An Introduction to Multimodal Biometric System: An Overview

Mamta Ahlawat[1] Dr. Chander Kant[2]
[1]Research Scholar [2]Assistant Professor
[1,2]Department of Computer Science and Application
[1,2]K.U., Kurukshetra, India

Abstract— Multimodal biometric system uses more than one biometric trait for authentication to individual. Unimodal biometric system uses a single biometric trait (fingerprint, face, hand geometry, iris, retina, voice, gait, signature etc.) for authentication (either verification or identification) of user. Unimodal biometric system have some limitations like noise in sensed data, intra-class variation, inter-class variations, distinctiveness, spoof attacks etc. So unimodal biometric system is less secure and less reliable. Some of limitations imposed by unimodal biometric system can be overcome by including multiple traits of individuals. Such systems, known as multimodal biometric system, are more reliable and securable due to presence of multiple traits. This paper represents a brief introduction of multimodal biometric system.

Key words: Fusion Levels, Multimodal Biometric System, System Modules

I. INTRODUCTION

Multimodal biometric is a technique by which two modalities (for e.g. face and fingerprint) of a single user combined to acquire higher secure and reliable authentication of the user. For example, before one year while making of aadhar card, system asked us to give our iris, face and fingerprint as for identification. The combination of these two or more types of biometric information trait, this information keep the advantage of the proficiency of each individual biometric trait and help to meet rigid performance requirements, reliability, security and robustness against attacks. As shown below figure 1, two biometric traits are used for verification and identification. One of the traits is fingerprint that acquires by a sensor and extracts its feature set for matching it to stored template of fingerprint in the database. Another trait is the face that acquires by a digital camera and extracts its landmarks then match with stored face templates in the database. After matching process finish there should be fusion strategies to combine both decision and put a perfect result to system or individual. Multimodal biometric system tries to provide higher security, reliability, acceptability, easy to measure and less circumvention. Multimodal and Multibiometric systems both are different as Multibiometric system use more than one phase of a single biometric trait (example:left face, right face, centre face) on the other hand multimodal system uses more than one biometric trait of an individual (example: face and fingerprint).

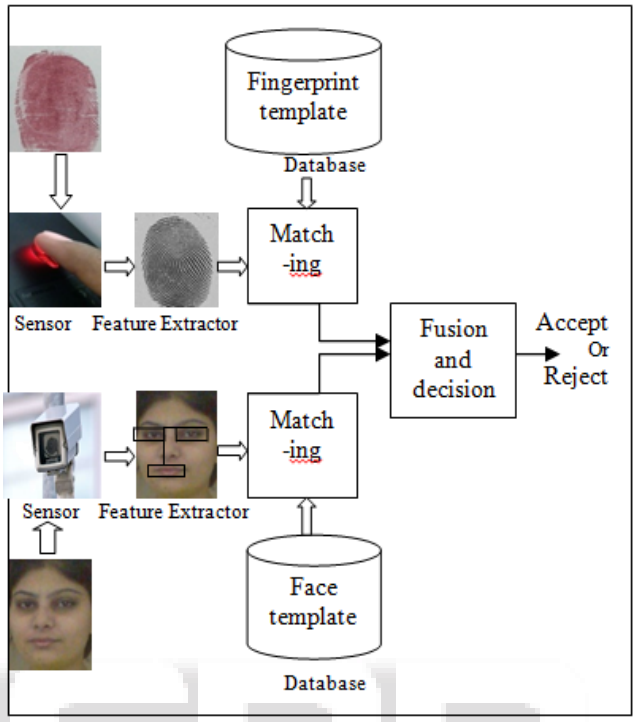

Fig. 1: Multimodal Biometric System

To overcome limitations of unimodal; multimodal biometric system provides a higher security and reliability over unimodal biometric system [2].

A. Limitations of Unimodal biometric:

Some of the commonly challenges encountered by biometric systems are listed below:

1) Noise in Sensed Data:

Noisy data may result from defective or improperly maintained sensors or unfavourable ambient conditions or by human beings variations in their biometric traits. Noisy biometric data may not be successfully matched with corresponding templates in the database, result a genuine user being incorrectly rejected.

2) Intra-Class Variations:

It is caused by an individual who is incorrectly interacting with the sensor or due to change in biometric characteristic over a period of time. Although it can be handled by updated these template over time but can't be fully remove this limitation.

3) Inter-Class Similarities:

Overlap of feature spaces corresponding to multiple classes or individual.

4) Distinctiveness:

When a biometric trait is expected to vary significantly across individuals, there may be large inter-class similarities in the feature sets used to represent these traits.

5) Non Universality:

Whenever every user is expected to possess the biometric trait being acquired, in reality it is possible for a subset of the users to not possess a particular biometric.

6) Spoof Attacks:

An impostor may attempt to spoof the biometric trait of a legitimate enrolled user in order to circumvent the system and this attack is especially relevant when behavioural traits such as voice and signature are used. However, physiological traits are also susceptible to spoof attacks [1].

B. Why Multimodal Biometric System?

Over the limitations of unimodal biometric system multimodal biometric system provide some advantages and more enhance security and acceptability.

1) Accuracy:

Multimodal biometric acquires information from two or more biometrics trait – (e.g. fingerprint and face; or face and iris) whereas unimodal biometric systems acquire information from one biometric trait– (e.g. fingerprint, face, iris, signature, voice, hand geometry, etc.). The accuracy of multimodal biometric system is basically calculated in terms of image acquisition errors and matching errors. Image acquisition errors consist of failure-to-enroll (FTE) rate and failure-to-acquire (FTA) rate whereas comprise FNMR (false non-match) rates in which a legitimate user is rejected and a (FMR) false match rate in which an impostor is authorized to access. Multimodal biometric systems have almost zero FMR, FTE & FTA rates because in this system, each and every subsystem has a determination on the person's claim. The decision module uses different fusion strategies to combine each single subsystem decision and generate a conclusion. This is the true reason that multimodal biometric systems are more accurate than unimodal or any other traditional authentication system.

2) Increased and Reliable Recognition:

A multimodal biometric system authorized a greater level of confidence for an accurate match in identification as well as verification modes. As multimodal biometric systems uses multiple biometric traits, each single biometric trait can offer additional proof about the authenticity of any user's claim. For example, the patterns of movements (gait) of two persons of the same family or by coincidentally of two different persons can be similar. In this particular situation, a unimodal biometric system that depends only on gait pattern analysis might lead to a false recognition. If the same biometric trait additionally includes fingerprint matching then the system would absolutely results in increased recognition rate, because it is nearly impossible that two different persons have same gait as well as fingerprint pattern.

3) Enhanced Security:

In Multimodal biometric system, use of multiple methods of identification and verification, a system can acquire higher degree of threshold recognition and a system administrator can get a decision on the accurate level of security that is important. For an extremely high security point of view, you can use up to three biometric identifiers of an individual and for a lower security point of view; you could possibly require one or two biometric identifiers. If one of the attribute fails for any unknown reason although your system can still use another one or two of them in order to provide the accurate identification and verification of a person.

4) Vulnerability:

Spoof attacks are the biggest threat to authentication systems. Unimodal as well as Multimodal biometric systems are sometimes vulnerable to spoof attacks. Spoofing occurs whenever an unauthorized user has the capacity to authenticate as an authorized user. The potential threats due to artificial or fake fingers were examined by another experiment and researcher's team as exhibited that artificial fingers made with plastic molds could possibly enroll in the 11-12 tested fingerprint systems and were being accepted in the identification and verification procedures with the major probability of 68-100%, depending on the biometric system. In this case, alternative hardware device that depends on simultaneous multimodal authentication such as a biometric smart fingerprint scanner with liveness detection with the help of temperature sensing can remove spoofing. "Liveness" can be describes the capacity of a multimodal biometric system to distinguish between a fake and a living sample and is generally done by measuring biometric features like humidity, blood flow, pulse, temperature, etc.

e) User Acceptance: As already mention above multimodal biometric systems are more reliable, accurate, ability to avoid spoofing attacks, have good security options, and this type of systems are more widely accepted by many countries. However, in deployments of large countries where accuracy and security are paramount, no matter how small size, multimodal systems have become ubiquitous and necessary [2].

II. BIOMETRIC SYSTEM MODULES

Generally biometric system can be viewed as having four modules: a sensor module; a quality assessment and feature extraction module; a matching module; and database module as shown below figure:

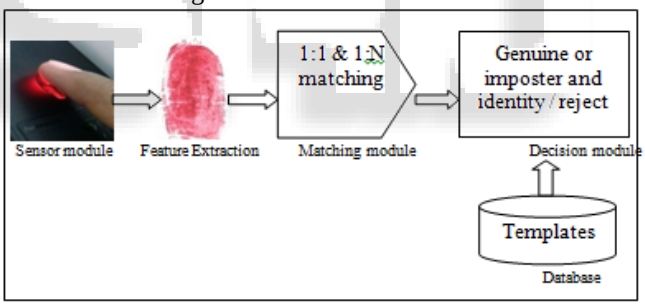

Fig. 2: Biometric System Modules

Each module is described below:

1) Sensor module:

A suitable biometric sensor is required to acquire the raw biometric data of an individual. For example, to acquire fingerprint images, an optical fingerprint sensor may be used to acquire ridges structure of the fingertip.

2) Quality assessment and feature extraction module:

The quality of the biometric data acquired by the sensor is assessed in order to determine its suitability for further processing. Sometimes, the quality of the acquire data may be so poor that the user is asked to present the biometric data again. The biometric data is then processed and a set of salient features extracted to represent the identity. For example, the position and orientation of minutia points (ridge and valley anomalies) in a fingerprint image are extracted by the feature extraction module in a fingerprint-based biometric system. During enrolment process, this feature set is stored in the database and is commonly known as a template.

3) Matching Module:

The extracted features are now compared against the stored templates in database to generate match scores. In a fingerprint-based biometric system, the no. of matching minutiae between the input and the stored template feature sets is computed and a match score generated. It may be one to one matching that is verification or one too many matching that is identification.

4) Decision Module:

Decision module generates output based on match score as in matching module. In verification process, the output is either imposter or genuine. In identification process, the output is either identity or reject. In both cases the low match score is emitted to the system [3].

A. Fusions in Multimodal Biometric:

Fusion is a mechanism that can combine the all classifications of result from different media/channels. Multimodal biometric system can acquire the two or more biometric traits to increase its strength due to present multiple traits and difficult to forge. The performance of the multimodal system is examined in term of image acquisition errors and matching errors. Matching errors are false match rate (FMR), in which an impostor user's sample matches with a legitimate user's template, and False Non Match Rate (FNMR), in which a legitimate user's samples don't match her/his own template. Image acquisition errors are Failure to Enrol (FTE) which is defined as a person unable to successfully enrol himself in a biometric system and Failure to Acquire (FTA) in which a person unable to provide a good quality of biometric trait at verification and identification [4].

There are various levels of fusion as defined below:

1) Sensor Level Fusion:

At sensor, the raw data acquired from multiple sensors (for e.g. one sample from optical sensor and other sample from solid state sensor) and from multiple traits (for e.g. one sample of face and another sample of fingerprint) and combine to generate a new biometric data from which a feature set can be extracted.

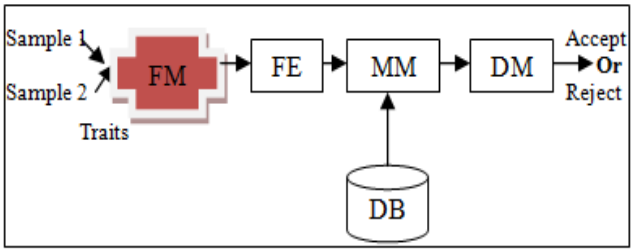

Fig. 3: Sensor Level Fusion

Figure 3 indicate, sensor level fusion as different biometric samples as inputs in sensor. Where FM: Fusion Module, FE: Feature Extraction module, MM: Matching Module, DM: Decision Module, DB: Database.

2) Feature Extraction Level Fusion:

At feature level, a set of features are extracted from different biometric traits can be fused by using a specific fusion algorithm and to form a composite feature set of that biometric traits. For e.g. a feature set of fingerprint and face can be combined. Fusion at Feature level is better than other fusion level and to increase accuracy of result.

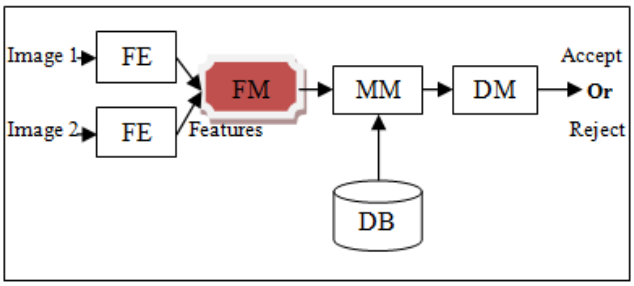

Fig. 4: Feature level Fusion

Figure 4 indicate the feature extraction level fusion where both channels feature set are fused for further processing. Where FM: Fusion Module, FE: Feature Extraction module, MM: Matching Module, DM: Decision Module, DB: Database.

3) Match Score Level Fusion:

At matching module, different sample's feature set is compared with the templates stored in the database and a match score is generated. After match score generated, fusion is apply and both match scores are combined to generate a new match score and then this new match score send to decision module.

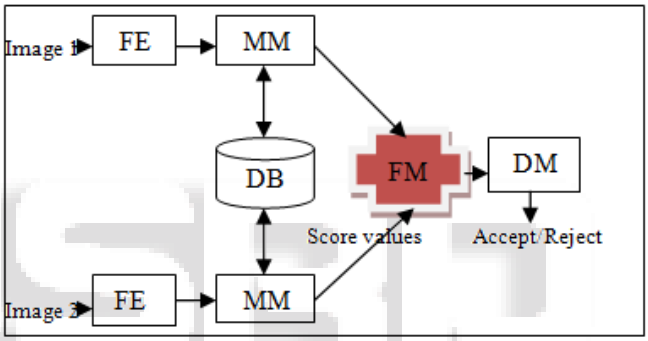

Fig. 5: Match Score Level Fusion

Figure 5 indicate match score level fusion and send this score to decision module. Where FM: Fusion Module, FE: Feature Extraction module, MM: Matching Module, DM: Decision Module, DB: Database.

4) Decision level Fusion:

At decision module, different match score are met from different modalities and then decision would be taken based on that match score. Although at this level fusion is easy but less powerful due to less availability of adequate information [4].

B. Performance Metrics for Multimodal Biometric System:

In password based authentication the perfect match between two alphanumeric strings is necessary to identify or verify persons. In biometric authentication system there should be a perfect match of feature set between a claimed identity and a stored identity. The following terms are uses as performance metrics for multimodal biometric systems:

1) False Match Rate (FMR):

It is the probability of a system that incorrectly matches the given input pattern to a non-match stored template in the database. It measures the percentage of invalid inputs which are incorrectly accepted by the system [5].

2) False Non-Match Rate (FNMR):

It is the probability that the system fails to detect a perfect match between the given input pattern and a matched template store in the database. It calculates the percentage of valid inputs which are incorrectly rejected by the system.

3) Receiver Operating Characteristic or Relative Operating Characteristic (ROC):
The ROC plot is a curve between the FAR and the FRR. The decision of rejection or acceptance of an individual is taken by comparing the score of the system to a threshold value (called the decision threshold). The values of FRR and FAR are dependent on that threshold value which is to be chosen so as to reduce the global errors of the system [6].
4) Equal Error Rate or Crossover Error Rate (EER or CER):
The curve at which both FAR and FRR errors are equal.
5) Failure To Enrol Rate (FTE):
The rate at which attempts to create a template from given input is unsuccessful to enrol. This is most commonly caused by low quality inputs.
6) Failure To Capture rate (FTC):
It is the probability of the systems fails to detect a biometric input even when presented correctly.

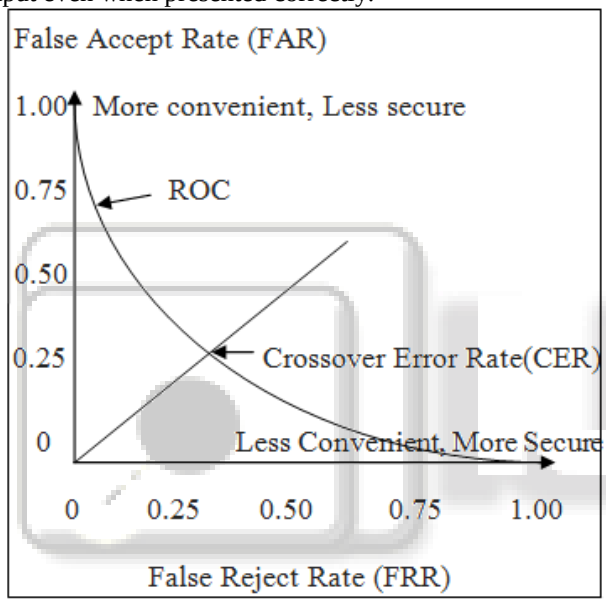

Fig. 6: Relationship between FAR, FRR and CER

Figure 6 represent ROC curve and a relationship between FAR (False Accept Rate), FRR (False Reject Rate) and Crossover Error Rate (CER).

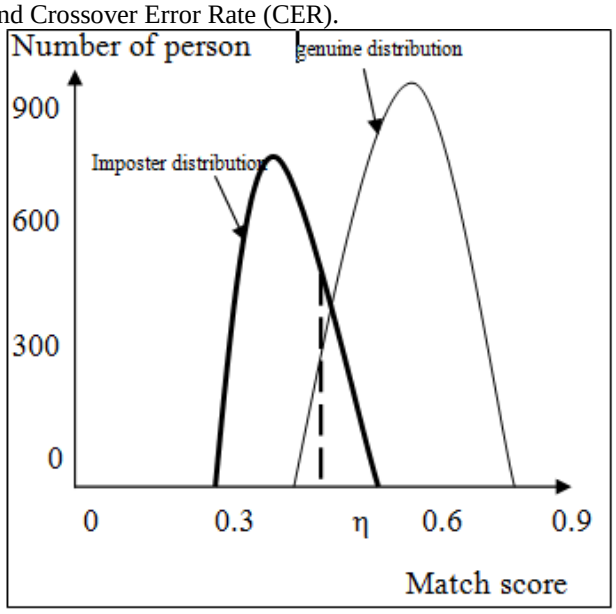

Fig. 7: Genuine – Imposter Distribution Curve

As shown above figure 7 an impostor score that will exceed the threshold η results in a false accept (or, a false match), while a genuine score that will fall below the threshold η results in a false reject (or, a false non-match). The Genuine Accept Rate (GAR) is the fraction of genuine scores exceeding the threshold η value. Therefore,

GAR = 1 – FRR (Fast Reject Rate)

When there are a large number of genuine and impostor scores is available, one could estimate the probability density functions of the two sets of scores in order to analytically derive the FAR (False Accept Rate) and FRR (False Reject Rate) [7,8]. Let p(s|genuine) and p(s|impostor) both represent the probability density functions of the score s under the genuine and impostor conditions, respectively. Then for a particular threshold, η,

$$FAR(\eta) = \int_{\eta}^{\infty} p(s|impostor)ds,$$

$$FRR(\eta) = \int_{-\infty}^{\eta} p(s|genuine)ds.$$

If the match score represents dissimilarity value, then FAR (η) and FRR (η) may be expressed as follows:

$$FAR(\eta) = \int_{-\infty}^{\eta} p(s|impostor)ds,$$

$$FRR(\eta) = \int_{\eta}^{\infty} p(s|genuine)ds.$$

In the case of identification process, the input Feature set is compared against all templates stored in the database in order to determine the best match (i.e. the top match) [3].

C. Existing Technologies of Multimodal Biometrics:

Multimodal biometrics uses more than one biometric trait for authentication purpose.
Already some existing multimodal technologies described below table:

Sno.	Multimodal traits	Database	Technique Adopted
1	Face + Finger veins [9]	CAIRO	Client specific linear Discriminate analysis(CSLDA)
2	Face + Speech [10]	UYVY. AVI 640 x 480, 15.00 fps	Gaussian mixture modal (GMM)
3	Lip Movement + Gestures [11]	Faces are Recorded using web camera	Artificial Neural Network (ANN)
4	Face + Ear [12]	MIT, Yale	Principal Component Analysis(PCA)
5	Face + Ear [13]	UWA, UNDFRGC, UND-F and FRGC V2	L3DF, Iterative closet point
6	Face + Ear [14]	MD I: Yale B and USTB. MD II : AR	Sparse representation Based classification

		and USTB	(SRC), Robust Sparse Coding (RSC)
7	Face + Ear [15]	USTB Database	KPCA, Kernel Fisher Discriminate Analysis(KFDA)
8	2D Face + 3D Ear [16]	West Virginia University Database	Weighted sum Technique
9	Face + Eye [17]	FERET, AR database	multi-level ellipse detector combined with a SVM verifier
10	Face + Palmprint [13]	AR, PolyU Database	FPCODE

Table 1: Existing Multi-Modal Technologies.

III. CONCLUSION

Multimodal biometric systems address some of the problems present in unimodal systems. By combining more than one sources of information, these systems increase population coverage, determination of spoofing, improve matching performance and facilitate indexing. Different type of fusion levels possible in multimodal biometric systems. Fusion at the match score level is the better than others and most popular due to the easy to access and confidence on matching scores. Performance metrics are use to measure the performance or multimodal system in terms of FAR, FRR and ROC curve. Multimodal biometric is spreading for the authentication purpose to maintain the interests of people regarding the security as strong as possible.

REFERENCES

[1] Anil K. Jain, Arun A. Ross, "An Introduction to Biometric Recognition", IEEE transaction on circuits and systems for video technology, vol.14, no.1, January 2004.
[2] Anil K. Jain Michigan State University, Arun A. Ross West Virginia University, "Multimodal biometrics: An Overview" Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224, September 2004.
[3] Anil K. Jain, Arun A. Ross, "Human Recognition Using Biometrics: An Overview" Appeared in Annals of Telecommunications, Vol. 62, No. 1/2, pp. 11-35, Jan/Feb 2007.
[4] Gandhimathi Amirthalingam, Radhamani, Research Scholar, "A Multimodal Approach for Face and Ear Biometric System", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 5, No 2, September 2013.
[5] Prof. Vijay M. Mane Department of Electronics Engineering, Vishwakarma Institute of Technology, Pune (India), "Review of Multimodal Biometrics: Applications, challenges and Research Areas".
[6] Muhammad Imran Razzak1, Rubiyah Yusof and Marzuki Khalid,"Multimodal face and finger veins biometric authentication", Scientific Research and Essays, Vol.5(17), pp. 2529-2534, 2010.
[7] Mohamed Soltane, Noureddine Doghmane, Noureddine Guersi, "Face and Speech Based Multi-Modal Biometric Authentication", International Journal of Advanced Science and Technology, Vol. 21(8), pp. 41-46, 2010.
[8] A.A. Darwish, R. Abd Elghafar and A. Fawzi Ali, "Multimodal Face and Ear Images", Journal of Computer Science, Vol. 5 (5), pp. 374-379, 2009.
[9] S.M.S. Islam, R. Davies, M. Bennamoun, R.A. Owens and A.S. Mian, "Multibiometric human recognition using 3D ear and face features", Pattern Recognition, Vol. 46, No. 3,pp. 613-627, 2013.
[10] Zengxi Huang, Yiguang Liu, Chunguang Li, Menglong Yang and Liping Chen, "A robust face and ear based multimodal biometric system using sparse representation", Pattern Recognition, Vol. 46, No. 8, pp.2156–2168, 2013.
[11] Xu Xiaona, Pan Xiuqin, Zhao Yue, Pu Qiumei, "Research on Kernel-Based Feature Fusion Algorithm in Multimodal Recognition", IEEE CS International Conference on Information Technology and Computer Science, pp.3-6, 2009.
[12] Mohammad H. Mahoor , Steven Cadavid, and Mohamed Abdel-Mottaleb, "Multi-modal Ear and Face Modeling and Recognition", Proc. IEEE 16th International Conference on Image Processing, pp. 4137-4140, 2009.
[13] M. Kawulok, J. Szymanek, "Precise multi-level face detector for advanced analysis of facial images", IET Image Process.,Vol. 6, Iss. 2, pp. 95–103l, 2012.
[14] Sahoo, SoyujKumar; Mahadeva Prasanna, SR, Choubisa, Tarun; Mahadeva Prasanna. "Multimodal Biometric Person Authentication: A Review". IETE technical Review 29(1): 54. doi:10.4103/0256-4602.93139 (inactive 2015-01-04). Retrieved 23 February 2012.
[15] B. Dorizzi, "Biometrics at the frontiers, assessing the impact on Society Technical impact of Biometrics", Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission, January 2005.
[16] Mohamed Soltane and Mimen Bakhti, "Multi-Modal Biometric Authentications: Concept Issues and Applications Strategies", International Journal of Advanced Science and Technology Vol. 48, November, 2012.
[17] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy Magazine, vol. 1, no. 2, pp. 33-42, April 2003.

