IMAGE PROCESSING BASED FINGER-VEIN BIOMETRIC RECOGNITION SYSTEM

R.Rahini*

Dr. P. Suresh M.E., PhD.,**

***Abstract*—**

Finger vein biometrics is a new approach of personal identification. It receives more attention today. It improves the security of mobile devices, laptops, ATMs and also it provide high security for defence purposes. The first task of identification process using finger-vein patterns is extracting the region of interest (ROI) from the near infrared finger image which get from imaging sensor. Knowing the person with whom you are conversing is an important part of human interaction and one expects computers of the future to have the same capabilities. This system consists of four modules, namely image acquisition, pre-processing, feature extraction, and matching. The feature extraction is done with the help of wavelet decomposition and matching is done with the help of Hausdorff Distance. This system is going to implement on embedded platform for real time application.

* PG Student of Mechatronics, Karpagam College of Engineering, Coimbatore.

** Professor- Mechanical Engineering, Karpagam College of Engineering, Coimbatore.

INTRODUCTION

Today the main threat in the security of any system is the possibility of intruders into the system. This can be overcome by some of the authentication schemes by mean s of portable devices such as personal tokens, identification cards or else based on the passwords. These devices have many constrains in case of performance, also there is the possibility of simulating these cards by intruders. In case of security by password, the password can be guessed or broken by simple dictionary attacks.To overcome the disadvantages of the above we move on to the biometric system. Nowadays biometric system has become more popular and alternative to the traditional systems. Compared to the traditional identification/verification methods such as photo or magnetic swipe identification (ID) cards, the use of biometrics is often more convenient for users, has lower costs for businesses, reduces fraud, and is more secure [1] and also it is the friendly way of providing security. Nowadays it attracted more attention and becoming one of the most popular and promising alternative to solve the problems of traditional methods. It is difficult to forge biometrics. There are number of biometric identification techniques have been developed for various commercial applications. Biometrics security such as finger print, palm print, iris, face, voice and signatures are already developed and implemented. But these biometric systems have some of the disadvantages and also the intruders are well trained to attack these systems now. So currently many researches are going on to protect these biometric systems from the attackers. Hence it is quite good to move on to the new method with high security.

In this paper we introduce a finger vein biometric system. This is the new and promising biometric identification system which is more secure and more convenience when compared with the existed biometrics.

While implementing the biometric system there are number of issues that should be considered, including:

• *performance*, which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed;

• *Acceptability*, which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;

• *Circumvention*, which reflects how easily the system can be fooled using fraudulent methods [2].

LITERATURE

A. Iris Recognition

A large number of iris biometric identification techniques have been developed and there are several literatures available for Iris recognition. Iris recognition combines computer vision pattern recognition,statistics, and the human-machine interface[1]. The iris recognition system involves a number of steps: First, a camera acquires an image of an eye. Next,the iris is located within the image. The annular region of the iris is "unwrapped," or transformed from raw image coordinates to normalized polar coordinates. A texture filteris applied to a set of locations on the iris, and the filterresponses are quantized to yield a binary iris code. Finally,the iris code is compared with a known iris code in thegallery, and a similarity or distance score is reported. In anidentity-verification application, the system uses the reportedscore to decide whether the two compared iris codesare from the same subject or from different subjects [3].

B. Periocular biometrics

Periocular biometrics is the recognition of individuals based on the appearance of the region around the eye which include eyelids, eyelashes, eyebrows, and the neighbouring skin area.Periocular-surrounding the eyeball but within the orbit. Periocularrecognition may be useful in applications where it is difficult to obtain a clear picture of an iris for iris biometrics, or a complete picture of a face for face biometrics [4].

C. Voice Recognition

Voice is a combination of physiological and behavioural biometrics.The Speech is most prominent & primary mode of Communication among of human being. The communication among human computer interaction is called human computer interface. Speech has potential of

being important mode of interaction with computer [5]. Voice Recognition is a biometric modality that uses an individual voice for recognition purpose. The features ofan individual's voice are based on the shape and size of the appendages (e.g., vocal tracts,mouth, nasal cavities, and lips) that are used in the synthesis of the sound. A popular choice for remote authentication by speech is due to the availability of devices for collecting samples and its ease of integration. Speech Recognition is the process of converting speech signal to a sequenceof words by means Algorithm implemented as a computerprogram.

D. Finger print Recognition

Fingerprint identification is one of the most well known and publicized biometrics. Humans have used fingerprints for personal identification for many centuries, more recently becoming automated due to the advancement in computing capabilitiesand the matching accuracy using fingerprints has been shown to be very high. A fingerprint is an impression of the friction ridges of all or any part of the finger.Multiple fingerprints of a person provide additional information to allow for large-scale recognition involving millions of identities. The traditional method uses the ink to get the finger print onto a piece of paper. This piece of paper is then scanned using a traditional scanner. Now in modern approach, live finger print readers are used .These are based on optical, thermal, silicon or ultrasonic principles [6].Normally a bank of Gabor filters, orientated to different angles are applied to the image to clean it from noises that can result on false alarms or authentication mistakes [7].

E. Face Recognition

Face recognition biometrics has not reached up to the level of fingerprint recognition biometrics. Face recognition is a non-intrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The major advancement in the past ten years has propelled the face recognition technology into the spotlight. Facial recognition technologies have recently developed into two areas and they are Facial metric and Eigen faces. Facial metric technology relies on the manufacture of the specific facial features.

The Eigen Face method is based on categorizing faces according to the degree of it with a fixed set of 100 to 150 Eigen faces. [6].

F. Signature Recognition

Signature Recognition examines behavioural aspects. Signature Recognition comes under behavioural recognition. Dynamic signature is the biometric modality that uses for recognition purpose, the anatomic and behavioural characteristics that an individual exhibits when signing his or her name. Most signature verification systems require either the use of electronic tablets or digitizers for online capturing or optical scanners for offline conversion. These interfaces are bulky and require the presence of dedicated hardware. Cameras, on the other hand, may be made as small as a pen cap and are becoming ubiquitous in the current computer environment [12].

SUMMARY OF LITERATURE REVIEW

In case of iris recognition system because of the uniqueness of the iris the possibility of making the artificial duplicating of iris is highly impossible. The disadvantage in the iris recognition system is when the iris image is captured at some distance the performance of the system get affected, also the performance is affected for the blind and contracts. In case of periocular recognition the acquisition of the periocular image does not require high user cooperation and close capture distance [4]. Since it is a new field, it needs more literature. The main advantages of voice recognition system is that the hardware we use for recognition is not very expensive, also it can be used remotely by means of telephone lines. Also it does not require high sampling rate. The main disadvantage in this recognition is accuracy gets reduced by background noise. It can be affected by emotion states and physical condition because it is based on behavioural characteristics. Also speech detection is complicated by variation from speaker to speaker and from session to session for the same speaker [11]. In case of finger print recognition system, although finger print can be widely used for biometric purposes, it can be affected by moisture, as the moisture significantly influences the capacitance. This shows that too wet or too dry fingers have the problem with these silicon figure print reader [6] also the finger print can be easily hacked by the intruders. The face recognition system has not reached up to the level of

finger print recognition but it increases the user friendliness in human computer interaction [8], it is not widely used, but when compared with the finger print recognition system the accuracy of this system improves with time, but it has not been very satisfying so far. Also there is a need for improvement of algorithm used for face recognition. This system can be widely used identification method in e-passports [9]. The main disadvantage of this system is, it have the problem to distinguish twins. The performance of face recognition and/or authentication systems isgreatly affected by within-person variations encountered in human faces [10].In case of Signature recognition technique theperson does not make a signature consistently thesame way. So, the data obtained from a signature of a person has to allow for quite somevariability. Most of the signature dynamics systems verify the dynamics only. They do notpay any attention to the resulting signature. A few systems claim to verify both (i.e. thesignature dynamics as well as the resulting signature look itself). The system does not verify the resulting dynamics vs. signature, then the signature that is accepted as a true match may look significantly different from the master template. The speed of writing is often the most important factor in the decision process, so it is possible to successfully forge a signature even if the resulting signature looks so different that any person would notice. The size of data obtained during the signing process is around 20 KB. The size of the master template, which is computed from 3 to 10 signatures, varies from around 90bytes up to a few kilobytes. If the size of the master template is relatively high the signaturerecognition has problems with match discrimination and thus is suitable for verification only the accuracy of the signature dynamics biometric systems is not high, the crossover rate published by manufacturers is around 2% [6].

MOTIVATION

In most existing biometric system, it have high complexity in time or space or both and thus not suitable for mobile devices. The biometric patterns already available are susceptible to forge and they can be copied and used to create artificial that can look like currently available biometric pattern. The finger prints and palm prints are usually frayed; voice, signatures, hand shapes and iris images are easily forged; face recognition can be made difficult by occlusions or face-lifts [15]. Due to the limitations mentioned above, new approaches have been proposed to overcome the existing problems. As a newly emerging biometric technology, finger vein recognition has

attracted more attentions in personal identification;it has inherent superiority on accuracy, speed, maintenance, sanitation and high security. The finger-vein is blood vessel network under finger skin, which is almost impossible to counterfeit and is believed to be quite unique for each individual, even in the case of identical twins and even between the different fingers of an individual. Compared with other biometric traits, the finger-vein has the following advantages [14]: 1.The vein is hidden inside the body and is mostly invisible to human eyes, so it is difficult to forge or steal. 2. The non-invasive and contactless capture of finger-veins ensures both convenience and hygiene for the user, and is thus more acceptable. 3. The finger-vein pattern can only be taken from a live body. Therefore, it is a natural and convincing proof that the subject whose finger-vein issuccessfully captured is alive.

Based on the advantages of finger-vein identification technique, we propose a novel security system using finger-vein technology. Here we are going to design this for mobile devices.

METHODOLOGY

The proposed system consists of four modules: 1. Image acquisition, 2. Pre-processing, 3. Feature extraction, 4. Matching.

A. Image acquisition

In this stage, finger-vein image is capture. The finger vein image is capture with the help of near-infrared camera. Because patterns of the vein cannot be observed using normal, visible rays of light since they are hidden by the skin.The finger-vein image capture device mainly consists of near-infrared light source, lens, transparent acryl and light filter. Here light-emitting diode (LED) or laser was used as the illumination source for NIR light. However, vein patterns can be viewed through an image sensor which is sensitive to near-infrared light (wavelengths between 700 and 1000 nanometres), because near-infrared light passes through human body tissues and are blocked by pigments such as haemoglobin or melanin. As haemoglobin exists densely in blood vessels, near-infrared light shining through causes the veins to appear as dark shadow lines in the near- infrared image. This vein image is then subjected to the pre-processing. This can be done by using MATLAB.

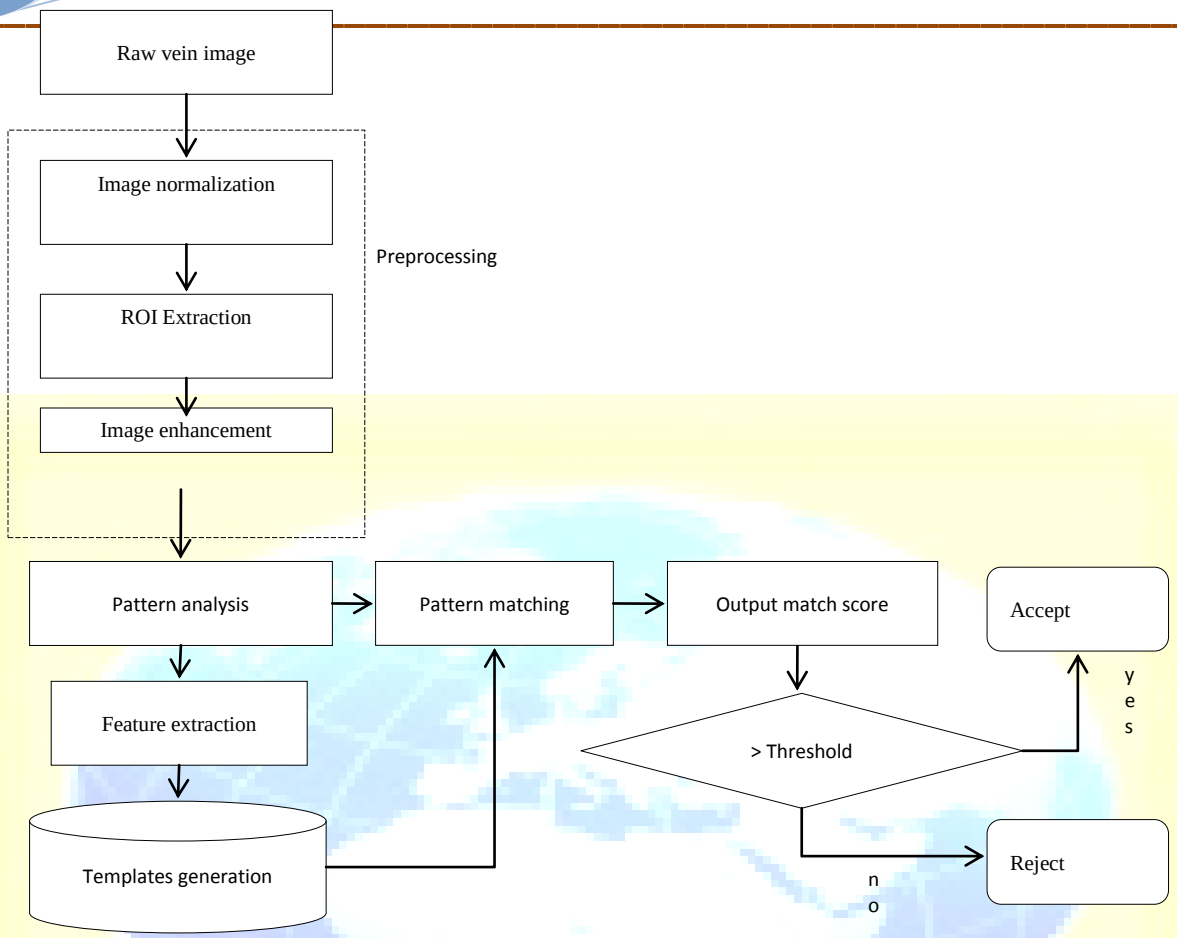
Raw vein image
Image normalization
ROI Extraction
Image enhancement
Preprocessing
Pattern analysis
Pattern matching
Output match score
Accept
Feature extraction
> Threshold
yes
Templates generation
Reject
no

Fig. Flow chart of our system.

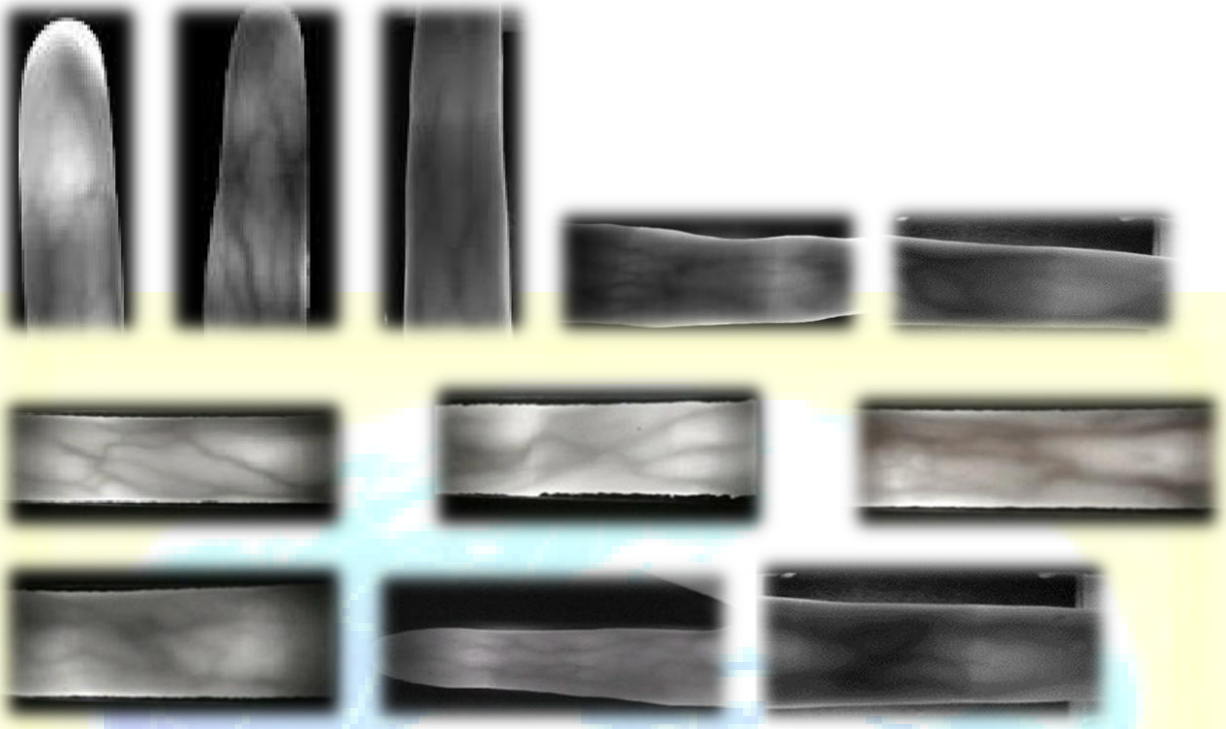

Fig. Raw finger-vein image captured by NIR camera.

B. Pre-processing

The acquired finger-vein images are firstsubjected to pre-processing steps, which automatically extract the region-of-interest (ROI) images.In this stageImage segmentation and enhancement process are done by using Image processing technique. Here we use MATLAB software to process the image.

C. Feature extraction

The segmented finger-vein image is not clear, so it is enhanced to improve the contrast of the image. The image is resized to 1/4th of the original size and then histogram equalization is used for enhancing the grey level contrast of the image. The finger-vein patterns are extracted by calculating various parameters like vein Width, Length, Position, Pixels and Intersection points of vein. They are then stored as templates for feature extraction. Wavelet decomposition is used for feature extraction of the image.

D. Matching

If the extracted image value greater than the threshold value, then the image is from the authorized person. If the extracted image value less than the threshold value, then the image not belongs to the authorized person. After did the coding in MATLAB, in the GUI window make the block for image restoration, histogram equalization, feature extraction and matching. The hardware parts are implemented in embedded platform.

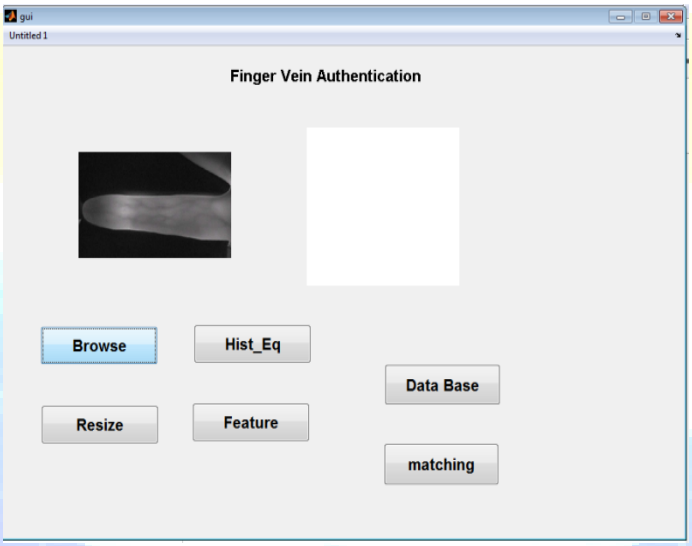

Fig. Input image.

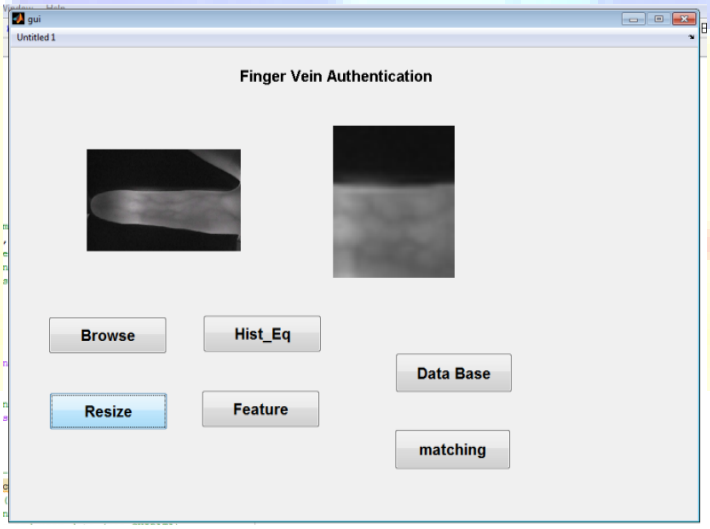

Fig. Resizing.

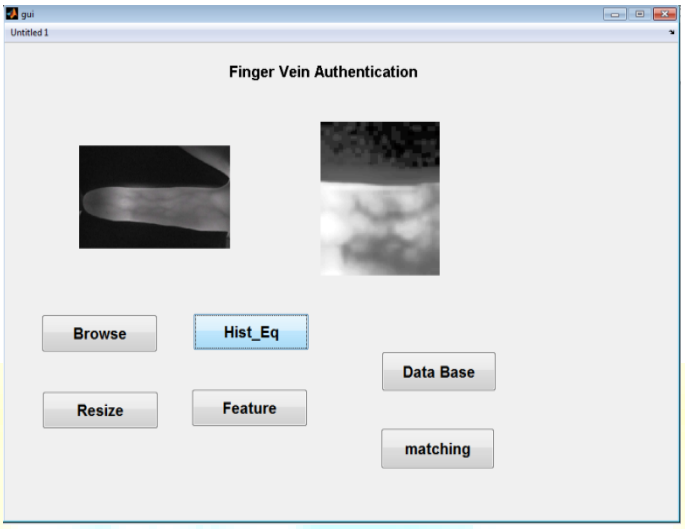

Fig. Histogram Equalization.

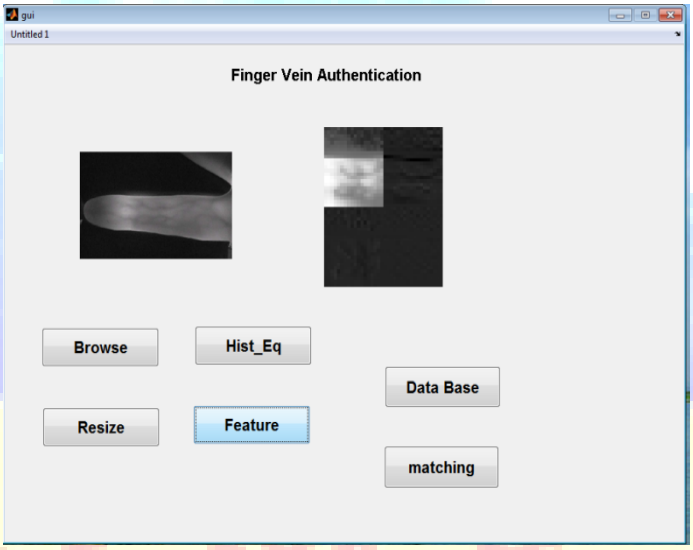

Fig. Feature Extraction.

CONCLUSION

This paper proposes a finger vein recognition system which is a promising biometric. The proposed system consists ofNIR camera for capturing finger-vein images. MATLAB software is used for processing the images. The proposed system is more advantageous because it is highly secured. Since we are going to implement this system on embedded platform the power consumption is highly reduced, so thissystem is suited for mobile devices, also it is suited for security of ATM machine, defence purposes. This can be used for personal identification.

REFERENCES

[1] Robert W. Ives, Yingzi Du, Delores M. Etter and Thad B. Welch, "A Multidisciplinary Approach to Biometrics", IEEE Transactions On Education, Vol. 48, No. 3, August 2005.

[2] Anil K. Jain, Arun Rossand Salil Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems For Video Technology, Vol. 14, No. 1, January 2004.

[3] Karen P. Hollingsworth, Kevin W. Bowyer and Patrick J. Flynn, "Improved Iris Recognition through Fusion of Hamming Distance and Fragile Bit Distance", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 33, No. 12, December 2011.

[4] P.Fasca Gilgy Mary, P.Sunitha Kency Paul, J.Dheeba, " Human identification using periocular biometrics", ISSN: 2278 – 7798 International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 5, May 2013.

[5] Santosh K.Gaikwad, Bharti W.Gawali, Pravin Yannawar, "A Review on Speech Recognition Technique", International Journal of Computer Applications (0975 – 8887) Volume 10– No.3, November 2010.

[6] Debnath Bhattacharyya1, Rahul Ranjan, Farkhod Alisherov A, and Minkyu Choi, "Biometric Authentication: A Review", International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009.

[7] Alfredo C. López, Ricardo R. López, Reinaldo Cruz Queeman, "Fingerprint Recognition".

[8] Shang-Hung Lin, "An Introduction to Face Recognition Technology",informing science special issue on multimedia informing technologies-part2, vol. 3 No-1, 2000.

[9] Haiping Lu, Karl Martin, Francis Bui, K. N. Plataniotis, Dimitris Hatzinakos, "Face Recognition with Biometric Encryption for Privacy-Enhancing Self-Exclusion".

[10] Andreas Lanitis, "Facial Biometric templates and aging: problems and challenges for artificial intelligence", AIAI-2009 Workshops Proceedings.

[11] P. A. Tresadern, C. McCool, N. Poh, P. Matejka, A. Hadid, C. Levy, T. F. Cootes and S. Marcel, "Mobile biometrics (MiBio): Joint Face and Voice Verification for a Mobile Platform".

[12] Mario E. Munich and Pietro Perona, "Visual Identification by Signature Tracking", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 25, No. 2, February 2003.

[13] Ravi Das, "Signature recognition", Keesing journal of documentation and identity, issue 24, 2007.

[14] Nicolae Duta, Anil K. Jain and Kanti V. Mardia, "Matching of Pattern Recognition" Letters 23, 2002, pp. 477-485.

[15] Y. Kim, J. Yoo, and K. Choi, "A motion and similarity-based fake detection method for biometric face recognition systems," IEEE Transactions on Consumer Electronics, vol.57, no.2, pp.756-762, May 2011.