Journal of
Information Technology & Software Engineering

Research Article Open Access

Designing a Bio-Capsule Secure Authentication System

Logeshwari R[1]*, Karthikayani K[1], Sindhuja A[2] and Ashok D[1]

[1]*Assistant Professor, Department of Computer Science, SRM University, Chennai, India*
[2]*Assistant Professor, Department of Information Technology, Prathyusha Institute of Technology and Management, Thiruvallur, India*

Abstract

In this modern world, especially on the Internet, user might have more and more usernames or IDs and passwords, which contains his/her private information. There are too many for user to remember and it is unsafe to write them down on you notebook. To solve this problem, this paper made a designed a User data Management System (UMS), by which user can manage his/her private information's efficiently. With the fast evolution in sensor technology biometric authentication system becomes more popular in daily lives. The biometrics is improving the capability to recognize the persons. The construction of Bio-Capsule from biometrics is used generally to secure the system. The biometrics used in this paper is fingerprint and iris. These two features are combined with the help of fusion algorithm. From the combined features, Bio-Capsule is generated which used for authenticating User data Management Systems.

Keywords: Biometrics; Bio-capsule generation; Minutiae points; Morphological operation; Histogram Equalization; Weiner filtering; Fusion algorithm

Introduction

Information security and privacy has become an important factor in the present world. As an individual, everyone has the security problem on their private information‟s, which is accompanied by password protection. With the services on the internet increased, user may become a member of different websites, and also use many other network services and online transactions, thus the password setting problem occurs. For the convenience, some users may assign same passwords for all the internet services, resulting in onelost- all-lost security risk. Also some users may have high awareness of security, so they passwords for each service. But he/she may likely forget some of them when they have not been used for long time. To effectively alleviate the contradiction between password security and memory defects of human beings, a design of User Data Management System (UMS) is needed to manage user‟s data. A biometric system is a standard method for identification and verification of a human being based on the personal or physical identification of characteristics. Biometric cryptosystems is a new technique which combines biometrics and cryptography, and is popularly known as crypto-biometric systems. The integration of biometrics and cryptography is broadly carried now-a-days. In biometrics bio-capsule resetting is very much complicated. This paper uses two biometrics features to generate the bio-capsule. The biometrics used in this paper is fingerprint and iris. These two biometrics features are combined using a technique called fusion. From these combined features, bio-capsule is generated which is used for authenticating UMS.

Related works

Biometrics is a powerful tool for human verification and authentication. It is done with the help of human biometric templates namely Finger-Knuckle- Print, Finger Print, Iris, Palm Print etc. Recently more research going on hand based samples, because it is highly sensitive and distinct. Cryptography needs for reliable communication (Figure 1), but cryptography alone is not enough to achieve it. In such a way, cryptography deals with security levels and biometric handles identity of human. Biometric key generation is mainly used for user identification. The generated key is totally differs from biometric features. So the key is never ever overridden with cryptographic systems. Each biometric feature has its own strengths and weaknesses and the choice typically depends on the application. The better biometric characteristic has five qualities: robustness, distinctiveness, availability, accessibility and acceptability. Fingerprints are unique and it is most widely used to identify the person. Its matching accuracy was very high [1]. Iris is the ideal part of the eye in human body. It contains many distinctive features such as furrows, ridges and rings etc. [2]. Iris technology provides greater unique identification. According to the above features

Fingerprint and iris are taken to develop the proposed system. A Multi biometric system combines characteristics from different biometric traits [3] uses approach to making a feature vector compact and efficient by using Haar wavelet transform, and two straightforward but efficient mechanisms for a competitive learning method such as a weight vector initialization and the winner selection. The system proposed by Tisse [4]. Uses gradient decomposed Hough transform integro-differential operators combination for iris localization and the "analytic image" concept (2D Hilbert transform) to extract pertinent information from iris texture. The concept of multimodal biometric system has been proposed by Ross and Jain [5] where apart from fusion strategies various levels of integration are also presented. In [6] fusion of iris and face biometrics has been proposed. The score level fusion in multimodal biometrics system is proposed in [7]. A novel fusion at feature level for face and palm-print has been presented in [8].

A proposed bio-capsule generation: Biometric cryptosystems combines cryptography and biometrics to afford the advantages of both for security [9]. This technique will provide the advantages like better and modifiable security levels which are the advantages of cryptography and advantages like eliminating the must to memorize passwords or to carry tokens etc. which are the advantages of using biometrics. This paper combines the features of fingerprint and iris and with that combined feature; Bio-capsule generated which provides secure authentication to UMS as shown in (Figure 1).

Over view of fingerprint: A fingerprint is made of a number of

***Corresponding author:** Logeshwari R, Assistant Professor, Department of Computer Science, SRM University, Chennai, India, Tel: 044 2745 6730; E-mail: Loge.shwari54@gmail.com

Received December 09, 2014; **Accepted** January 02, 2015; **Published** January 12, 2015

Citation: Logeshwari R, Karthikayani K, Sindhuja A, Ashok D (2015) Designing a Bio-Capsule Secure Authentication System. J Inform Tech Softw Eng 5: 138. doi:10.4172/2165-7866.1000138

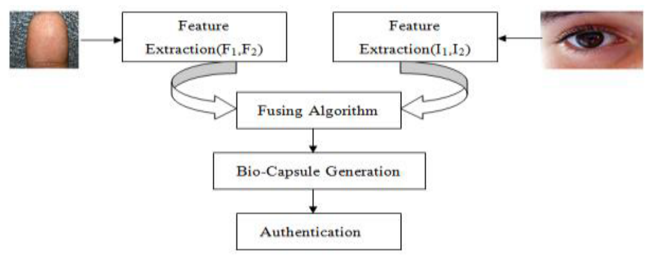
Feature Extraction(F_1,F_2)
Feature Extraction(I_1,I_2)
Fusing Algorithm
Bio-Capsule Generation
Authentication

Figure 1: Bio-Capsule Generation.

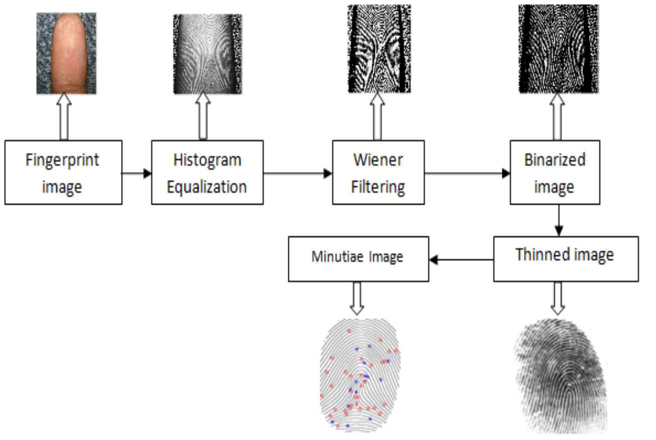

Figure 2: Feature Extraction of Fingerprint.

ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutia points: ridge endings (where a ridge end) and ridge bifurcations (where a ridge splits in two). Many types of minutiae exist,

- Dots-Very small ridges
- Islands-Ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges
- Ponds or lakes-Empty spaces between two temporarily divergent ridges
- Spurs-A notch protruding from a ridge
- Bridges-Small ridges joining two longer adjacent ridges
- Crossovers-Two ridges which cross each other.

Feature extraction from fingerprint: We have selected fingerprint as the biometrics feature for generating Bio-Capsule. We have extracted minutiae points from the fingerprint and used that point set for generating capsule [10].

Fingerprint image preprocessing: For image preprocessing Histogram Equalization and Filters are used to enhance the image. Binarization is applied on fingerprint image. Then Morphological operation is used to extract Region of Interest (Figure 2).

Histogram equalization

Histogram equalization defines a mapping of gray level p into gray level q such that the distribution of gray level q is uniform. This mapping stretches contrast (expands the range of gray levels) for gray level near the histogram maxima. Since contrast is expanded for most of the image pixels. The transformation improves the delectability of many image features. The probability density functions of pixel intensity level rkis given by:

Pr(rk)=nk/n (1) Where 0 ≤ rk ≤ 1 where k=0,1,2…255 nk is the number of pixels at the intensity level rk and n is the total number of pixels.

Wiener filtering noise reduction

We proposed to use a pixel-wise adaptive Wiener method for noise reduction. T the filter is based on local statistics estimated from a local neighborhood of size 3×3 of each pixel, W (n1,n2)=μ+ (σ2 – v2)/σ2(I(n1,n2)-μ) (3) When v2 is noise variance and σ2 are local mean and variance, I represent the gray level intensity in n1, n2€ ∩.

Binarization: The operation that converts a grayscale image into a binary image is known as binarization by computing the mean value of each 32-by-32 input block matrix and transferring the pixel value to 1 if larger than the mean or to 0 if smaller [11].

Thinning: The final image improvement pace normally performed before minutiae extraction is thinning. Thinning is a morphological process that consecutively takes away the foreground pixels till they are one pixel apart. By applying the thinning technique to a fingerprint image maintains the connectivity of the ridge structures during the formation of a skeleton stage of the binary image. This skeleton image is subsequently utilized in the following extraction of minutiae. Inew(n1 , n2,)={1 if I old(n1,n2)≥ local mean (4) Thinned (one pixel 1 thickness) ridgelines are obtained using morphological thinning operations.

Minutiae feature extraction

The next step is to obtain the minutiae from the thinned image. The most commonly used technique of minutiae extraction is the Crossing Number (CN) model. This process involves the utilization of the skeleton image in which the ridge flow pattern is eight-connected [12]. The minutiae are obtained by examining the local neighborhood of every ridge pixel in the image by means of a 3×3 window. The CN value is then calculated which is defined as partially the addition of the differences among the pairs of neighboring pixels in the eight-neighborhood indicates the list of minutiae in a fingerprint image.

Mapping function

The coordinate system utilized for the purpose articulating the minutiae point locations of a fingerprint is a Cartesian coordinate system. The X and Y coordinate of the minutiae points are in pixel units. Angles are represented in regular mathematical format, with zero degrees to the right and angles rising in the counter-clockwise direction [13]. The obtained minutiae points are stored as below F1 = [x1,x2,x3,……xn] F2 = [y1,y2,y3,…..yn]

Overview of iris: The iris is a thin circular diaphragm, which lies between the cornea and the lens of the human eye. The average diameter of the iris is 12 mm, and the pupil size can vary from 10% to 80% of the iris diameter. Due to epigenetic nature of iris patterns, the two eyes of an individual contain completely independent IRIS patterns and identical twins possess uncorrelated iris patterns.

IRIS image processing

Iris localization: The acquired iris image has to be preprocessed to detect the iris, which is an annular portion between the pupil (inner boundary) and the sclera (outer boundary). The first step in iris localization is to detect pupil which is the black circular part surrounded by iris tissues [14]. The center of pupil can be used to detect the outer radius of iris patterns. The important steps involved are:

1. Pupil detection
2. Outer iris localization

Pupil detection: The iris image is converted into grayscale to remove the effect of illumination. As pupil is the largest black area in the intensity image, its edges can be detected easily from the binarized image by using suitable threshold on the intensity image. But the problem of binarization arises in case of persons having dark iris. Thus the localization of pupil fails in such cases. In order to overcome these problems Circular Hough Transformation for pupil detection can be used. The basic idea of this technique is to find curves that can be parameterized like straight lines, polynomials, circles, etc., in a suitable parameter space. The transformation is able to overcome artifacts such as shadows and noise as shown in (Figure 3).

Outer Iris localization: External noise is removed by blurring the intensity image. But too much blurring may dilate the boundaries of the edge or may make it difficult to detect the outer iris boundary, separating the eyeball and sclera. Thus a special smoothing filter such as the median filter is used on the original intensity image. After filtering, the contrast of image is enhanced to have sharp variation at image boundaries using histogram equalization as shown in (Figure 4) shows an example of localized iris image.

Iris normalization: When the iris image is proficiently localized, then the subsequent step is to transform it into the rectangular sized fixed image.

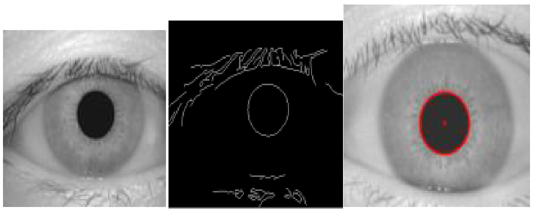

Figure 3: Steps involved in detection of inner pupil boundary.

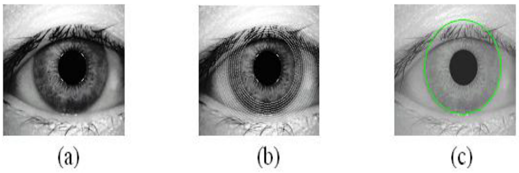

Figure 4: (a) Contrast enhanced image (b) Concentric circles of different radii (c) Localized Iris image.

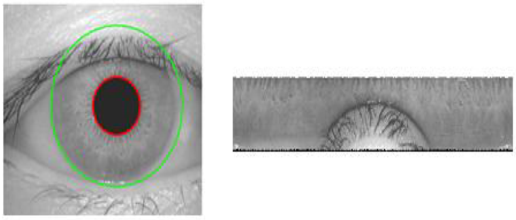

Figure 5: Daugman"s Rubber Sheet Model–Normalisation.

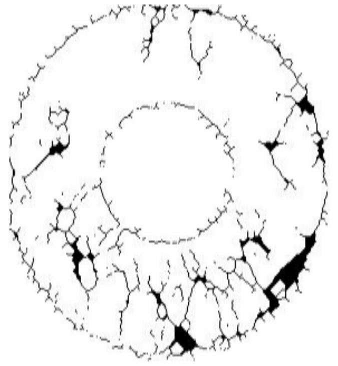

Figure 6: Iris textures after thinning operation.

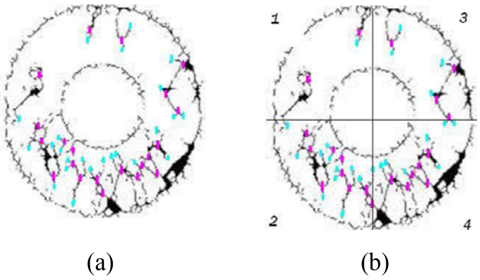

Figure 7: Minutiae representation (a) Nodes are shown in pink dots and end points are shown in blue dots (b) Iris rim divided into 4 quadrants.

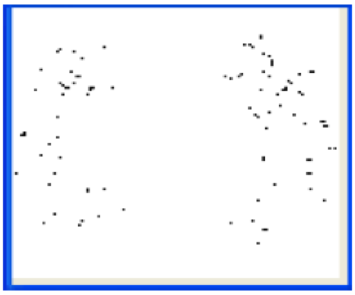

Figure 8: Minutiae representation of Nodes and endpoints are shown in circles.

Daugman's rubber sheet model: Normalization process includes unwrapping the iris and transforming it into its polar equivalent. It is performed utilizing Daugman"s Rubber sheet model and is depicted in the following (Figure 5).

Extraction of Iris texture

For appropriate representation of structures, thinning is used so that every structure presents itself as an agglomerate of pixels as shown in (Figure 6).

From the above iris rim containing iris pseudo textures, the polar coordinates of minutiae (nodes and end points of iris textures)are extracted by resizing the image into a standard format of 256×256 as shown in (Figure 7).

From the above iris rim containing iris pseudo textures, the polar coordinates of minutiae (nodes and end points of iris textures) are obtained by resizing the image into a standard format as represented in (Figure 8).

These obtained Minutiae points are kept as I1 = [x1,x2,x3,……xn] I2 = [y1,y2,y3,….yn]

Algorithm for feature fusion: This phase will perform the fusion process for the gathered fingerprint and iris features. The input to the fusion process will be four vectors F1, F2, I1 and I2 which are obtained from fingerprint and iris.

The steps involved in fusion of biometric feature vectors are as follows.

Shuffling of individual vectors: 1. Initialize a Random vector RVi (Size of F1)

2. J=RVi×Large Integer Value

3. Interchange ithand jthIndex Values

Above steps are repeated for all the components of F1 which given as S1. This procedure is repeated for all vectors F2, I1 and I2 to produce S2, S3 and S4.

Concatenation of shuffled vectors: In this process the shuffled Fingerprint vectors S1 and S2 is concatenated with Iris vectors S3 and S4.

1. Initialize a vector M1 (size of |S1| + |S3|) and Initial values of |S3| is filled with S3 for S1

2. Select „t‟ (size of M1)

3. Do logical right shift operation in M1 from index t

4. The components of S1 are inserted into emptied th index of M1. The above mentioned procedure is performed among shuffled vectors S2 and S4 to obtain a vector M2. In this manner, the concatenation process yields two vector M1 and M2.

Merging of concatenated vectors: The final process in creating the biometric template BT is the merging of two vectors M1 and M2

1. The component M1 and M2 are converted to binary form M11 and M21.

2. Do Binary NOR operation on M11and M21.

3. Convert the binary value into decimal form.

4. Store these decimal values in vector BT.

Generation of Bio-capsule–UMS authentication: The final process of the proposed technique is the creation of Bio-Capsule from the biometric template BT.

BT=[bT1, bT2, bT3 …bTh] The set of different components in the template vector BT are recognized and are stored in another vector UBT. UBT=[u1, u2, u3, …ud] |UBT| ≤ |BT| The vector UBT is then resized to k components appropriate for creating the k-bit Bio-Capsule.

u1, u2, … . uk, if UBT > k

u1 u2 … ud $\ll ui; d + 1 \geq i \geq k$

if |UBT| < k

Where,

Ui=1 duj dj=1

Finally, the key K

B

is created from the vector BT.

KB<<Bi mod 2, i = 1,2,3…k

This finally obtained key serves as an authentication Bio-capsule for the individual in the system. This key is definitely very difficult for the theft to generate. Therefore, a better secure system is created using the proposed technique.

Conclusion

In this paper, we propose a novel Bio-Capsule authentication to provide security to his/her private information's. To effectively alleviate the contradiction between password security and memory defects of human beings, a design of User data Management System (UMS) is needed to manage user's data. Securing the information system becomes most challenging task because of the increased number of theft. To overcome these issues, biometrics of a person is used to secure the system. This paper used fingerprint and iris biometrics to secure the system. The features obtained from these two biometrics are combined using fusion technique. From these fused features, bio capsule is generated which is more secure than other techniques. In future it will be extended with other biometric samples like finger knuckle print, retina, palm-print etc.

References

1. Chih L, Sheng W (1999) WFingerprint feature extraction usinggabor filters. Electron. Lett volume 35: 288-290.
2. Xiang C, Fan XA, Lee TH (2006) Face recognition using Recursive Fisher of Linear Discriminant. IEEE Trans. ImageProcess 15: 2097-2105.
3. Lee BK, Byeon O, Lim S, Lee K, Kim T (2001) "EfficientIris Recognition through Improvement of Feature Vector and Classifier". ETRI Journal 23: 61-70.
4. LocTisse C, Martin L, Torres L, Robert M (2002) Person Identification Technique using Human Iris Recognition. International Conference on Vision Interface, Canada.
5. Arun R, Sarat D, Anil J (2005) "A deformable model for fingerprint matching." Pattern Recognition. 38:95-103.
6. Chen X, Tian J, Yang X, Zhang Y (2006) "An algorithm fordistorted the fingerprint matching based on local triangle feature set." IEEE Trans. Inf. Forensics Security 1: 169–177.
7. Vajna ZMK (2000) "A fingerprint verification system based ontriangular matching and dynamic time Warping." IEEE Trans.Pattern Anal. Mach. Intell 22: 1266-1276.
8. Hong L, Yifei W, Anil J (1998) "Fingerprint image enhancement: Algorithm and performance evaluation." IEEE Trans. Pattern Anal. Mach. Intell 20: 777–789.
9. Schreiner K (1997) Biometrics Prospects for going the distance. IEEE Intelligent Systems, Nov./Dec.1999.
10. Wildes RP, Corp S (1997) Iris Recognition: An Emerging Biometric Technology. IEEE 85: 1348-1363.
11. Arul P, Shanmugam A (2009) Generate a Key For AES Using Biometric For VOIP Network Security. Journal of Theoretical and Applied Information Technology
12. Dodis Y, Ostrovsky R, Reyzin L, Smith A (2004) Fuzzy Extractors: How to generate Strong Keys from Biometrics and other Noisy Data. Proceedings of International Conference on Theory and Applications of Cryptographic Techniques.
13. Chang YJ, Zhang W, Chen T (2004) Biometrics based cryptographic key generation. IEEE International Conference on Multimedia and Expo.
14. Chen B, Chandran V (2007) "Biometric Based Cryptographic Key Generation from Faces," Proceedings of the 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, Usa.