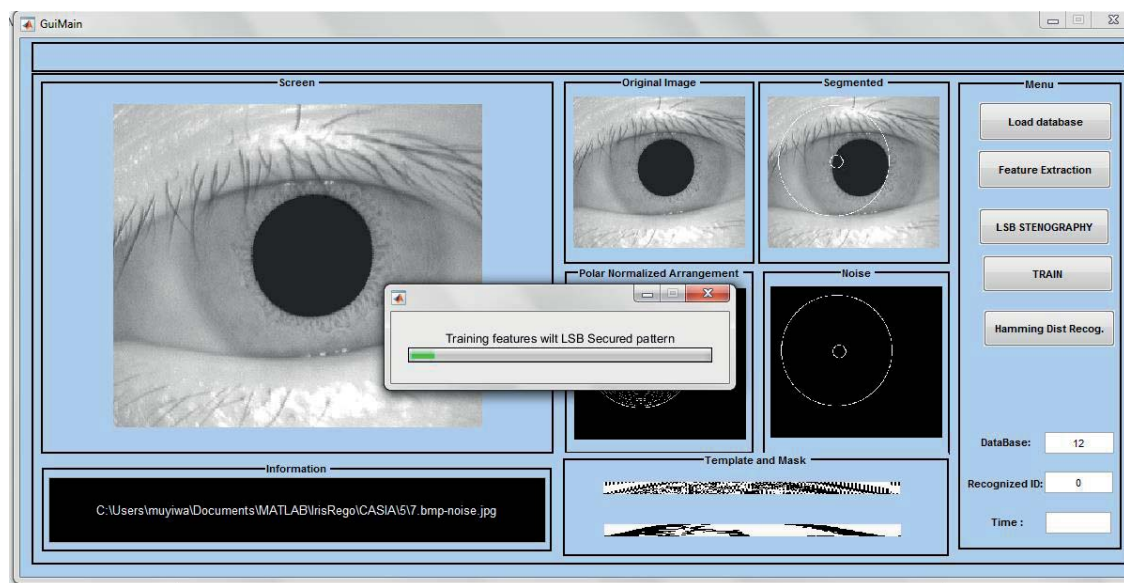


Figure 4.9 Training Sample Interface

4.4 Hamming Distance Recognition

This page shows the result of the testing of the images. The iris image was detected to recognised

correctly by correlating the iris probe image with the name of the class and subjecting it to the one located in the database.

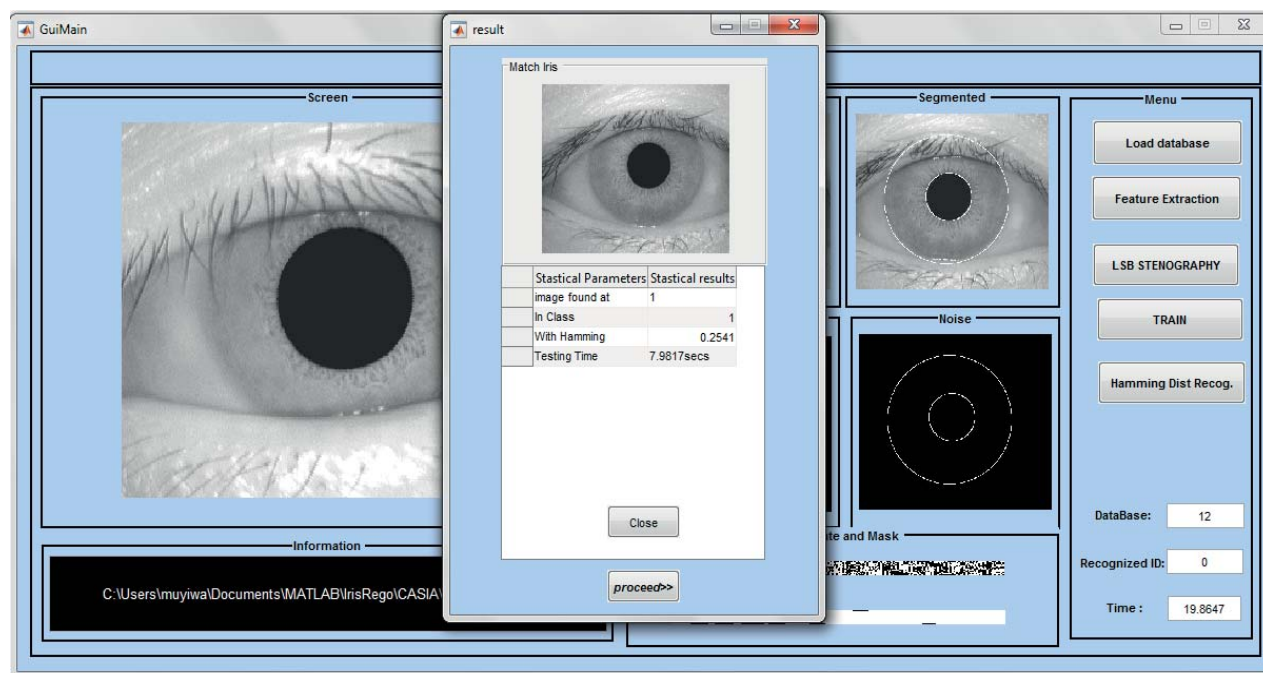


Figure 4.10 Testing Sample Interface

4.5 LSB Authentication Initiation

The least significant bits (LSB) key will be provided here for next stage to be accessed.

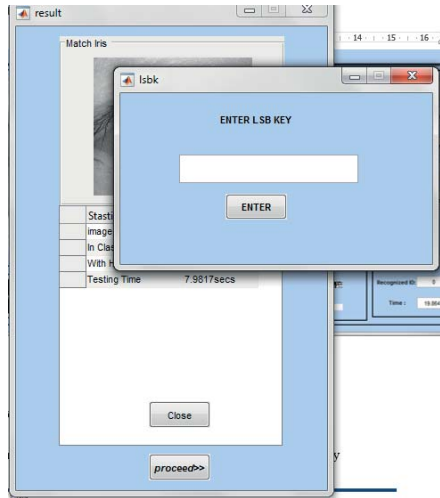


Figure 4.11 LSB Initiation Authentication

4.6 LSB Authentication

The figure below shows when the least significant bit (LSB) key is triggered to search the iris encoded database to find its match.

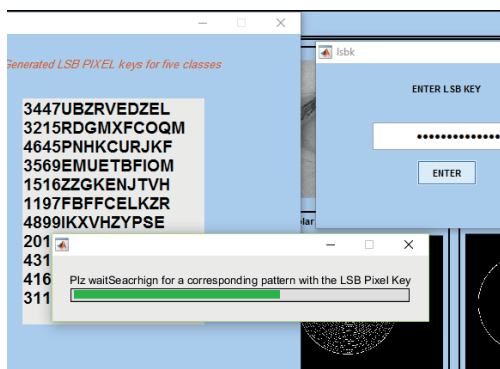


Figure 4.12 LSB Authentication

The figure below shows when the incorrect key is inserted

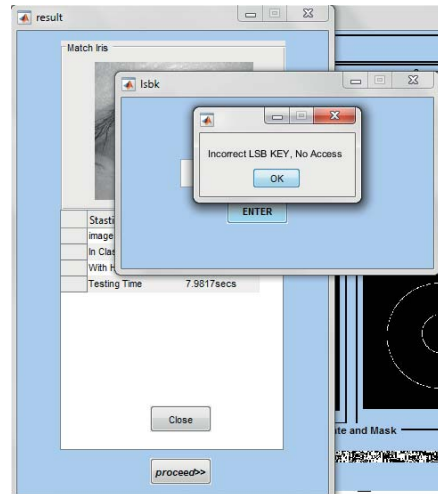


Figure 4.13 Blocked Authentication

The figure below shows when the incorrect key is inserted

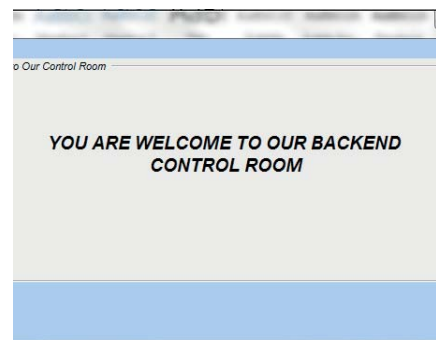


Figure 4.14 Access Grant

4.7 Presentation of recognition results

The recognised results are presented on Tables 4.1 and 4.2 as well as Figure 4.6.

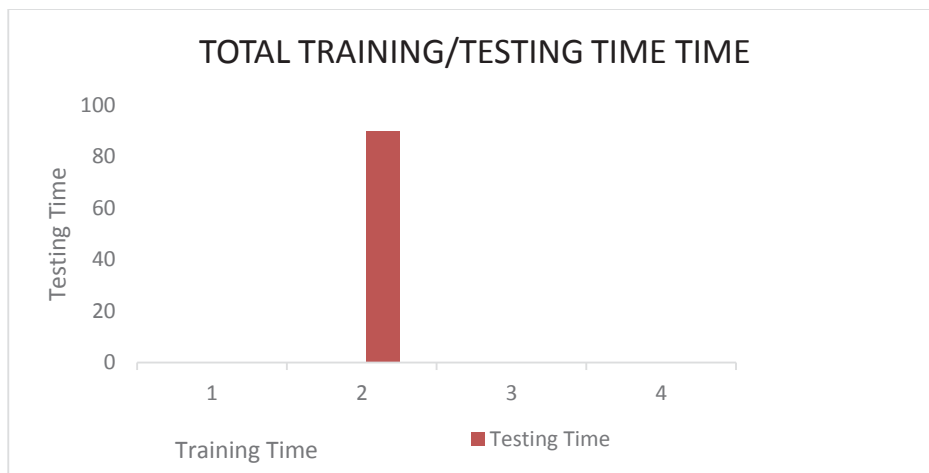
Table 4.1 Hamming Result Evaluation

Serial number	Class	Index of image recognized	Hamming distance	Testing time	Matched
1	1	1	0.2541	5.5567secs	Matched
2	1	3	0.2279	5.4991secs	Matched
3	2	2	0.1347	5.5254secs	Matched
4	2	2	0.1620	5.2367secs	Matched
5	3	1	0.2541	5.3485secs	Matched
6	3	3	0.2279	5.4863secs	Matched
7	4	2	0.1347	6.4831secs	Matched
8	4	2	0.1620	6.388secs	Matched
9	5	2	0.1620	6.3616secs	Matched
10	5	1	0.2541	4.9278secs	Matched
11	6	1	0.2541	4.5416secs	Matched
12	6	1	0.2541	5.4471secs	Matched
13	7	3	0.2279	4.676secs	Matched
14	7	2	0.1347	5.2055secs	Matched
15	8	2	0.1620	5.4618secs	Matched
16	8	1	0.2541	5.4533secs	Matched
17	10	3	0.2279	5.4833secs	Mismatched
18	9	2	0.1347	5.4022secs	Matched
19	10	2	0.1620	5.0313secs	Matched
20	1	2	0.1620	5.1632secs	Matched

Table 4.2 Imposter Result

Serial number	Class	Index of image recognized	Hamming distance	Testing time
21	No Class Found	No Image Found	No Value Found	5.1822secs
22	No Class Found	No Image Found	No Value Found	5.8061secs
23	3	0.1347	0.1347	5.0359secs
24	No Class Found	No Image Found	No Value Found	6.2378secs

The system operated at a very good training time and high level of conditional testing, signifying high optimization as shown in figure 4.6.

**Figure 4.6: Training and testing time**

5 Conclusion

This paper proposed an iris biometric system security based on steganography. The LSB algorithm was chosen to secure the iris template. The proposed system operated at a very good training time. The 1 D log-Gabor filter was adopted for feature extraction and Hamming distance was chosen and used as a matching metric. The proposed system is efficient, reliable and provides a better security.

References

- Boddeti, V. N. and B. V. K. Vijaya Kumar (2010) Extended-Depth-of-Field Iris Recognition Using Unrestored Wavefront-Coded Imagery *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 40(3), 495-508.
<http://www.sinobiometrics.com/resources.htm> (Accessed on 15 January 2017).
- Daugman, J. (1993) High Confidence Visual Recognition of Persons by a Test of Statistical Independence *IEEE Trans. Pattern Analysis and Machine Intelligence*, 15(11), 1148-1161.
- Daugman, J. (2003) Demodulation by Complex-Valued Wavelets for Stochastic Pattern Recognition, *Int'l J. Wavelets, Multiresolution and Information Processing*, 1(1), 1-17.
- Daugman, J. (2004) "How Iris Recognition Works", *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 21-30.
- Daugman, John (1991) Biometric Personal Identification System Based on Iris Analysis,

- <https://patents.google.com/patent/US5291560A/en> (Accessed on 17 January 2017).
- Hambali, M. A. and Jimoh, R. G. (2015) Performance Evaluation of Principal Component Analysis and Independent Component Analysis Algorithms for Facial Recognition, *Journal of Advances in Scientific Research & Its Application (JASRA)*, 47–62.
- Iris Recognition and Identification, Retrieved 30th July 2017 from <http://www.iris-recognition.org/>, 2017 (accessed on 17 January 2017).
- Saheed, Y. K., Hambali, M. A., Adeniji, I. A. and Kadri, A. F. (2017) Fingerprint Based Approach for Examination Clearance in Higher Institutions *FUOYE Journal of Engineering and Technology*, 2(1), March, 47-50.
- Simranjit, Kaur and Jasmeen T. (2014) Survey of Different Approaches in Biometric Iris Recognition System, *International Journal of Advanced Research in Computer Science and Software Engineerin*, 4(7), 768-771.
- Wildes, R., Asmuth, J., Green, G., Hsu, S., Kolczynski, R., Matey, J. and McBride, S. (1996). A Machine-Vision System for Iris Recognition, *Machine Vision and Applications*, 9, 1-8.