ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Design of Two Tier Security ATM System with Multimodal Biometrics By Means of Fuzzy Logic

Mr.P.Akilan[1], Mr.K.Gunasekaran[2], M.Tech. Mr.D.Saravanan[3], M.E., (Ph.D),

PG Scholar, Dept. of CSE, Pavendar Bharathidasan College of Engg & Tech, Tiruchirappalli, India[1]
Assistant Professor, Dept. of CSE, Pavendar Bharathidasan College of Engg & Tech, Tiruchirappalli, India[2]
Associate Professor & Head/CSE, , Pavendar Bharathidasan College of Engg & Tech, Tiruchirappalli, India[3]

ABSTRACT: Unimodal biometrics uses the single source of physiological/biological characteristics (e.g. face, fingerprint, online signature, DNA) for person authentication. So, if any issue persists in the person's physiological/biological traits then the system leads to serious issue. To overcome this issue, we move into the Multimodal biometrics. Multimodal biometrics is the integration of two or more types of biometrics (e.g. Fingerprint and Face, Face and Iris, Iris and Fingerprint).In Multi biometrics the noise in any one of the biometrics will lead to high false reject rate (FRR) while identification. If any multi biometrics failure means, we can use another type of multi biometrics. To keep the biometric template as secure we use the soft computing technique i.e. Fuzzy Logic. The proposed work is to enhance the security in ATM system with multimodal biometrics along with email verification code which provides two level securities to the system.

General Terms: Biometric Cryptosystem, Security, Biometrics, Template Protection

Keywords: ATM (Automated Teller Machine),Biometric Cryptosystem, Biometrics, Face recognition, Fingerprint recognition, Iris recognition, Multi biometrics, Multimodal biometrics, Template Protection, Two-tier security.

I. INTRODUCTION

Biometrics [6] is a combination of two words"bio" (life) and "metrics" (to measure).It is used to authenticate the person's physical behavioral characteristics. Biometrics system based on single source of information is called Unimodal biometrics system. Multimodal biometrics system is the integration of two or more biometric systems. The integration of two of biometrics gives more secure and meets user satisfaction. After determining which type of biometric sources to be integrated the next step is to build the system architecture. Fuzzy logic means "partial truth". It may have a truth value that ranges in degree between 0 and 1.

Multimodal biometric system can operate in three different modes [11]:

- Serial Mode – It checks each modality before the next modality to be investigated. It is also known as cascade mode.
- Parallel Mode – It combines all the information modalities are processed together to perform recognition.
- Hierarchical Mode – It forms treelike structure for the combination of individual classifiers.

Multimodal biometrics is designed to operate in the following five scenarios:

- Multiple Sensors – It combines the different biometric information of a single user from different sensors.
- Multiple Biometric– Different biometric characteristics of a single user can be combined. It will obtain from different sensors.
- Multiple Units of the same Biometric – Iris from left and right side of the eyes of a single person may be combined.
- Multiple Snapshots of the Same Biometric– Collects multiple snapshots of the same instance are combined for recognition and enrollment.
- Multiple Representations and Matching Algorithms for the same biometrics – Combining various approaches to feature extraction and matching of the multi biometrics.

The rest of the paper is organized as follows: The section 2 presents the existing unimodal biometrics in ATM multi biometrics in ATM which overcomes the problem

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

of unimodal biometrics. Multimodal biometrics and two tier security is used to enhance the security of ATM in section 3 and section 4. In section 5 performance evaluation has been presented and in section 6 conclusions has been presented.

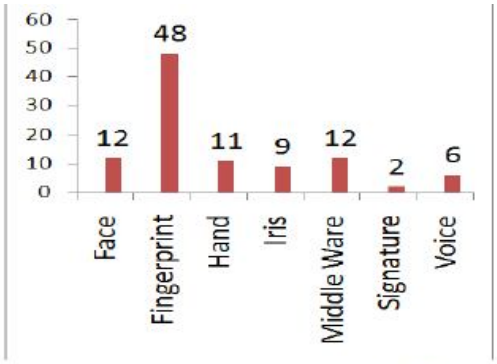
II. UNIMODAL AND MULTIMODAL BIOMETRICS

Biometrics are classified into three Categories [6]
i) Physical biometrics ii) Biological biometrics iii) Soft biometrics. Physical biometrics is static. It does not change. It includes fingerprint, face, iris, retina etc..,. Biological biometrics is dynamic. It can change. It includes signature, keystroke, handwriting and gait. Soft biometrics refers human characteristics. It includes height, weight and color of hair.

2.1 Unimodal Biometrics

The most successful technology used in ATM system is Fingerprint recognition [7].Because the fingerprint is not changing his Characteristic in the human being life Span. So, all the ATM systems preferred finger print recognition only. After the user inserts the card into the ATM enter their PIN number into the system. If it matches with the PIN number stored in the Database. The next step is to enroll their fingerprint biometric identity with the ATM system. If it matches with the template that stored in the database, the system allows the user to access the account. If it mismatches, the card will be ejected.

A fingerprint biometric technique is fused with the ATM for person authentication to ameliorate the security level was dealt. In the world today, fingerprint is one of the essential variables used for enforcing security and maintaining a reliable identification of any individual. The result of the survey conducted by the International Biometric Group (IBG) in 2004 on comparative analysis of fingerprint with other biometrics is presented in the Figure 1.



Comparative survey of fingerprint with other biometrics

Figure 1: comparative Survey of Fingerprint with Other Biometrics

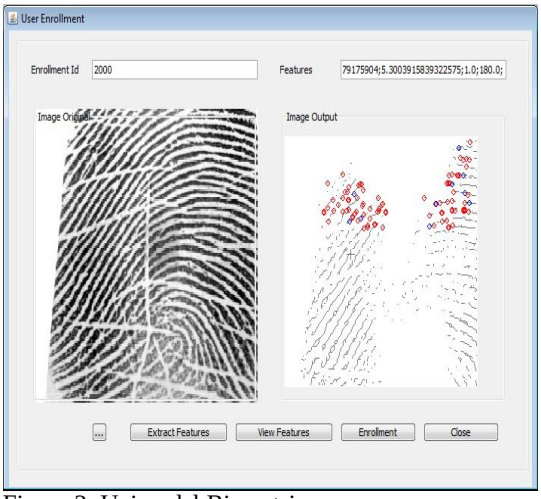


Figure 2: Unimodal Biometrics

2.2 Multimodal Biometrics

Memorizing a password for a human being during his life span is more difficult. So only Unimodal biometrics was developed. In that too, there are many difficulties to face. So that in order to develop the biometrics, now they developed multimodal biometrics. In the Multimodal biometrics [1], it has the combination of two or more biometrics. For securing the biometric template here they used the concept of Fuzzy Logic from Soft Computing. Fuzzy logic is the concept of "partial truth" that defines the matching performance between the stored template and the present given input. The matching value between the templates is between 0 to 1.The biometric cryptosystem approach for multi biometric template protection is for two reasons. Well-known biometric cryptosystems such as fuzzy vault and fuzzy commitment are available for securing [1] a different type of biometric features and it is relatively easy to analyze the security (non invariability) of a secure sketch by leveraging on the characteristics of error correcting codes. Multi biometrics is a combination of one or more biometrics is implemented in ATM. Feature level fusion makes use of embedding algorithms to convert different biometrics into common representation [17].

Embedding algorithm converts binary strings to point-sets, point-sets to binary strings and fixed-length real-valued vectors to binary strings. Biometric cryptosystems have been designed only for specific biometric feature representations. The fuzzy commitment scheme assumes

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

a binary string representation, where the dissimilarity between template and query is measured in terms of the Hamming distance.
Matching performance of a biometric system is based on False Acceptance Rate (FAR), False Reject Rate (FRR), and Genuine Acceptance Rate (GAR).

III. MULTIMODAL BIOMETRICS IN ATMSYSTEM

Nowadays, ATM systems are not more secure. For security reasons the proposed system use multimodal biometrics in the ATM system. In the proposed system, it uses the combination of biometrics together. So that it can manage if any biometrics leads failure. It uses another combination of biometrics .It avoids forge activities. In the proposed system it used face and fingerprint, fingerprint and Iris, face and Iris. The system randomly generates one combination of multi biometrics then the user enrolls their identity for authentication. If the enrollment matches with the stored template the user allows accessing the account otherwise the system allows the user to enroll their other combination of images with one time password generated by the database through e-mail.

3.1FEATURE EXTRACTION FROM FINGER PRINT BIOMETRICS

In both fingerprint identification and finger print verification, the image has been extracted using feature extraction method. It has the following steps [6][14]:

- Image Acquisition:
  Here the image is captured using the fingerprint reader and extract the features into machine readable format.
- Normalization:
  It enhances the contrast of image by transforming the values in the fingerprint image. It distinguishes the ridges and valley of an image.
- Ridge Orientation:
  It is used to obtain the angles of an image and calculated by 16x16 block size.
- Gabor Filter:
  It is used to remove the noise from an image and it preserves ridges and valleys.
- Thinning Algorithm:
  It is used to remove the pixels from an image until it has one pixel wide.
- Binarization:
  It is used to convert the grey level image into binary image using threshold values. The pixels with higher values more than the threshold value as white other pixel values are black.
- Minutiae Extraction:
  In minutiae extraction, it is to count the number of ridge pixels, every ridge pixel on the thinned image is surrounded by and depending on the rule and we can assign the minutiae points to pixels. In minutiae matching, it is to match the minutiae obtained from two sample fingerprint images and test whether they are from the same fingerprint or not.

3.2 FEATURE EXTRACTION FROM IRIS BIOMETRICS

The steps involved in extraction of iris biometrics are[15]:

- Iris localization:
  It is used to identify the boundaries of the Iris. By using boundaries, it is easy to extract the iris pattern. It is done by using Hough transform. The advantage of using Hough transform is isolate features within an image, it does not affect by noise.
- Unwrapping:
  It is used to create the template form for Iris into binary form. Sampling of unwrapped iris is made by applying Haar wavelets to decompose the data in the iris region into different frequency resolutions.
- Binarization:
  It converts the gray level vector signal into black and white vector signal. For converting, it uses threshold values .The value which is greater than the threshold value is set to 1.The value which is lesser than the threshold value is set to 0.
- Matching:
  It does not consider the image size and position for matching with the template. Hamming Distance is used to matching the iris templates.XOR detect the disagreement between two iris codes, AND is to ensure both pair of bits is uncorrupted by eyelashes and lids on iris. Hamming distance is calculated where code A is first iris code and code B is the iris code which is stored in the database. 0 in the mask bits corresponds to a bad bit in that position in iris code.

$$HD = \frac{\|(codeA \otimes codeB) \cap maskA \cap maskB\|}{\|maskA \cap maskB\|}$$

If the HD is zero then the irises are same and if the HD is one then the irises are different.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

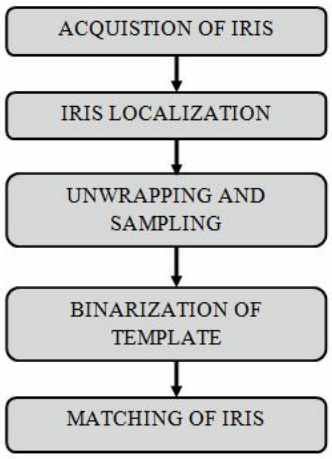


Figure 4. Steps Involved in Iris Recognition System

3.3FEATURE EXTRACTION FROM FACE BIOMETRICS

Face recognition matching is quite difficult because faces are multi dimensional and complex. Here, Eigen face method is used .It converts the full face image into small set of characteristic feature images.

The steps involved in face recognition are:

- Acquire the face images and calculate the eigenfaces, which define the face spaces.
- When a new face image is encountered, calculate a set of weights based on the input image.
- Determine if the image is a face at all (whether it is known or unknown) by checking to see if the image is sufficiently close to face space.

IV. TWOTIER SECURITY IN ATM SYSTEM

Due to some unavoidable reasons, the user can't able to prove himself as genuine user. At that time, the user needs to prove himself as a genuine person so the system generates another combination of biometrics for authentication to enroll the user as a genuine user with the onetime password generated by the database. Here the two level securities take place.

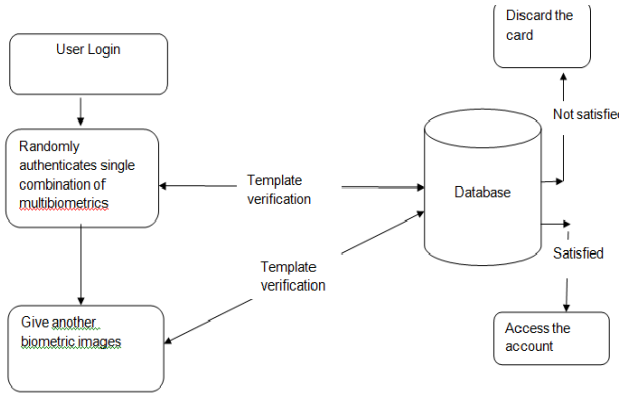


Figure 5: System Architecture diagram for two tier securities ATM system

4.1 DESCRIPTORS USED

4.1.1 FUZZY COLOR AND TEXTURE HISTOGRAM (FCTH)

It deals the extraction of a new low level feature that combines, in one histogram, color and texture information. This feature is named FCTH - Fuzzy Color and Texture Histogram - and results from the combination of 3 fuzzy systems. FCTH size is limited to 72 bytes per image, rendering this descriptor suitable for use in large image databases. It is appropriate for accurately retrieving images even in distortion cases such as deformations, noise and smoothing. It is tested on a large number of images selected from proprietary image databases or randomly retrieved from popular search engines. To evaluate the performance of the FCTH feature, the averaged normalized modified retrieval rank was used.

4.1.2 COLOR AND EDGE DIERCTIVITY DESCRIPTOR (CEDD)

The structure of CEDD consists of 6 texture areas. In particular, each texture area is separated into 24 sub regions, with each sub region describing a color. CEDD's color information results from 2 fuzzy systems that map the colors of the image in a 24-color custom palette. To extract texture information, CEDD uses a fuzzy version of the five digital filters proposed by the MPEG-7 EHD. The CEDD extraction procedure is outlined as follows: when an image block (rectangular part of the image) interacts with the system that extracts a CCD, this section of the image simultaneously goes across 2 units. The first unit, the color unit, classifies the image block into one of the 24 shades used by the system. Let the classification be in the color $m, m \in [0,23]$. The second unit, the texture unit, classifies this section of the image in the texture area $a, a \in [0,5]$. The image block is classified in the bin $a \times 24 + m$. The

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

process is repeated for all the image blocks of the image. On the completion of the process, the histogram is normalized within the interval [0,1] and quantized for binary representation in a three bits per bin quantization.

V. PERFORMANCE EVALUATION

This optimization model is evaluated in terms of its receiver operating characteristics (ROC) curve for test data sets. This enables the user to evaluate a model in terms of the trade-off between sensitivity and specificity. ROC matrices are used to show how changing detection threshold affects detection versus false alarms. If the threshold is set too high then the system will miss too much detection. Conversely, if the threshold is very low then there will be heavy false alarms. The percentage of detections classified correctly is plotted against the percentage of non –detections in correctly classified as detections (i.e. false alarms) as a function of the detection threshold. ROC is the best way to evaluate a detector [18].

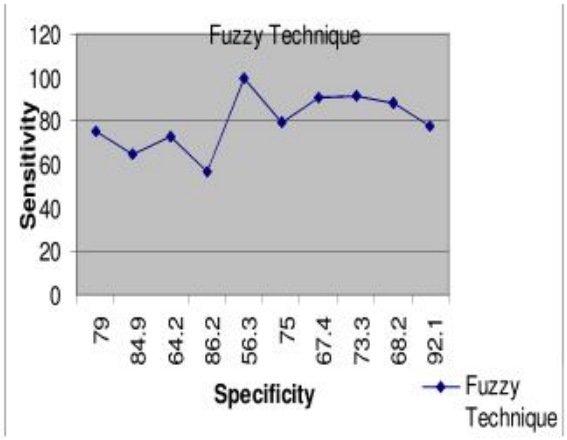


Figure 6: ROC of Fuzzy classifiers

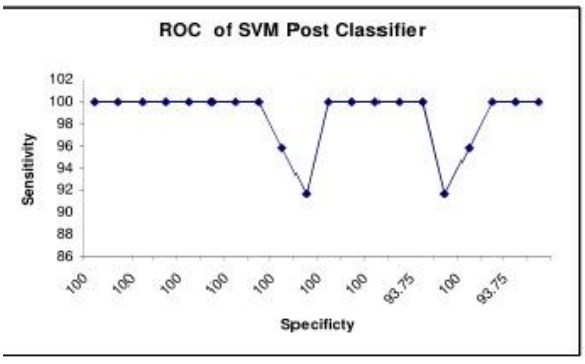


Figure 7: FOC of SVM classifiers

VI. CONCLUSION AND FUTURE WORK

A feature-level fusion framework for the design of multi biometric cryptosystems that simultaneously protects the multiple templates of a user using a single secure sketch. A realistic security analysis of the multi biometric cryptosystems has also been conducted. Experiments on two different multi biometric databases containing fingerprint, face, and iris modalities demonstrate that it is indeed possible to improve both the matching performance and template security using the multi biometric cryptosystems.

There are four critical issues that need to be investigated further:1) Embedding schemes for transforming one biometric representation into another, while preserving the discriminative power of the original representation; 2) a better feature fusion scheme to generate a compact multi biometric template that retains most of the information content in the individual templates; 3)methods to improve the security analysis by accurately modeling the biometric feature distributions; and 4) evaluation of the proposed cryptosystem on large multimodal database.

REFERENCES

[1] Abhishek Nagar, KarthikNandakumar and Anil K. Jain," Multibiometric Cryptosystems Based on Feature-Level Fusion", IEEE transactions on information forensics and security ,vol.7,no.1255-268,February, 2012.

[2] Adams Wai-Kin Kong, "Modeling Iris Code and Its Variants as Convex Polyhedral Cones and Its Security Implications", IEEE transactions on image processing, vol.22, no.3, March,2013.

[3] Arun Ross and RohinGovindarajan," Feature Level Fusion in Biometric Systems ", IJCSA, vol 45,no 13,July2012.

[4] BalajiKrishnapuram, Lawrence Carin, Ma´ rio A.T. Figueiredo, and Alexander J.Hartemink," Sparse Multinomial Logistic Regression: Fast Algorithms and Generalization Bounds".IEEE transactions on pattern analysis & machine intelligence, vol.27,no.6,June 2005.

[5] HarbiAlMahafzah, Ma'enZaidAlRwashdeh, "A Survey of Multibiometric Systems", IJCSA,vol 43,no 15,July2012.

[6] Kenneth Revett, PhD, "Behavioral biometrics, A Remote Access Approach", © 2008 John Wiley & Sons, Ltd. ISBN: 978-0-470-51883-0

[7] Moses OkechukwuOnyesolu, Moses Okechukwu Onyesolu,"ATM Security using fingerprint biometric identifier: An investigate study ", IJACSA, Vol.3, 4,2012.

[8] SabaraDinerstein, Jonathan Dinerstein, and Dan Ventura," Robust Multimodal Biometric Fusion via Multiple SVMs", IEEE

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

transactions on pattern analysis & machine intelligence, vol.29, no.8,June 2012.

[9] ShaikhAnowarul Fattah, Hafiz Imtiaz," A Spectral Domain Dominant Feature Extraction Algorithm for Palmprint Recognition", IJIP, vol 5, Issue 2, 2011.

[10] Umutuludag,Sharathpankanti,Salilprabhakar and Anil k. Jain,"Biometric Cryptosystems: Issues and Challenge"s,Proceedings of the IEEE,vol.92,no.6,June 2004 .

[11] Waheeda Al-Mayyan,"Performance Analysis of Multimodal Biometric Fusion",Ph.dThesis,DeMontfort University.2012.

[12] Yunhong Wang ,Li Ma, Tieniu Tan and Dexin Zhang," Personal Identification Based on Iris Texture Analysis",IEEE transactions on Pattern analysis & machine intelligence", vol.25, Issue 12,December 2003.

[13] S.Pravinthrja and K. Umamaheswari"Multimodal Biometrics for Improving Automatic Teller Machine Security", Bonfring International Journal of Advances in Image Processing, Volume 1, December, 2011.

[14] ChiragDadlani, Arun Kumar Passi, Herman Sahota and MitinKrishan Kumar, "Fingerprint Recognition Using Minutiae-Based Features",EE85I: Biometrics, Indian Institute of Technology, Delhi.

[15] Michael Boyd, DragosCarmaciu, Francis Giannaros, Thomas Payne and William Snell,"Iris Recognition", Imperial College London, MSc Computing Science Group Project, March 19, 2010.

[16] RoliBansal, PritiSehgal and PunamBedi "Effective Morphological Extraction of True Fingerprint Minutiae based on the Hit or Miss Transform", IJBB, Volume 4, Issue 2, 2010.

[17] B. Yanikoglu and Kholmatov, "Combining multiple biometrics to protect privacy", in Proc. ICPR-BCTP Workshop, Cambridge, August, England.

[18] A. Keerthi Vasan, R. Harikumar, M. Logesh Kumar,"Performance Analysis of Support Vector Machine (SVM) for Optimization of Fuzzy Based Epilepsy Risk Level Classifications Using Different Types of Kernel Functions from EEG Signal Parameters", Proceedings of the International MultiConference of Engineers and Computer Scientists 2009 Vol I IMECS 2009, March 18 - 20, 2009, Hong Kong.