CRYPTOGRAPHY AND ERROR CORRECTION CODE FOR IRIS BIOMETRIC RECOGNITION SYSTEM

[1] A.Sundar Raj, [2] C. Deepa, [3] M. Jagathiya
[1] Associate Professor,
[1] E.G.S. Pillay Engineering College, Nagapattinam, India
[2,3] E.G.S. Pillay Engineering College, Nagapattinam, India

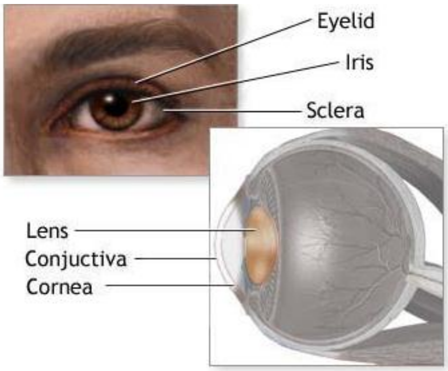
---***---

Abstract: Digital image processing is the use of computer algorithms to perform image processing on digital images. As a subcategory or field of digital signal processing, digital image processing has many advantages over analog image processing. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the build-up of noise and signal distortion during processing. Since images are defined over two dimensions (perhaps more) digital image processing may be modeled in the form of multi dimensional system.

Digital image processing allows the use of much more complex algorithms for image processing and hence can offer both more sophisticated performance at simple task and the implementation of methods which would be impossible by analog means.

INTRODUCTION TO IRIS RECOGNITION SYSTEM

A biometric is unique among all individuals, it is not possible to use biometric as a direct cryptography key for the system due to the difference bits occur in the template during every authentication. Biometric iris images or templates are variable by nature which means each new biometric sample is always different. Noises and error may occur in the captured image due to burst or background error and hence the generated template is different during every authentication. There is also awareness concerning the privacy and the security of personal information due to the storage of the biometric templates. The loss or compromise of biometric templates may end up to unusable biometric. Human physiological biometric is hardly change or do modification if the image template has been stolen or compromised.



iris recognition system

This paper presented an ideal iris biometric authentication system which fulfils the important properties such as non-repudiation, privacy, and security. The important idea to achieve these properties is by combining both the iris biometrics and password. The intra personal variation (noises and error occurred in the genuine iris code) is solved by introducing the Error Correction Codes (ECC). The Error Correction Codes helps to correct errors on the genuine identification making the threshold value to be smaller which significantly helps in improving the user separation of the impostor verification. In this paper, two different distance metric function used in the template matching process will be compared. The next section provides the review of the literature work, followed by the methodology and experimental results. Finally, the last section gives the conclusion remarks and the future work of this paper.

IMAGE SEGMENTATION AND PRIMAL SKETCH

There have been numerous research works in this area, out of which a few have now reached a state where they can be applied either with interactive manual intervention (usually with application to medical imaging) or fully automatically. The following is a brief overview of some of the main research ideas that current approaches are based upon.

The nesting structure that Wit kin described is, however, specific for one-dimensional signals and does not trivially transfer to higher-dimensional images. Nevertheless, this general idea has inspired several other authors to investigate coarse-to-fine schemes for image segmentation. Koenderink proposed to study how iso-intensity contours evolve over scales and this approach was investigated in more detail by Lifshitz and Pizer.

Unfortunately, however, the intensity of image features changes over scales, which implies that it, is hard to trace coarse-scale image features to finer scales using iso-intensity information. Lindeberg studied the problem of linking local extrema and saddle points over scales, and proposed an image representation called the scale-space primal sketch which makes explicit the relations between structures at different scales, and also makes explicit which image features are stable over large ranges of scale including locally appropriate scales for those.

Bergholm proposed to detect edges at coarse scales in scale-space and then trace them back to finer scales with manual choice of both the coarse detection scale and the fine localization scale. Gauch and Pizer studied the complementary problem of ridges and valleys at multiple scales and developed a tool for interactive image segmentation based on multi-scale watersheds.

The use of multi-scale watershed with application to the gradient map has also been investigated by Olsen and Nielsen and been carried over to clinical use by Dam Vincken et al. proposed a hyperstack for defining probabilistic relations between image structures at different scales. The use of stable image structures over scales has been furthered by Ahuja and his co-workers into a fully automated system.

More recently, these ideas for multi-scale image segmentation by linking image structures over scales have been picked up by Florack and Kuijper. Bijaoui and Rué associate structures detected in scale-space above a minimum noise threshold into an object tree which spans multiple scales and corresponds to a kind of feature in the original signal. Extracted features are accurately reconstructed using an iterative conjugate gradient matrix method.

VARIOUS BIOMETRIC TECHNOLOGIES

There were many biometric technologies available but they have some disadvantages, there are,

3.2.1 Facial Recognition

3.2.2 Finger Print Technology

3.2.3 Hand Geometry.

3.2.4 Iris Technology

Facial Recognition:

- ❖ Failure to enroll: **1%**
- ❖ Moderate difficult to use
- ❖ Reenrollment may be necessary(age ,hair)
- ❖ No interoperability

Finger Print Technology

- ❖ False accept rate:**1:100000**
- ❖ Failure to enroll: **1%-2%**

❖ Difficult to use

❖ Reenrollment may be necessary (physical ,disease)

❖ No interoperability.

3.2.3 Hand Geometry

❖ False accept rate: **1:100000**

❖ Failure to enroll: **1%**

❖ Moderate difficult to use

❖ Reenrollment may be necessary(age, physical work)

❖ No interoperability.

3.2.4 Iris Technology

❖ Iris of the same person captured in different time may differ due to signal noise or Environment problem.

❖ Due to iris camera problem.

Different iris patterns

THE METHODOLOGY

This section discussed the overall process for the iris biometric verification. It consists of two main phases which is the enrollment and verification process. Dataset and the template matching distance metric that is use for the experimental result will be describe in detail in this particular section.

FRONT END DESIGN

We are implementing our project using matlab programming methodology with "C" codings. Our output operation was made by GUI (Graphical User Interface) because it is easy to understand the output operation of figures andalso we use the normal matlab output figurre window.

Cryptography and error correction code for biometric Iris Recognition system has some advantages over other biometric and iris biometric techniques.

❖ It provides high security

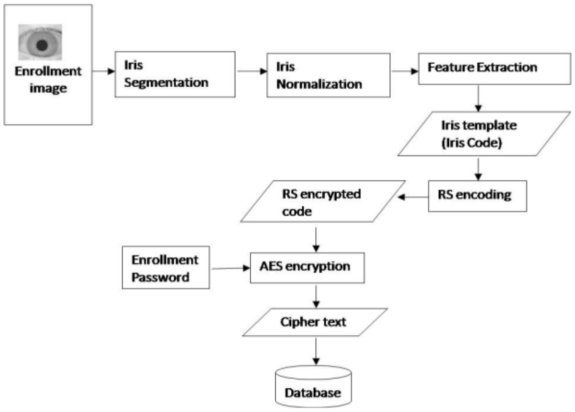
❖ Complete fraud detection during enrollment

❖ Complete privacy though anonymous authentication

❖ High speed even when using database of million records

- Search speed: **100000** iris codes per seconds.
- Error correction code is used to reduce variability or noise of the Iris Data.
- The above Proposed approach is tested to use of two different metric distance measurement's such as "HAMMING DISTANCE" and "WEIGHTED EUCLIDEAN DISTANCE.

Enrollment Process



Flow chart of enrollment process

Enrollment process consists of following steps:

Step 1: Iris is extracted through iris Segmentation, IrisNormalization and Feature Extraction process to generate theiris template and to produce the iris binary code.

Step 2: The binary code for the iris image will then undergo the Reed Solomon Code Encoding Process.

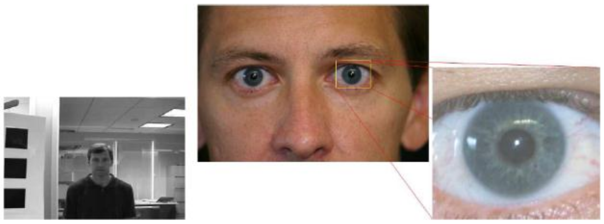
Step 3: A RS Code is then generated after the enrolment process.

Step 4: The RS Code is then encrypted with the enrolment password using Advanced Encryption Standard Cryptography Algorithm to generate a cipher text.

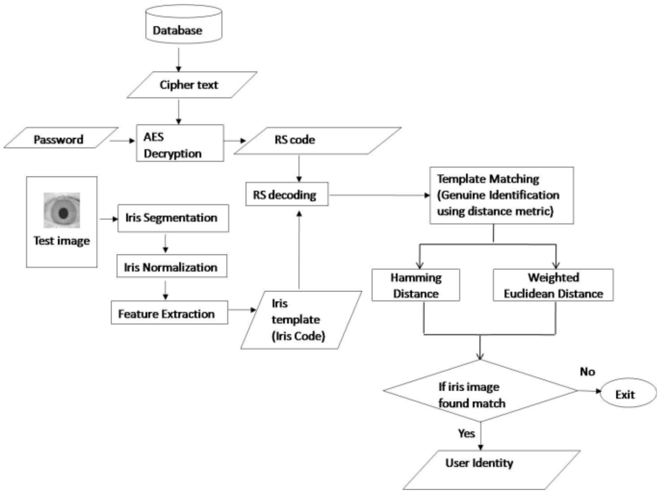
Step 5: The generated cipher text is then stored into the data base.

4.3.2 Verification process:

Test image:



test image



Flow chart of verification process

Verification Process consists of following steps:

Step 1: A tested iris image is extracted using iris segmentation, normalization, and feature extraction to obtain the iris binary code and the iris template of the testing iris image

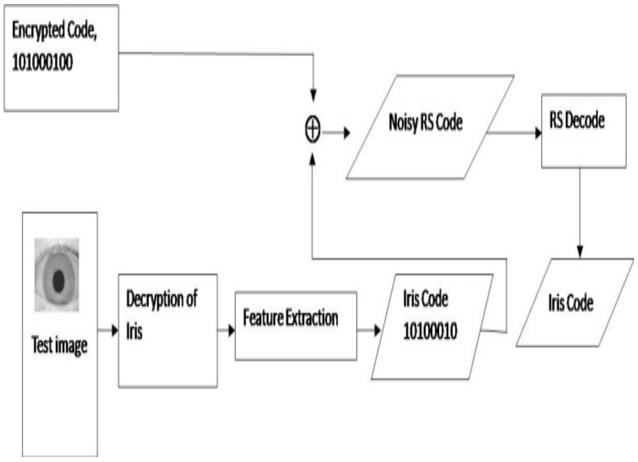
Step 2: A password is required to authenticate the user, and this password is use to decrypt with the cipher text obtain from the database using AES decryption process to obtain the RS code.

Step 3: The RS code is then use to decode with the testing iris template code to obtain the enrolled iris template code using Reed Solomon decoding process. Reed Solomon decoding process is also used to correct the error of the testing iris template code in this process.

Step 4: The both iris template code is then undergoes the template matching process using Distance Metric Function (Hamming Distance, Weighted Euclidean Distance).

Step 5: If the iris template is found match under a corresponding threshold value, the user will be authenticate, otherwise the system will be exit.

Reed Solomon code:



Block Diagram of Reed Solomon Error Correction Process on Iris Verification

DATA BASE

Datasets used for the experimentation is CASIA Iris Database Version 1.0. The Chinese Academy of Sciences – Institute of Automation (CASIA) eye image database version 1.0 contains 756 grayscale iris images taken from 108 candidates and with 7 different images for each candidate collected in two sessions

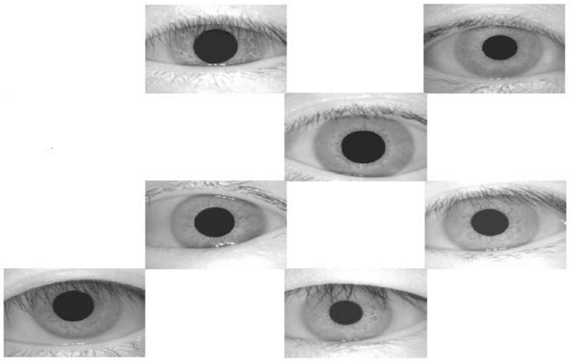


Figure (5.1) Data base diagram

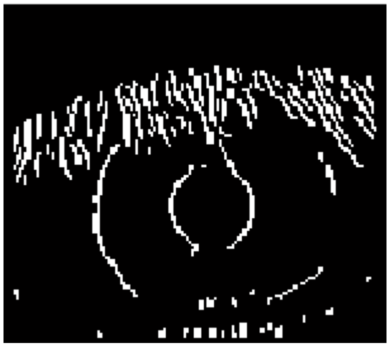
Image captured is especially for iris recognition research using specialized digital optics developed by the National Laboratory if Pattern Recognition, China and also educational purpose. All iris images are 8 bit gray-level JPEG files, collected under near infrared illumination. This data base is used for reference only.

Image segmentation

Segmentation divides an image into its constituent regions or objects. Segmentation of images is a difficult task in image processing. Still under research. Segmentation allows to extract objects in images. Segmentation is unsupervised learning. Model based object extraction, e.g., template matching, is supervised learning.

Method of segmentation system:

The first action of Preprocessing is to determine iris edges include inner (with pupil) and outer (with sclera) edges. Iris can be introduced as follows: a diaphragm with rich texture encircling a circular region (pupil). Both the inner boundary and the outer boundary of a typical iris can approximately be taken as circles but these two circles are usually not co-centric.

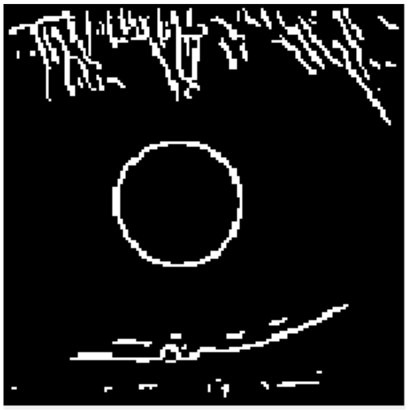


Iris Edge Detection Diagram

There are two brilliant characteristics in iris which are useful in detection process. The more darkness of pupil region versus other parts and having medium gray level of iris district that limited between pupil (very low) and sclera (very high) levels. So we design a method for detecting these two boundaries. Mathematical morphological operators with a suitable threshold are applied to iris images. This algorithm is very rapid compared to Hough transform and precise. The pupil and limbus centers with respect radiuses are calculated.

Iris boundary Edge Detection:

To get the outer boundary (with sclera) first the preprocessed image is filtered with Extended-Minima (EM) morphology operator. EM transform is the regional minima of the H-minima transform. H-Minima transform suppresses all minima in the intensity image whose depth is less than a scalar. Regional minima are connected components of pixels with the same intensity value whose external boundary pixels all have a greater value than a scalar.

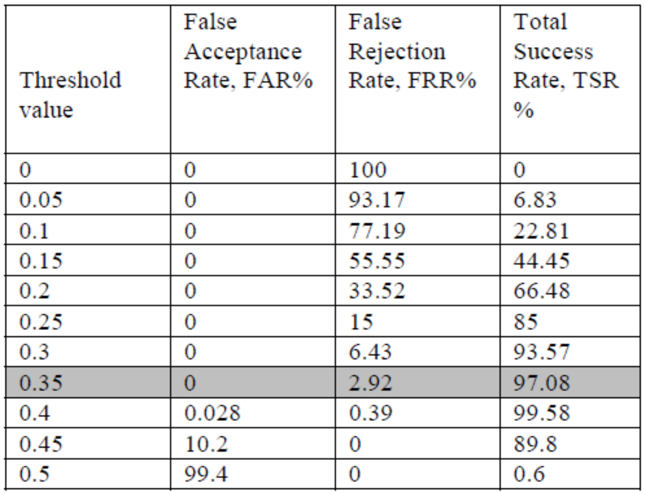


Iris boundary Edge Detection We used 8-connected neighborhoods in this process. By choosing an appropriate scalar in EM transform, a perfect edge of outer boundary is gotten. This scalar is chosen with trial and error.Now we encircled a circle unto the outer boundary with the best fitting. The XOR of these two images will generate the whole iris edge image

Iris Normalization

The variant conditions of image capturing can influence the size of iris which must be processed in the system.To compensate the stretching of the iris texture as the pupil changes in size, and have a new model of iris which removes the non-concentricity of the iris and the pupil. We used modified Daugman's Cartesian to polar transform. This transformation (Daugman rubber sheet model) will project the iris disk to a rectangular region with prefixed size. The following formulas perform the transformation,

DIFFERENT THRESHOLD VALUES USING HAMMING DISTANCE



Threshold value	False Acceptance Rate, FAR%	False Rejection Rate, FRR%	Total Success Rate, TSR %
0	0	100	0
0.05	0	93.17	6.83
0.1	0	77.19	22.81
0.15	0	55.55	44.45
0.2	0	33.52	66.48
0.25	0	15	85
0.3	0	6.43	93.57
0.35	0	2.92	97.08
0.4	0.028	0.39	99.58
0.45	10.2	0	89.8
0.5	99.4	0	0.6

Different threshold value using hamming distance

The FAR and FRR on different threshold values for the measurement using Hamming Distance. From the above result, 0.35 gives the best FAR and FRR and hence, it is chosen as the threshold value for this proposed iris cryptography system.

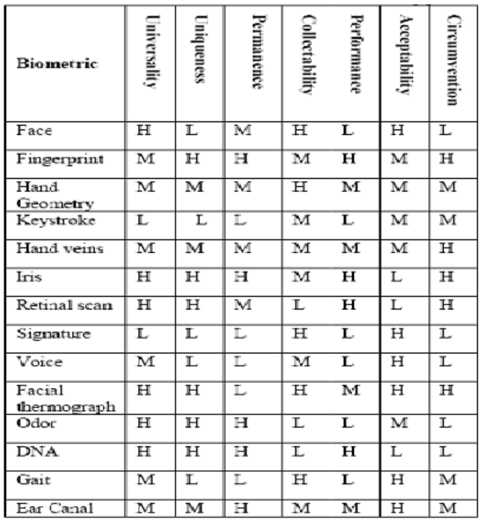
Although threshold value of 0.4 gives result of higher total success rate, it is not chosen because the system not allowed successful decryption from imposter, therefore the FAR must be 0.

Simple GUI display

A graphical user interface (GUI) is a graphical display that contains devices, or components, that enable a user to perform interactive tasks. To perform these tasks, the user of the GUI does not have to create a script or type commands at the command line. Often, the user does not have to know the details of the task at hand. The GUI components can be menus, toolbars, push buttons, radio buttons, list boxes, and sliders—just to name a few. In MATLAB, a GUI can also display data in tabular form or as plots, and can group related components. The following figure illustrates a simple GUI.

- ❖ The GUI contains An axes component.
- ❖ A pop-up menu listing three data sets that correspond to MATLAB functions: peaks, membrane, and sinc.
- ❖ A static text component to label the pop-up menu.
- ❖ Three buttons that provide different kinds of plots: surface,mesh, and contour.

COMPARISION OF IRIS RECOGNTION WITH OTHER BIOMETRIC SYSTEMS:



Biometric	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke	L	L	L	M	L	M	M
Hand veins	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial thermograph	H	H	L	H	M	H	H
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear Canal	M	M	H	M	M	H	M

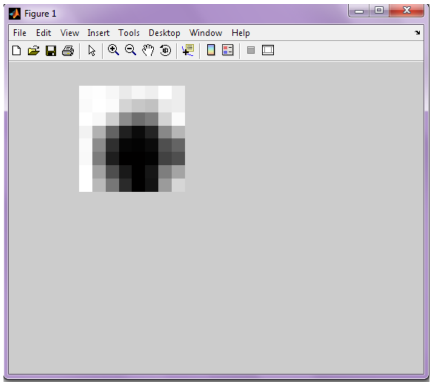
H=High, M=Medium, L=Low

APPLICATIONS:

- ❖ Passport control.
- ❖ Computer login control.
- ❖ Secure electronic banking, bank ATM, credit cards.
- ❖ Premises access control.
- ❖ Border crossing, airport , mobile phones.
- ❖ Internet security.
- ❖ Anti-terrorism.
- ❖ Online shopping.
- ❖ Building security.
- ❖ Data security.
- ❖ Computer and access network identification.
- ❖ Credit card authentication.
- ❖ Automobile ignition.

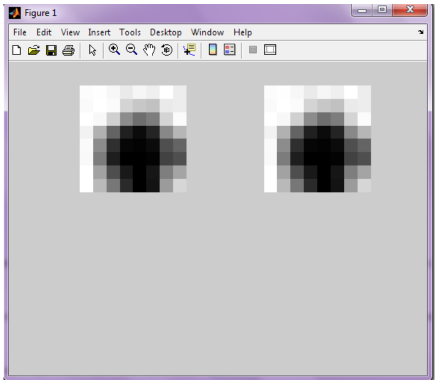
ENROLLMENT PROCESS

Reed solomon encoding and decoding



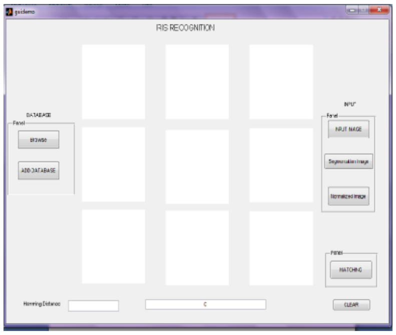
Reed solomon encoding

AES encryption



AES encryption

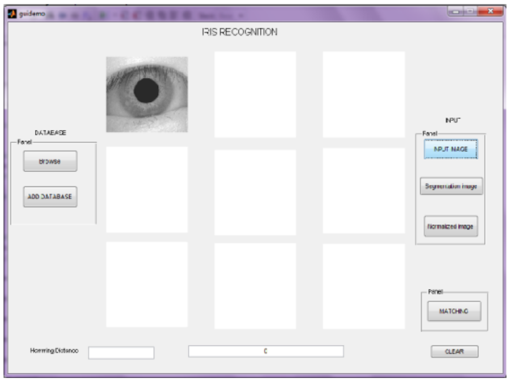
General GUI window



Input GUI Window

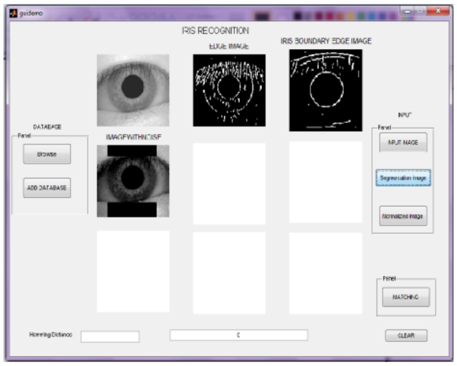
VERIFICATION PROCESS FOR AUTHENTICATION:

Input iris image



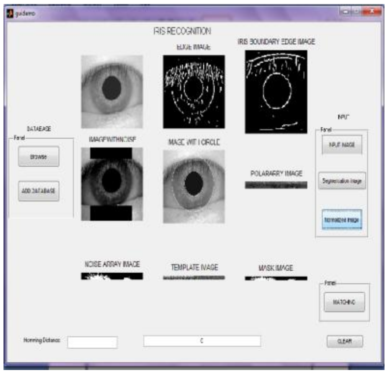
Input iris image diagram

Iris segmentation process



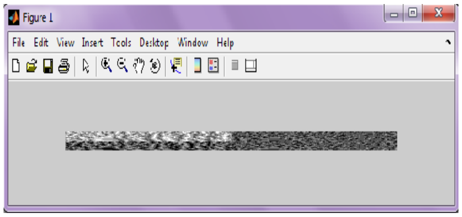
Iris segmentation process diagram

Iris normalization image



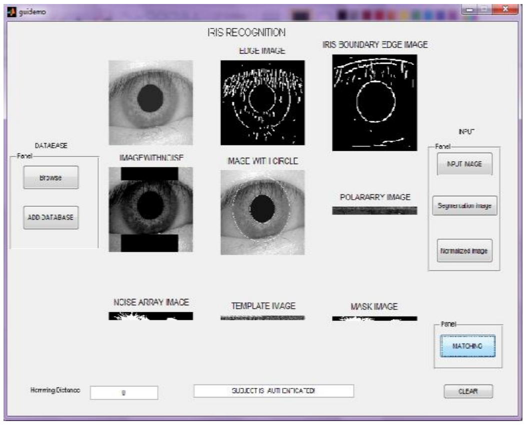
C

Template image



Template image

Matching process



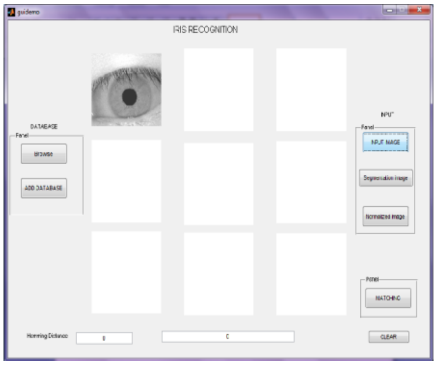
0

SUBJECT IS AUTHENTICATED!

Matching process diagram

VERIFICATION PROCESS FOR NON-AUTHENTICATION:

Input iris image

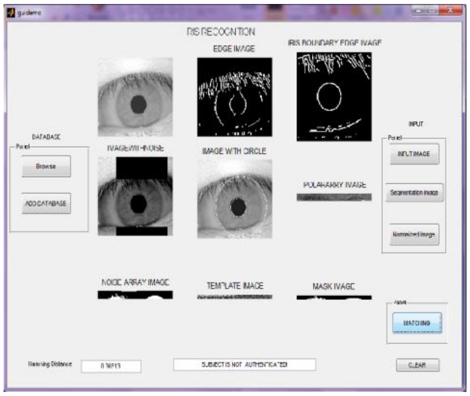


0

C

Input iris image diagram

Matching process



0.36813

SUBJECT IS NOT AUTHENTICATED!

Matching process diagram

CONCLUSION

The main aim of our project is to produce a robust and reliable iris recognition approach by minimize the intra variance (FRR) and maximize the inter variance of the iris. Conventional biometric system store templates directly in database, hence if stolen, they will lose permanently and become unusable in that system and other system based on that biometric. In our approach, an iris biometric template is secured using iris biometric and passwords. Error Correction Code, ECC is also introduce to reduce the variability and noisy of the biometric data. The Error Correction Code used in this research is Reed Solomon Codes.

Reed Solomon Codes is proven as a very powerful cryptography error correction codes and very suitable for iris biometric cryptography Using Reed Solomon Codes, the FRR is reduced from our previous work [23] of 26% to around 2.92% which enhanced the recognition performance of the iris. Both of the performance is nearly the same between two of the distance metric functions. Among the two distance function which is Hamming Distance and Weighted Euclidean Distance, we found that

Hamming Distance provides the best result. Advanced Encryption System (AES) is utilized to assure a more secured transaction on the password. With the combination of password usage, the security of the iris biometric authentication has also increase to a higher level. The security of AES has been identified as a world standard algorithm that has been used for many protections on sensitive information. Since this is the preliminary works, only one dataset has been used for the experimental results, different dataset of the iris will be tested in the future.

REFERENCE

[1] John Daugman, University of Cambridge, How Iris Recognition works. Proceedings at International conference on Image Processing.

[2] Reed I. S. and Solomon G., "Polynomial Codes Over Certain Finite Fields" SIAM Journal of Applied Mathematics, Volume 8.

[3] Wildes, R.P.: Iris Recognition: An Emerging Biometric Technology. Proceedings of IEEE 85, 1348–1363 (1997).

[4] Pattraporn A., Nongluk C., "An Improvement of Iris Pattern Identification Using Radon Transform," ECTI Transactions On Computer And Information Technology, vol. 3, No.1 May 2007, pp.45–50.

[5] Wu, X., Qi, N., Wang, K., and Zhang, D., " A Novel Cryptosystem Based on Iris Key Generation". In Proceedings of the 2008 Fourth international Conference on Natural Computation - Volume 04 (October 18 - 20, 2008). ICNC. IEEE Computer Society, Washington, DC, 53-56.