IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

nCORETech

LBS College of Engineering, Kasaragod

Vol. 3, Special Issue 1, February 2016

Fused Iris Biometrics for Person Identification

Mithja P[1], Sambhu D[2]

PG Scholar, Electronics and Communication Engineering, LBS College of Engineering, Kasargod, India[1]

Assistant Professor, Electronics and Communication Engineering, LBS College of Engineering Kasargod, India[2]

Abstract: The conventional authentication methods such as proxy based and biometrics based are not user centric and endangers security and privacy, system provides automatic identification of an individual based on a unique feature or characteristic possessed by the individual. Iris authentication is a biometric modality which can be used to identify a person. In this paper, proposes a method in which a reference subject (RS) is securely fused with user's biometrics, developing a Biocapsule (BC) from the fused biometrics for authentication. Selection of the reference subject can be a physical RS or a logical RS. The pre-processing techniques are done before the fusion process. Features of user biometrics and RS biometrics are extracted. Individual features make the proposed BC mechanism a user-centric authentication approach. Fusing the transformed user biometrics and RS biometrics, a BC is developed from fused biometrics. The generated BC is matched with BC in the database which is already stored during the enrolment stage. If the matching is true, user identity is correct else wrong identification. Fusion aims to increase the security of the biometrics because through the fusion, user biometrics is hidden by RS biometrics, thus provides secure biometric that is privacy preserving. BC carries no hints that the user is weighted more than the RS and equally treats user and RS. This biometric system possesses various properties such as security, privacy preservation, cross matching resistance, etc.

Keywords: Authentication, privacy-preserving, Biocapsule (BC), secure fusion, Reference subject (RS).

I. INTRODUCTION

A biometric system provides automatic recognition of an individual. Iris Recognition based on the unique feature of an individual. Biometric system based on fingerprints, handwriting, retina, facial features, voice, hand geometry, and iris. First capturing a sample of the feature, such as taking a digital colour image for iris recognition. Mathematical function used to transform some sample into a biometric template. Efficient and highly distinctive representation of the features provided, which is biometric template and can then be objectively compared with other templates to determine similarity. Two modes of operation are allowed by biometric systems. An enrolment mode for selecting templates to a database, and an identification mode, where template formed in an individual.

Passwords, ID cards and token are the traditional methods of identity verification based on knowledge. Only low level of security provided those methods because passwords and PIN can be forgotten, ID cards and token can be lost. Biometric based verification systems an validate an individual's identity based on the physiological and/or behavioural characteristics of the user. There is nothing to lose or forget with biometrics and it is relatively difficult to entrap.

In this paper, proposes a new approach for iris identification [1]. This method involves reference biometric securely fused with user's biometric, developing a Biocapsule (BC), which is used for authentication. We develop gray scale invariant local texture patterns (LTP) [2] to extract iris key. 1D Log-Gabor is used to extract user feature set and RS feature. Hamming distance is used to measure the matching between 2 iris templates but it have low recognition rate. In this work Support vector machine classification methods are proposed rather than a hamming distance method [10]. Support vector machine is used as a main classifier. The proposed authentication system is divided in two phase. In the first phase, iris patterns need to store the system as an enrolment phase. At the time of identification, we capture current iris feature and compare it with the stored Biocapsule, which is called identification phase.

II. RELATED WORK

Previously proposed Biocapsule is based on the difference of the user's biometric feature and that of a proposed reference subject (RS). Difference based Biocapsule [2] design have some limitations. BC generation is at the feature level, this possibility is limited. Because features can be easily attacked.

The biometric system attains various properties such as security, privacy preservation, cross matching resistance, etc. And existing Biometric Crypto System(BCS) and Cancellable Biometrics(CB) [4] methods cannot fully focus one or more of these properties. In this paper, proposes "secure fusion" of the user biometrics and the RS biometric and focus

DOI 10.17148/IJIREEICE

these issues in a comprehensive manner. This iris recognition is considered as the most reliable and precise biometric identification system. This iris recognition system is based on the Daugman's algorithm. Daugman's algorithm able to localize the circular iris and pupil region. The extracted iris region was then normalized then key and features are extracted. Fusing the key and feature to form Biocapsule. The generated BC is matched with BC in the database which is already stored during the enrolment

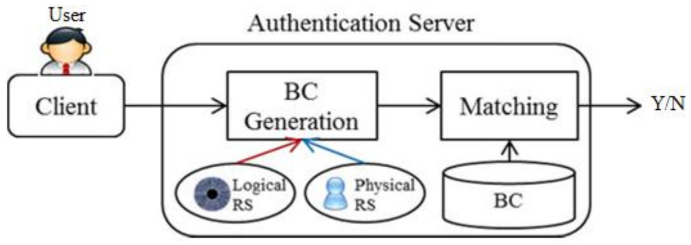

Fig. 1. System Architecture

If the matching is true, user identity is correct else wrong identification. Fusion aims to increase the security of the biometrics because through the fusion, user biometrics is hidden by RS biometrics, thus provides secure biometric that is privacy preserving. BC carries no hints that the user is weighted more than the RS and equally treats user and RS. If the BC is lost, fusion approach prevents the recovery of the user biometrics or RS biometrics from a compromised BC. Such approach is user friendly and revocable once a BC is compromised. The fusion based approach prevents various attacks so privacy is preserved [8]. Ability to handle privacy enhancement without compromising security.

This proposed system four possible decisions are the authorized person is accepted, the authorized person is rejected, the unauthorized person is accepted and the unauthorized person is rejected. The accuracy of the proposed system is then specified based on FRR and FAR rate. False Rejection Rates (FRR) are the measure of the system to reject the authorized person and False Acceptance Rates (FAR) is the rates of the system to accept the unauthorized person. Both performances are can be expressed as:

$$\text{FRR} = \frac{\text{NFR}}{\text{NAA}} \text{x}100\% \qquad (1)$$

$$\text{FAR} = \frac{\text{NFA}}{\text{NIA}} \text{x}100\% \qquad (2)$$

NFR is the numbers of false rejections and NFA is the number of false acceptances, while NAA and NIA are the numbers of the authorized person attempts and the numbers of unauthorized person attempts respectively. Furthermore, low FRR and low FAR is the main objective in order to obtain both high usability and high security of the system.

III. NEW BIOMETRIC AUTHENTICATION

The system contains two stages registration and verification. During registration, user biometric fused with the RS Biometric and developed Biocapsule which is stored in the system. For verification request, user biometric fused with an RS biometric and compared with a stored BC.

Selection of the reference subject can be a physical RS or a logical RS. The user’s biometric is captured via camera by the authenticated user and sent to the authentication server. Through some pre-processing, the user biometric fused with the RS biometric and stored in the server. The server matches the generated BC against the stored BC in the system for an authentication decision is Y or N. The system architecture model is shown in Fig.1.

A. Segmentation

Daugman makes use of an integro-differential operator [6] for locating the circular iris and pupil regions, and also find the arcs of the upper and lower eyelids. The integro-differential operator is defined as,

$$\max_{(r,\ xo,\ yo)} = \left| G_\sigma(r) * \frac{\mathbf{d}}{\mathbf{dr}} \oint_{\mathbf{r,xo,yo}} \frac{\mathbf{I(x,y)}}{\mathbf{2\pi r}} \mathrm{ds} \right| \qquad (3)$$

Where $I(x, y)$ is the eye image, r is the radius to search for, G_σ is a Gaussian smoothing function. The contour of the circle s given by r, x_0, y_0. Varying the radius and centre x and y position of the circular contour gives maximum change in pixel values. The operator searches for the circular path where there is change in pixel values.

Iris and pupil are extracted by performing segmentation of an eye image. Also, isolates noise areas such as occluding eyelashes and eyelids.

B. Normalization

For normalisation of iris regions Daugman's rubber sheet model is used. The reference point is the centre of the pupil. A number of data points are chosen across each radial line and this is called as the radial resolution. The number of radial lines going around the iris region is defined as the angular resolution. The rubber sheet model constructs by Daugman [6]. Each point within the iris region remaps into pair of polar coordinates (r,θ), where r is in [0,1] and θ is angle [0,2π].

Perform normalisation of the iris region. Unwrapping is used to form rectangular block of constant dimensions from circular region.

C. Feature Extraction

Feature encoding is performed by convolving the normalized iris pattern with 1D Log-Gabor wavelet [5]. 2D normalized patterns are divided into a number of 1D signals. Each row corresponds to a circular ring on the iris region. User feature and RS feature are extracted from biometric data. Convolving each row of an image with 1D log Gabor filters. Convolution results a 1D cell array of complex value.

D. Key Extraction

Compute the gray scale-invariant LTP [3]. The LTP computation starts with the definition of two windows 2 Windows T and B Window. LTP for each pixel inside B is $|I_{ij} - A_T|$. Where I_{ij} is the gray scale value and A_T is the mean gray scale value inside T. $A_{T=} \frac{1}{N} \sum_{x,y \in T} Ixy$ with N the total number of pixels contained within T. Generate Temporary signature by averaging the LTP values of rows. Compute the mean V of the temporary signature Given a system mean parameter M, obtain the iris signature by, $S = \tilde{s} - V + M$ with V obtained by $V = \frac{1}{m} \sum \tilde{s}$.

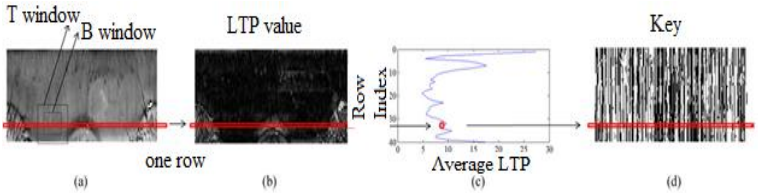

Fig.2. key extraction process

Encode the iris signature to key. Encoding is an part of the key extraction. An average of a row of LTP values is the iris signature component. The iris signature component could possibly range from 0:0 to 18:0. To encode an iris signature component, create an encoding book which is a mapping Map : {0:0 - 18:0}→ {1, -1}^{n} considering the 10th decimal part of the iris signature component. Applying map on iris signature component a m x n length key is obtained. The Key extraction process is shown in Fig.2.

E. Secure Fusion

For secure fusion user feature and RS key are multiplied and user key and RS feature are multiplied and fused. On biometric inputs F^u(user feature), F^r(reference feature),K^u (user key),and K^r (reference key, where $F^u,F^r \in \{F_i\}^n$ ($f^L \leq Fi \leq f^U$) and K^u, $K^r \in \{K_i\}^n$ ($K_i = 1,-1$), through "secure fusion" the fused biometric $F^{u,r}$(or $\{F_i^{u,r}\}^n$) is obtained by,

$$F_i^{u,r} = (F_i^u .K_i^r + F_i^r .K_i^u \ (f^U - f^L)) + f^l \qquad (4)$$

Within F_i^u is one component of the user biometrics, F_r^u is one component of the RS biometrics, K_i^u is one key bit of the key and K_i^u is one key bit of the RS key. It is obvious that $F^{u,r} \in \{Fi\}n$ ($f^L \leq Fi \leq f^U$). This $F_i^{u,r}$ is the Biocapsule which is stored in the system. Secure fusion is shown in Fig. 3.

F. Matching

For matching, the Hamming distance, [7] is chosen as a metric for recognition. The result of this computation is then used as the best match, with smaller values indicating better matches. If two patterns are derived from same iris, the hamming distance between the same iris close to 0. During the matching process, any iris image is given to and Hamming distance based classification approach. If correct classification is not done by Hamming distance, then SVM is used for classification.

DOI 10.17148/IJIREEICE

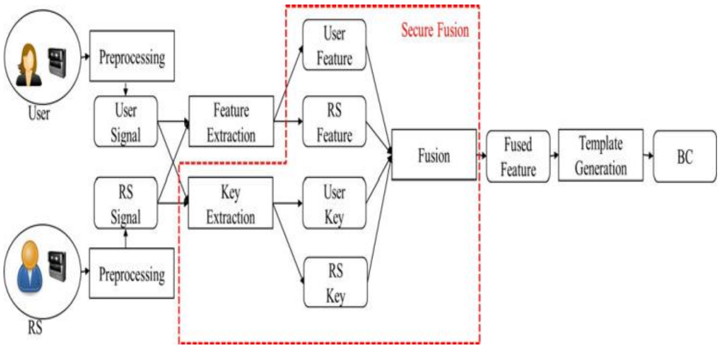

Fig. 3 Secure Fusion

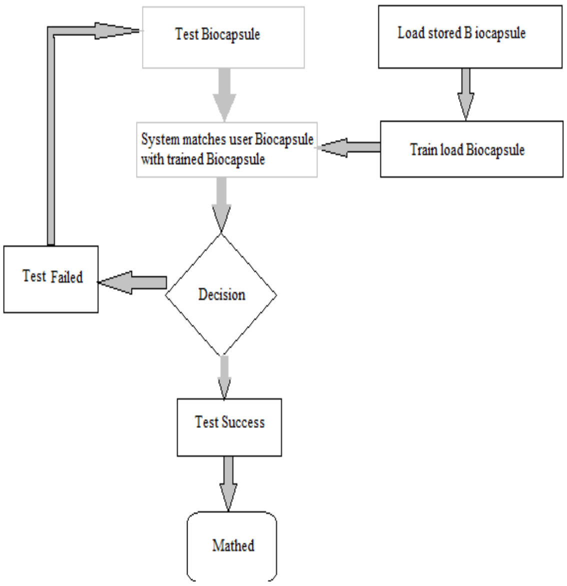

Fig.. 4 SVM classifications

G. Support Vector Machine

To verify a person’s identity based on the Biocapsule SVM is used. This pattern matching method as shown in Fig. 4. There are different classifiers presented for iris recognition. Kernel based techniques reduce the dimensionality of the extracted feature vectors. Kernel based biometric recognition systems are converting scalar features to the vector feature space. Therefore, vector based classifiers have got more significance over other classifiers like neural network and nearest neighbour classifier. Support vector machine is essentially a two class classification problem. Feature vector of the low dimensionality plane to high dimensionality plane are transformed by this technique. This feature is easily distinguishable. Different kernel functions like Gaussian, RBF and Linear functions are used for the same transformation. SVM, [9], [10] is used for classification of data points. There are two classes in the data points which may be genuine or imposter. The efficient method is to classify the two data points is hyper planes. The margin denotes the maximum width in the hyper planes. Moreover support vector is used to disparate the vectors. To distinguish between objects of dissimilar class memberships is known as hyper planes classifiers. Support Vector Machines are particularly proper to handle such tasks.

IV. SIMULATION AND RESULTS

Daugman's Integro-differential proved to be successful. Iris image is then automatically segmented. The IITD database provided good segmentation, since those eye images are taken for iris recognition and boundaries of iris pupil and sclera were clearly distinguished. In the IITD database, the Daugman's Algorithm based segmentation is performed. Using Integro-differential equations methods locating the pupil and limbus assumes that the boundaries are perfect circles. Iris features are extracted by using 1D log Gabor filter and key is extracted by LTP technique. Biocapsule are used for training and testing of the SVM. For this database 400 images (20 persons) were used for the training and 40 images for the testing purpose. The recognition accuracy was compared between the hamming distance method and SVM method.

Matching performance of hamming distance evaluation is based on EER, FRR and FAR values in which it hard to achieve zero FAR and FRR. SVM method compares this approach to existing approaches by providing the FAR and FAR. We have used the linear kernel function. However, further study has to be done to improve the level of classification using different kernel function for better classification.

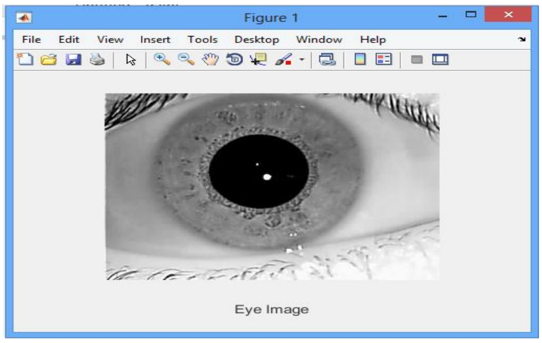

Fig. 5 Input Image

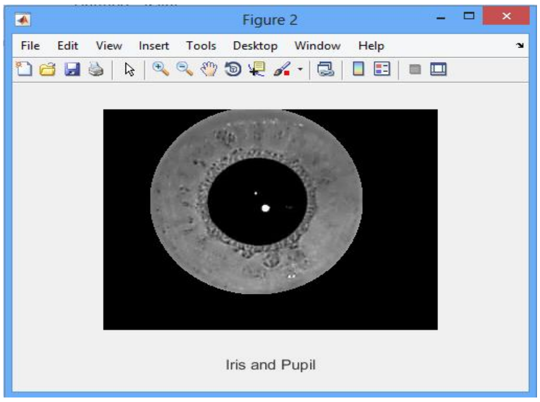

Fig. 6 Pupil and Iris

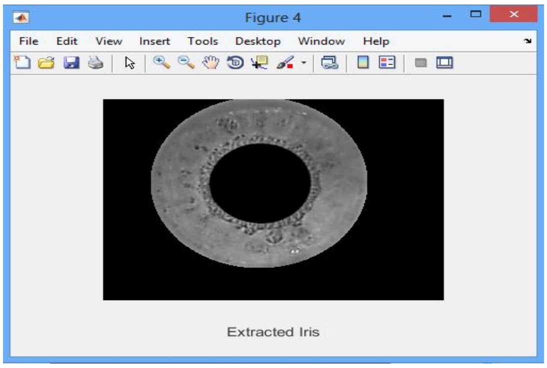

Fig. 7 segmented iris

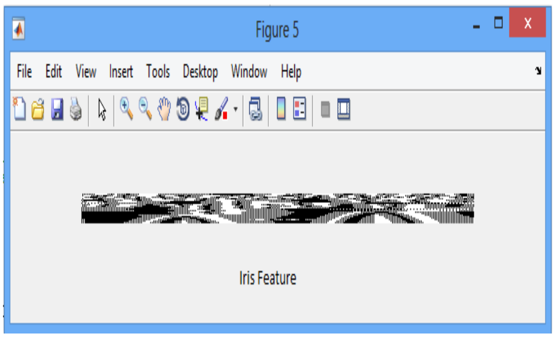

Fig. 8 Iris Feature

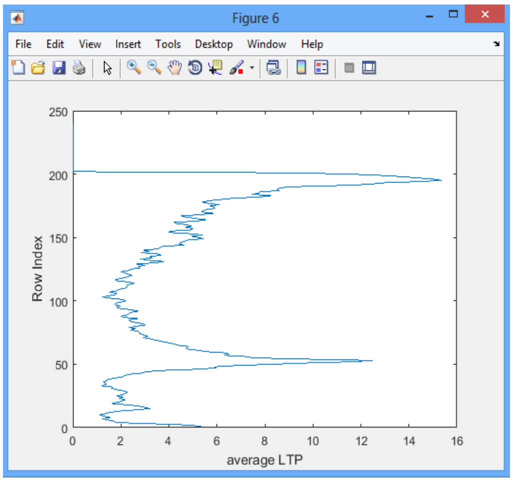

Fig. 9 LTP values

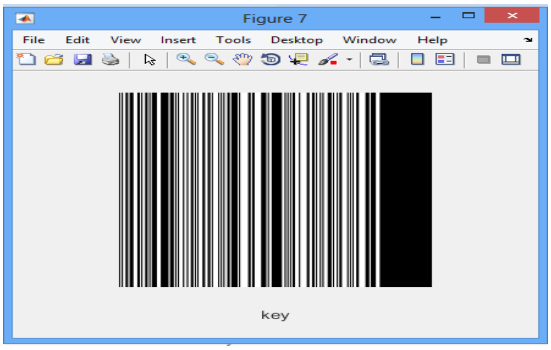

Fig. 10 Iris Key

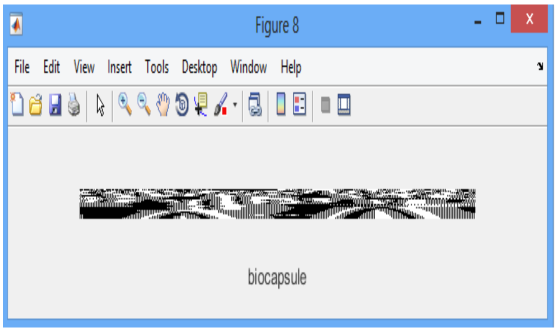

Fig. 11. Biocapsule

Table 1 Comparison of Hamming distance and SVM

	Hamming distance		SVM	
Authorized user	EER	FRR(FAR=10^{-4})	EER	FRR(FAR=10^{-4})
User 1	0.0108	0.0204	0.0023	0.0013
User 2	0.0290	0.0370	0.0031	0.0039
User 3	0.0119	0.0478	0.0011	0.0014
User 4	0.0138	0.0263	0.0041	0.0021
User 5	0.0218	0.0562	0.0022	0.0020
Average	0.0174	0.0375	0.0025	0.0023

V. CONCLUSION

This paper presents an iris recognition system, in which segmentation is done using Daugman's algorithm. Next, segmented iris region was normalised to eliminate dimensional inconsistencies between iris regions. This is achieved by implementing a version of Daugman's rubber sheet model, which is unwrapped into a rectangular block with constant polar dimensions. Features of the iris were encoded by convolving the normalized iris region with 1D Log-Gabor filters. The key is extracted by using Local Texture Pattern(LTP). Fusing user biometric and reference biometric for secure fusion. Fused biometrics are attached into an existing biometric system to develop a Biocapsule for authentication. The proposed BC mechanism has many desired features. Security analysis shows that the approach is secure and allowed to reduce attacks, thus the security of the user biometrics is assured and the user privacy is preserved. The Support Vector Machine was taken as classifier in order to develop the user model based on iris code data. Experimental study using IITD database is carried out to evaluate the effectiveness of the proposed system. The recognition accuracy was compared with the previous reported approaches. Based on obtained results, SVM classifier produces a slightly less results than previous method, But can be improved by using other kernels.

ACKNOWLEDGMENT

The authors would like to express special thanks to teacher for providing an excellent guidance in the research, parents and friends who help a lot for finalizing the research work. Finally, sincere thanks to God who is the power of the strength with each step of progress towards its successful completion.

REFERENCES

[1] Yan Sui et al, “Design and Analysis of a Highly User-Friendly, Secure, Privacy-Preserving, and Revocable Authentication Method”, IEEE Transaction on Computers,volume.63,number.4,april 2014.

[2] Y. Sui, X. Zou, and E. Du, “Biometrics-Based Authentication: A New Approach,” Proc. 20th Int’l Conference on Computer Communication System. and Networks (ICCCN), pp. 1-6, August. 2011.

[3] Y. Du, R. Ives, D. Etter, and T. Welch, “Use of One-Dimensional Iris Signatures to Rank Iris Pattern Similarities,” Optical Engineering. volume. 45, number. 3, 2006.

[4] F. Hao, R. Anderson, and J. Daugman, “Combining Crypto with Biometrics Effectively,” IEEE Transaction on Computers, volume. 55, number. 9, pp. 1081-1088, September. 2006

[5] Richard Yew Fatt Ng, et al “A Review of Iris Recognition Algorithms” IEEE 2008

[6] J. Daugman, “How Iris Recognition Works,” IEEE Transaction Circuits and Systems for Video Technology, volume. 14, number. 1, pp. 21-30, Jan. 2004.

[7] Ashish kumar Dewangan, Majid Ahmad Siddhiqui “Human Identification and Verification Using Iris Recognition by Calculating Hamming Distance”, International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-2, May 2012

[8] Przemysław Strzelczyk, “Privacy Preserving And Secure Iris-Based Biometric Authentication For Computer Networks”,Journal of telecommunications and information technology,volume 4,2011

[9] Ali, H., Salami, M.-J. E., & Wahyudi, "Iris recognition system using support vector machine". International conference on computer and communication engineering, pp. 516–521, 2008.

[10] Rai, H., & Yadav, A. Iris recognition using combined support vector machine and Hamming distance approach., Expert Systems with Applications, 2013.