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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

Security System in ATM using Multimodal Biometric System and Steganographic Technique

Prerana Kamble[1], Sangita Nikumbh[2]

P.G. Student, Department of Electronics & Telecommunication Engineering,YTIET, Bhivpuri Road, Karjat, India[1]

Professor, Department of Electronic Engineering, YTIET, Bhivpuri Road, Karjat, India[2]

ABSTRACT:The paper proposes to implement the biometric security system based on combination of iris and palm print with Steganographic technique for authentication purpose. Here the data hiding approach involves to conceal secret personal informatics within their biometric for still enhance the privacy protection. A Biometric system is essentially a pattern recognition system that makes use of biometric traits to recognize individuals. The most unique phenotypic feature visible in a person's face is the detailed texture of each eye's iris. Palm is the inner surface of a hand between the wrist and the fingers. Palm print is referred to principal lines, wrinkles and ridges on the palm. This system proposes a multi-resolution approach based on Wavelet Packet Transform (WPT) for texture analysis of iris and Weber's local descriptors based texture analysis of palm print will be proposed here. Weber local descriptor is used to represents the changes of illumination in an image and it determines the features such as differential excitation and gradient orientation. The development of this approach is motivated by the observation that dominant frequencies of iris texture are located in the low and middle frequency channels. The hand palm print image is aligned and cropped according to the key points. The palm print image is enhanced and resized. The features of palm print and iris are fused then compared with database image feature vectors and its recognized using Euclidean or Hamming distance. If this module is completed successfully then person information which contains person authentication number with four digits key will be matched with extracted data from already hidden image for second level security. Crime which is happening in ATM became a serious issue that affects not only customers but also bank operators. The main solution to this problem is Multimodal biometrics. Finally the multimodal system along with Steganographic approach shows the better performance accuracy for this automatic identification and authentication in ATM system.

KEYWORDS:Biometric, iris, palm, WPT, WLD, Stegnography.

I. INTRODUCTION

In a society, Authenticationis the act of confirming the truth of an attribute of a single piece of data (datum) or entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a website with a digital certificate, tracing the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labelling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification. There are many different types of authentication available today, one of them are biometric authentication that make use of biometric traits. “Biometric technologies” are automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioural characteristics. Merriam-Webster defines biometry as “the statistical analysis of biological observations and phenomena”. Biometrics is related to Human characteristics and traits, which are characterized as physiological versus behavioural characteristics. Physiological refers to the shaper of the body and include but at the same time not limited to finger prints, face recognition, DNA, Palm Print ,hand geometry, iris recognition and odor/scent. Behavioural Characteristics are related to personal behaviour of the person includes typing speed, gait, digital signature and voice. The traditional access control is based on tokens such as passport and

DOI: 10.15680/IJIRSET.2015.0404068

knowledge based identification system such as password or PIN. Today, the device will recognize the following biometric finger prints, hand geometry, retina and iris, voice, handwriting, blood vessels in the fingers and faceauthentication. If we combine multiple characteristics then we can design full and secured authentication system.As biometric technique, iris recognition and palm print recognition is getting preference over other methods and has drawn great attention of scientists because of uniqueness, non-invasiveness and stability of human iris patterns and palm print patterns.

There are various techniques which uses unimodal biometric traits for authentication purpose.Multimodal biometric systems use multiple sensors or biometrics to overcome the limitations of unimodal biometric systems. For instance iris recognition systems can be compromised by aging irides and finger scanning systems by worn-out or cut fingerprints. While unimodal biometric systems are limited by the integrity of their identifier, it is unlikely that several unimodal systems will suffer from identical limitations. Multimodal biometric systems can obtain sets of information from the same marker (i.e., multiple images of an iris, or scans of the same finger) or information from different biometrics (requiring fingerprint scans and, using voice recognition, a spoken pass-code). Multimodal biometric systems can integrate these unimodal systems sequentially, simultaneously, a combination thereof, or in series, which refer to sequential, parallel, hierarchical and serial integration modes, respectively.The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" defining it as "covered writing". There are various techniques which uses unimodal biometric traits for authentication purpose.

This paper proposes to implement the biometric security system based on combination of iris and palm print recognition using wavelet packet transform and WLD with steganography technique for authentication purpose.

II. Related Work

The research has focused on the single biometric trait for recognition and authentication. The palm is the inner surface of the hand between the wrist and the fingers. Early works in automatic palm print recognition utilized palm print images obtained off-line , while the newer systems typically obtain palm print image by using a scanner [6] or a CCD camera [5,7].Biometric trait like palm print has advantage like Noise Interference is less.
Several methods like Gabor filter, Sobel method, and Wavelet packet Transform, Fourier transform are available in the literature to extract. Shunyu Yang [1] proposes a real time personal identification based on Fourier transform for palm print recognition in which segmentation of hand gesture is done on which Fourier transform is applied for image processing. David Zhang[2] have used 2D Gabor algorithm in which lines and points are extracted from palms and it is considered as a texture image so an adjusted Gabor filter employed to capture the texture information on palm prints. Xiangqian Wu [3] used detectors to extract the line of palms in different direction and irregular lines are represented in this using chain code and palm prints are matched by matching the points on their palm lines.[4] helped in increasing overall system accuracy by reducing the (FAR) False Acceptance rate. The person authenticated by reference threshold is again verified by using second level authentication using MMTR method. Zhang et al. [5] developed an online palm print recognition system. Palm images are obtained using a CCD camera. A ring light source is used to ensure uniform light on the surface of the palm. After preprocessing and locating the palm region based on stabile points in the valleys between the fingers, the system extracts palm print features using a 2D Gabor filter.

Iris biometric technique as another trait to fuse it together for more security purpose,[8] shows the iris pattern recognition technique using wavelet packet transform and Morlet wavelet approaches that dominant frequencies of iris texture are located in the low and middle frequency channels, images are quantized into 1,0,-1 as iris signature. [9]Paper, it includes the preprocessing system, segmentation, feature extraction and recognition. Especially it focuses on image segmentation and statistical feature extraction for Iris Recognition, this method determines an automated global threshold and pupil centre.

Stegnography is also used in order to hide the personal information for second level security.[10]approaches to security and authentication of border crossing using unimodal biometric passport and the conclusion says that inclusion of multiple biometric identification information into machine readable passport will improve their robustness against identity and additional security measures are implemented in order to compensate for the limitation of the biometric technologies, so this paper approaches for multimodal biometric technique for authentication purpose.

Biometrics plays a major role in Automated Teller Machine (ATM) system, E-Commerce, Online banking, Passports. The growth in electronic transactions has been increased tremendously; there is a greater demand for fast and accurate user identification and authentication, to overcome the hacking activities, the proposed work is developed to provide protection to the biometric template and to enhance the security in the ATM system with Multibiometrics [12].

III. PROBLEM DEFINITION

Unimodal biometrics limitations

The unimodal biometric verification systems are more reliable than classical authentication systems. Unimodal biometric systems perform person recognition based on a single source of biometric information. Such systems are often affected by the following limitations and problems

• The lack of universality of some characteristics (for instance, in the case of fingerprints, approximately 4% of people cannot enlist because of weak fingerprints, and this per cent increases at 7% in the case of the iris).
• Noisy signals captured from the sensors due to the incorrect usage by the clients and due to the environmental conditions (humidity, dirt, dust etc.); the lack of the safety of the used sensors.
• The limitation of the discrimination of biometric systems due to a high in-class and low inter-class variability;
• The recognition performances of the systems are upper limited at a certain level;
• Unacceptable error rates for the unimodal biometric systems;
• The lack of permanence and variability in time of the biometric characteristics;
• The fraud possibility through voluntarily or involuntarily cloning (of) a biometric characteristic.

Multimodal systems

To over fulfill the mentioned problems and limitations the multimodal systems are used, leading to the improvement of the system's performances and the increase of the number of enlisted population in the systems and discouragement of fraud.
Multimodal biometric systems that have been proposed in references may be classified using four parameters:

-architecture;
- Sources that provide multiple evidence;
- Level of fusion;
- Methodology used for integrating the multiple verifiers

III.PROPOSED METHODOLOGY

Person authentication system based on multimodal biometric and Stegnography, it involve

- Data Protection system using bits wraps algorithm
- Iris with palm print recognition based on wavelet packet and webers local descriptor.

A generic biometric system has 4 main modules namely a) Sensor module, b) Feature extraction module, c) Matching module, d) Decision module. In a multimodal biometric system, information reconciliation can occur in any of the previously mentioned modules as a) Fusion at the sensor level where the combination of raw biometric data takes place b) Fusion at data or feature level, (data/features) where combination of different feature vectors are obtained.

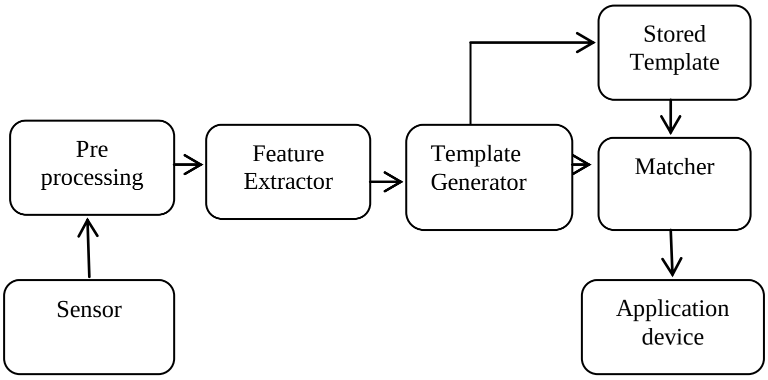


Fig1.Working of Biometric Authentication.

In the Physical world when we want to hide an object, we wrap it in some unmarked paper. This work is similarly done in the digital world but here we have the pixels in the cover image instead of wrap paper. Data Hiding is referred to as a process to hide data (representing some information) into cover media. That is the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data.

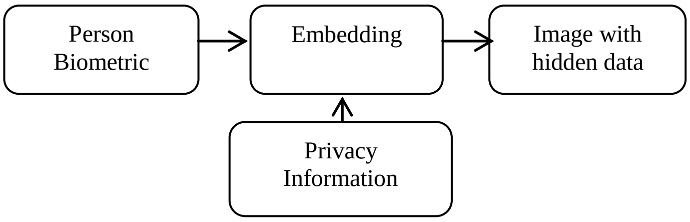


Fig 2.Individual Database Creation

In this module, the palm print and eye image samples are collected and stored into separated directory to identify the authorized person during recognition stage.

In that, stegnographic approach involved to wrap the secret data's within palm print biometric to improve the security level in person authentication.

Iris biometric will be included with palm print to reduce the problem of single biometric which may produce less accuracy in recognition.

To wrap the privacy information such as 4 digit and personal authentication number within palm, bits wrap method will be used.

Palm print Extraction

First process is to crop an input hand image with fixed width and height for extracting palm print for finding the features. Then an image will be applied to extract texture pattern with help of weber's local descriptor and statistical features. WLD is used to determine changes of illuminance conditions from an image and it is powerful tool in texture analysis.

It is determined from two characteristics such as, Differential excitation and orientation.

This descriptor represents an image as a histogram of differential excitations and gradient orientations, and has several interesting properties like robustness to noise and illumination changes, elegant detection of edges and powerful image representation.
WLD descriptor is based on Weber's Law. According to this law the ratio of the increment threshold to the background intensity is constant
Weber's Law, can be expressed as:

$$\frac{\Delta I}{I} = k,$$

Where ΔI represents the increment threshold (just noticeable difference for discrimination); I represents the initial stimulus intensity and k signifies that the proportion on the left side of the equation remains constant despite variations in theIterm. The fraction ΔI/I are known as the Weber fraction.

Iris analysis

An eye is selected as input first and before extraction, iris region is segmented out. From the input, iris is localized for segmentation and it is normalized as a rectangle matrix for texture analysis. The multi-level wavelet decomposition is applied to that rectangle matrix for multi resolution analysis to extract texture feature effectively. This various level decomposition will be used to provide the depth of texture and edges of an iris pattern. This will be characterized with the feature of energy which gives a uniformity level of gray level distributions.

LSB Embedding

This paper introduces a new, principled approach to detecting least significant bit (LSB) steganography in digital signals such as images and audio. It is shown that the length of hidden messages embedded in the least significant bits of signal samples can be estimated with relatively high precision. The new stegano approach is based on some statistical measures of sample pairs that are highly sensitive to LSB embedding operations. The resulting detection algorithm is simple and fast. To evaluate the robustness of the proposed stegano approach, bounds on estimation errors are developed.

Recognition

- At recognition stage, features from input images (palm print and iris) are combined to form a common feature vector.
- Before matching process, the same features are extracted from available iris and palm print pair of database.
- The first level of recognition is to match the input features with database image features to identify the authorized person. After this process, the keys are required i.e., 4digit key and 16digit PAN to match with extracted keys from database palm prints for second level of final authentication.
- Matching process will be performed using Euclidean distance and search desired minimum value for identification.
- Euclidean distance measures the similarity between two different feature vectors using
- **ED=** $\sqrt{}\sum_{j=0}^{j}(\boldsymbol{FV1,j-FV2,j})\mathbf{2}$

  Where J is the length of the feature vector, FVi is the feature vector for individual i.

DOI: 10.15680/IJIRSET.2015.0404068

Secret Code Wrap Approach

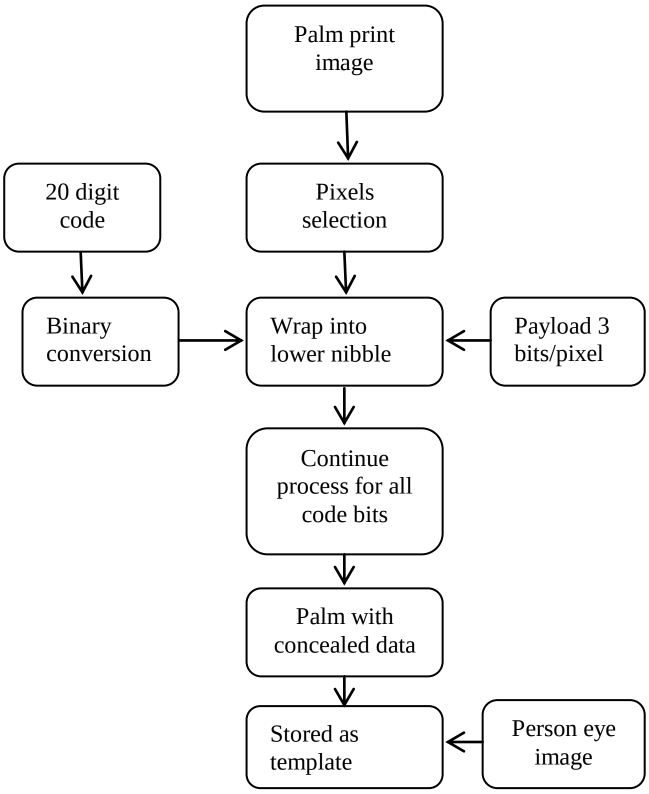
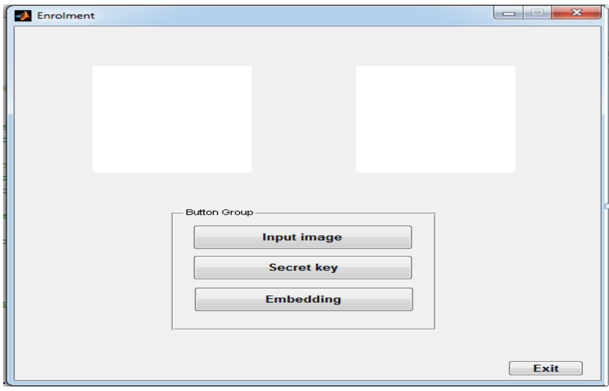
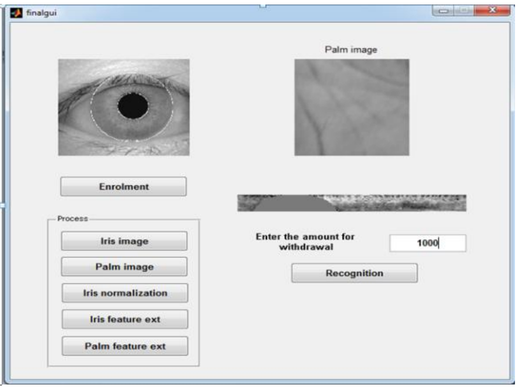


Fig 3 Secret codes wrap approach

V.RESULTS



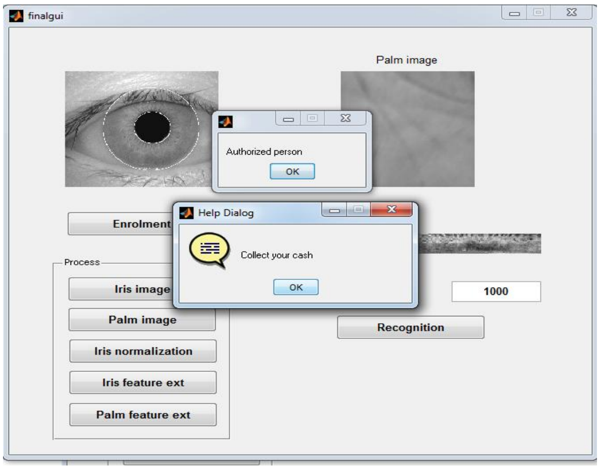
(a)



Enter the amount for withdrawal 1000

(b)

DOI: 10.15680/IJIRSET.2015.0404068



Authorized person

Collect your cash

1000

(c)

Fig 4 (a) Enrolment window ,In enrolment window we enrol the customer using their customer id and iris, palm image with secret key embedded in it.(b) recognition procedure windowThis window is shown during recognition procedure in which images are scanned and extraction procedure is applied on them and amount is entered which is to be withdrawn from ATM.(c) final window in which procedure is completed

IV.CONCLUSION

Multimodal security system for recognition and authentication purpose using iris and palmprint biometric traits by Wavelet Transform and Weber's Local Descriptor, in ATM system, this system provides better data protection and less complexity. This system gives more security compared to unimodal system because of two biometric features, and steganography technique enhances more security .Thus it can be used in defences system and any privacy protection security system.

REFERENCES

[1] Shyunyu Yang "A real time personal identification based on Fourier transform of palm print recognition"978-0-7695-4606-3/11 IEEE 2011.
[2] Wai Kin Kong, David Zhang and Wenxin Li" Palmprint Feature Extraction Using 2-D Gabor Filters" Prof. David Zhang Biometrics Research Centre Department of Computing The Hong Kong Polytechnic University Hung Hom, Kowloon, Hong Kong.
[3] Xiangqian Wu, David Zhang, Kuanquan Wang," Palm Line Extraction and Matching for Personal Authentication" 1083-4427 © 2006 IEEE
[4]Jyoti Malik, Rusundharatna Dahiya and G. Sainarayanan" Fast Palmprint Authentication by Sobel Code Method**"** ICTACT Journal on Image and Video Processing, ay 2011, Volume: 01, Issue: 04, ISSN: 0976-9102(Online) ICTACT JOURNAl.
[5] D. Zhang, W.K. Kong, J. You, and M. Wong, "Online Palm Print Identification", IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 25, No. 2, pp. 1041-1050, 2003
[6] C. C. Han, H. L. Cheng, K. C. Fan and C. L. Lin "Personal Authentication Using Palm-print Features", Pattern Recognition, Vol. 36, pp. 371-381, 2003.
[7] J. Daugman, "How Iris Recognition Works, IEEE Tran.Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 21 – 30, 2004.
[8] S.Hariprasath, V.Mohan" Biometric Personal Identification Based on Iris Pattern Recognition Using Wavelet Packet Transform" 978-1-4244-6589-7/10/ ©2010 IEEE
[9] Khin Sint Sint Kyaw"Iris Recognition System using statistical features for Biometric Identification**"** 978-0-7695-3559-3/09 2009 IEEE
[10]P.Prabhusundar, V.K.Narendra Kumar "Border Crossing Security and Privacy in Biometric Passport using Cryptographic Authentication Protocol"978-4673-2907-1/132013 IEEE.
[11] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004
[12] KardeArchana, Dr.A.Govardhan"Enhance the Security in the ATM System with Multimodal Biometrics and Two-Tier Security "Volume 3, Issue 10, October 2013 ISSN: 2277 128X