IJCSBI.ORG

A Hybrid Model of Multimodal Approach for Multiple Biometrics Recognition

P. Prabhusundhar
Assistant Professor, Department of Information Technology,
Gobi Arts & Science College (Autonomous),
Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India.

V.K. Narendira Kumar
Assistant Professor, Department of Information Technology,
Gobi Arts & Science College (Autonomous),
Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India.

B. Srinivasan
Associate Professor, PG & Research Department of Computer Science,
Gobi Arts & Science College (Autonomous),
Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India.

ABSTRACT
A single biometric identifier in making a personal identification is often not able to meet the desired performance requirements. Biometric identification based on multiple biometrics represents an emerging trend. Automated biometric systems for human identification measure a "signature" of the human body, compare the resulting characteristic to a database, and render an application dependent decision. These biometric systems for personal authentication and identification are based upon physiological or behavioral features which are typically distinctive, although time varying, such as Face recognition, Iris recognition, Fingerprint verification, Palm print verification in making a personal identification. Multi-biometric systems, which consolidate information from multiple biometric sources, are gaining popularity because they are able to overcome limitations such as non-universality, noisy sensor data, large intra-user variations and susceptibility to spoof attacks that are commonly encountered in uni-biometric systems. In this paper, it addresses the concept issues and the applications strategies of multi-biometric systems.

Keywords

Biometrics, Fingerprint, Iris, Palm print, Face recognition and Sensors.

1. INTRODUCTION

A Biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Statistically analyzing these biological characteristics has become known as the science of *biometrics*. These days, biometric technologies are

typically used to analyze human characteristics for security purposes. Five of the most common physical biometric patterns analyzed for security purposes are the fingerprint, hand, eye, face, and voice. Biometric fusion is the process of combining information from multiple biometric readings, either before, during or after a decision has been made regarding identification or authentication from a single biometric. The data information from those multiple modals can be combined in several levels: sensor, feature, score and decision level fusions.

Security is not enforced by focusing on a single parameter. Instead of solving a one-dimensional problem, a secure environment requires multiple dimensions of critical check points. Secure authentication is provided by multiple parameters. One parameter is a security token an individual uniquely possesses, such as a physical key or a smart card. Another parameter is an item an individual uniquely knows, such as a PIN. An additional parameter is an individual's unique biological characteristic, such as DNA or an iris code [8]. Some of the challenges commonly encountered by biometric systems are listed here:

a) Noise in sensed data: The biometric data being presented to the system may be contaminated by noise due to imperfect acquisition conditions or subtle variations in the biometric itself.
b) Non-universality: The biometric system may not be able to acquire meaningful biometric data from a subset of individuals resulting in a failure-to-enroll (FTE) error.
c) Upper bound on identification accuracy: The matching performance of a unibiometric system cannot be indefinitely improved by tuning the feature extraction and matching modules. There is an implicit upper bound on the number of distinguishable patterns (i.e., the number of distinct biometric feature sets) that can be represented using a template.
d) Spoof attacks: Behavioral traits such as voice and signature are vulnerable to spoof attacks by an impostor attempting to mimic the traits corresponding to legitimately enrolled subjects.

Some of the limitations of a unibiometric system can be addressed by designing a system that consolidates multiple sources of biometric information. This can be accomplished by having multiple traits of an individual or multiple feature extraction and matching algorithms operating on the same biometric. Such systems, known as multibiometric systems, can improve the matching accuracy of a biometric system while increasing population coverage and deterring spoof attacks. This paper presents an overview of multibiometric systems.

2. MULTIPLE BIOMETRICS

Multiple Biometrics refers to the use of a combination of two or more biometric modalities in a verification / identification system. Identification based on multiple biometrics represents an emerging trend. The most compelling reason to combine different modalities is to improve the recognition rate. This can be done when biometric features of different biometrics are statistically independent. There are other reasons to combine two or more biometrics. One is that different biometric modalities might be more appropriate for the different applications. Another reason is simply customer preference [5].

A variety of factors should be considered when designing a multiple biometric system. These include the choice and number of biometric traits; the level in the biometric system at which information provided by multiple traits should be integrated; the methodology adopted to integrate the information; and the cost versus matching performance trade-off [8]. Multiple Biometric systems capture two or more biometric data. Fusion techniques are applied to combine and analyze the data in order to produce a better recognition rate. Such technologies can not only overcome the restriction and shortcomings from single modal systems, but also probably produce lower error rate in recognizing persons [7].

To integrate fully biometric identification systems will be a lengthy process, but the technology has the potential to change the way the world works, no more passwords and smart cards, just using your body as your key. However, biometrics has been usefully applied for matters of lower importance, time monitoring systems and industry authentication systems. As the progress of technology increases, it is assured that biometrics can be effectively applied to important systems. There is no doubt that biometrics is the next stage of ubiquitous security technology in our increasingly paranoid, authoritarian society. However, there is still much to be done: customers are scared off by high failure-to-enroll and false non-match rates as well as incompatibilities. Furthermore, system security as a whole needs more care to be taken of. Future improvements in acquisition technology and algorithms as well as the availability of industry standards will certainly assure a bright future for biometrics. Will this be the end of traditional password or token-based systems certainly not biometrics is not the perfect solution either; it is just a good trade-off between security and ease of use.

2.1 Face Recognition

Face recognition analyzes facial characteristics. It requires a digital camera to capture one or more facial images of the subject for recognition.

With a facial recognition system, one can measure unique features of ears, nose, eyes, and mouth from different individuals, and then match the features with those stored in the template of systems to recognize subjects under test. Popular face recognition applications include surveillance at airports, major athletic events, and casinos. The technology involved has become relatively mature now, but it has shortcomings, especially when one attempts to identify individuals in different environmental settings involving light, pose, and background variations. Also, some user-based influences must be taken into consideration, for example, mustache, hair, skin tone, facial expression, cosmetics, and surgery and glasses. Still there is a possibility that a fraudulent user could simply replace a photo of the authorized person's to obtain access permission. Some major vendors include Viisage Technology, Inc. and AcSys Biometrics Corporation.

2.2 Fingerprint Recognition

The patterns of fingerprints can be found on a fingertip. Whorls, arches, loops, patterns of ridges, furrows and minutiae are the measurable minutiae features, which can be extracted from fingerprints. The matching process involves comparing the 2-D features with those in the template. There are a variety of approaches of fingerprint recognition, some of which can detect if a live finger is presented, and some cannot. A main advantage of fingerprint recognition is that it can keep a very low error rate. However, some people do not have distinctive fingerprints for verification and 15% of people cannot use their fingerprints due to wetness or dryness of fingers. Also, an oily latent image left on scanner from previous user may cause problems. Furthermore, there are also legal issues associated with fingerprints and many people may be unwilling to have their thumbprints documented. The most popular applications of fingerprint recognition are network security, physical access entry, criminal investigation, etc. So far, there are many vendors that make fingerprint scanners; one of the leaders in this area is Identix, Inc.

2.3 Palm Print Recognition

Palm print recognition measures and analyzes Palm print images to determine the identity of a subject under test. Specific measurements include location of joints, shape and size of palm. Palm print recognition is relatively simple; therefore, such systems are inexpensive and easy to use. And there are not negative effects on its accuracy with individual anomalies, such as dry skin. In addition, it can be integrated with other biometric systems. Another advantage of the technology is that it can

accommodate a wide range of applications, including time and attendance recording, where it has been proved extremely popular. Since Palm print geometry is not very distinctive, it cannot be used to identify a subject from a very large population. Further, Palm print geometry information is changeable during the growth period of children. A major vendor for this technology is Recognition Systems, Inc [6].

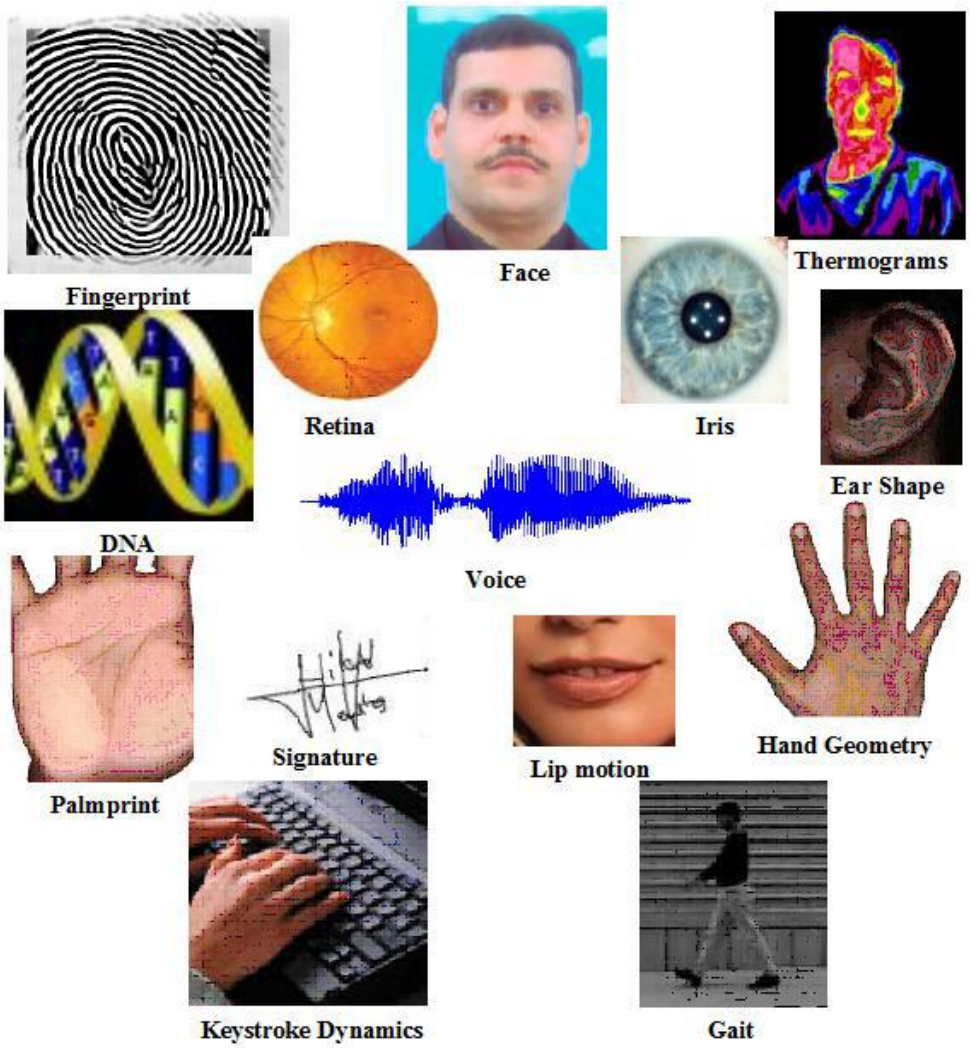

Figure 1. Examples of some of the biometric traits used for authenticating an individual

2.4 Iris Recognition

Iris biometrics involves analyzing features found in the colored ring of tissue that surrounds the pupil. Complex iris patterns can contain many distinctive features such as ridges, crypts, rings, and freckles. Undoubtedly, iris scanning is less intrusive than other eye-related biometrics. A conventional camera element is employed to obtain iris information. It requires no close contact between user and camera. In addition, irises of identical twins are not same, even thought people can seldom identify them. Meanwhile, iris biometrics works well when people wear glasses. The most recent iris systems have become more users friendly and cost effective. However, it requests a careful balance of light, focus, resolution and contrast in order to extract features from images. Some popular applications for iris biometrics can be employee verification, and immigration process at airports or seaports. A major vendor for iris recognition technology is Iridian Technologies, Inc.

3. CHALLENGES TO MULTI-BIOMETRIC SYSTEM

Based on applications and facts presented in the previous sections, followings are the challenges in designing the multi modal systems. Successful pursuit of these biometric challenges will generate significant advances to improve safety and security in future missions.

- The sensors used for acquiring the data should show consistency in performance under variety of operational environment. The sensor should be fast in collecting quality images from a distance and should have low cost with no failures to enroll.
- The information obtained from different biometric sources can be combined at five different levels such as sensor level, feature level, score level, rank level and decision level. Therefore selecting the best level of fusion will have the direct impact on performance and cost involved in developing a system.
- There are Numbers of techniques available for fusion in multi-biometric system; the multiple source of information is available. Hence it is challenging to find the optimal solution for the application provided.
- In multi-biometric systems the information acquired from different sources can be processed either in sequence or parallel. Hence it is challenging to decide about the processing architecture to be employed in designing the multi-biometric system.

4. IMPLEMENTATION

In general, the use of the terms multimodal or multi-biometric indicates the presence and use of more than one biometric aspect (modality, sensor, instance and/or algorithm) in some form of combined use for making a specific biometric verification/identification decision. The goal of multi-biometrics is to reduce one or more of the following:

- False accept rate (FAR)
- False reject rate (FRR)
- Failure to enroll rate (FTE)
- Susceptibility to artifacts or mimics

Multi modal biometric systems take input from single or multiple sensors measuring two or more different modalities of biometric characteristics. For example a system with fingerprint and face recognition would be considered "multimodal" even if the "OR" rule was being applied, allowing users to be verified using either of the modalities.

- **Multi algorithmic biometric systems**
  Multi algorithmic biometric systems take a single sample from a single sensor and process that sample with two or more different algorithms.
- **Multi-instance biometric systems**
  Multi-instance biometric systems use one sensor or possibly more sensors to capture samples of two or more different instances of the same biometric characteristics. Example is capturing images from multiple fingers**.**
- **Multi-sensorial biometric systems**
  Multi-sensorial biometric systems sample the same instance of a biometric trait with two or more distinctly different sensors. Processing of the multiple samples can be done with one algorithm or combination of algorithms. Example face recognition application could use both a visible light camera and an infrared camera coupled with specific frequency.

4.1 Fusion in Multimodal biometric systems

A Mechanism that can combine the classification results from each biometric channel is called as biometric fusion. We need to design this fusion. Multimodal biometric fusion combines measurements from different biometric traits to enhance the strengths. Fusion at matching score, rank and decision level has been extensively studied in the literature. Various levels of fusion are: Sensor level, feature level, matching score level and decision level [6].

4.1.1 Sensor level Fusion

In sensor Fusion we combine the biometric traits coming from sensors like Thumbprint scanner, Video Camera, Iris Scanner etc, to form a composite biometric trait and process.

4.1.2 Feature Level Fusion

In feature level fusion signal coming from different biometric channels are first preprocessed, and feature vectors are extracted separately, using specific fusion algorithm we combine these feature vectors to form a composite feature vector. This composite feature vector is then used for classification process.

4.1.3 Matching Score Level

Here, rather than combining the feature vector, we process them separately and individual matching score is found, then depending on the accuracy of each biometric channel we can fuse the matching level to find composite matching score which will be used for classification.

4.1.4 Decision level Fusion

Each modality is first pre-classified independently. The final classification is based on the fusion of the outputs of the different modalities. Multimodal biometric system can implement any of these fusion strategies or combination of them to improve the performance of the system.

5. EXPERIMENTAL RESULTS

Performance statistics are computed from the real and fraud scores. Real scores are those that result from comparing elements in the target and query sets of the same subject. Fraud scores are those resulting from comparisons of different subjects. Use each fusion score as a threshold and compute the false-accept rate (FAR) and false-reject rate (FRR) by selecting those fraud scores and genuine scores, respectively, on the wrong side of this threshold and divide by the total number of scores used in the test. A mapping table of the threshold values and the corresponding error rates (FAR and FRR) are stored. The complement of the FRR (1 – FRR) is the genuine accept-rate (GAR). The GAR and the FAR are plotted against each other to yield a ROC curve, a common system performance measure. We choose a desired operational point on the ROC curve and use the FAR of that point to determine the corresponding threshold from the mapping table.

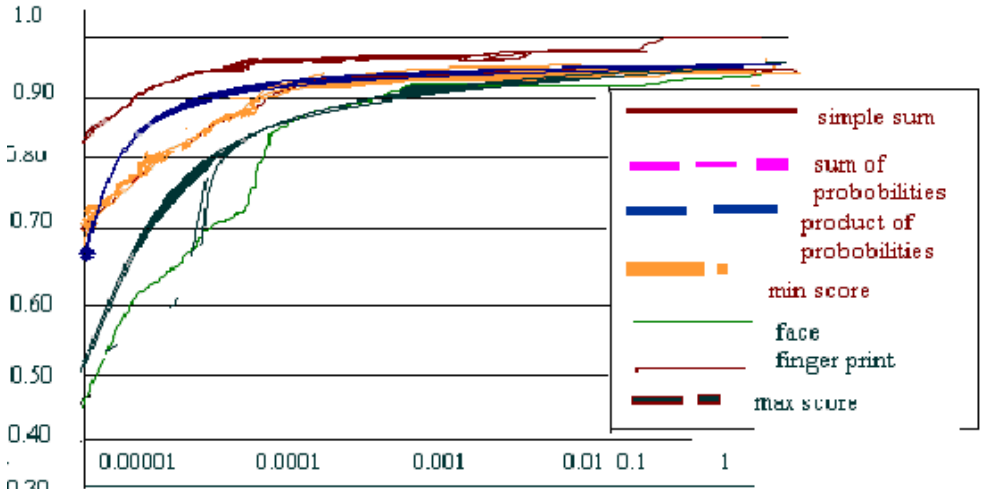

Figure 2. Min-Max Normalization with different fusions

For example, at a FAR of 0.1% the simple sum fusion with the min-max normalization has a GAR of 94.9%, which is considerably better than that of face, 75.3%, and fingerprint, 83.0%. Also, using any of the normalization techniques in lieu of not normalizing the data proves beneficial. The simplest normalization technique, the min-max, yields the best performance in this example. Figure 2 illustrates the results of Min-Max normalization for a spectrum of fusion methods. The simple sum fusion method yields the best performance over the range of FARs. Interestingly, the Genuine-Accept Rate for sum and product probability rules falls off dramatically at a lower FAR. GAR for the spectrum of normalization and fusion techniques at FARs of 1% and 0.1% respectively. At 1% FAR, the sum of probabilities fusion works the best. However, these results do not hold true at a FAR of 0.1%. The simple sum rule generally performs well over the range of normalization techniques. These results demonstrate the utility of using multimodal biometric systems for achieving better matching performance. They also indicate that the method chosen for fusion has a significant impact on the resulting performance. In operational biometric systems, application requirements drive the selection of tolerable error rates and in both single modal and multimodal biometric systems, implementers are forced to make a trade-off between usability and security. In operational biometric systems, application requirements drive the selection of tolerable error rates and in both single-modal and multimodal biometric systems, implementers are forced to make a trade-off between usability and security. Clearly the use of these fusion and normalization techniques enhances the performance significantly over the single-modal face or fingerprint classifiers.

6. PERFORMANCE OF MULTIMODAL BIOMETRICS

Multimodal Biometric systems are often evaluated solely on the basis of recognition system performance. But it is important to note that other factors are involved in the deployment of a bio-metric system. One factor is the quality and ruggedness of the sensors used. Clearly the quality of the sensors used will affect the performances of the associated recognition algorithms. What should be evaluated is therefore the sensor/algorithm combination, but this is difficult because often the same sensors are not used in both the enrolment and test phases. In practice therefore the evaluation is made on the basis of the recognition algorithm's resistance to the use of various types of sensor (interoperability problem). Another key factor in determining the acceptability of a biometric solution is the quality of the associated communication inter-face. In addition to ease of use, acquisition speed and processing speed are key factors, which are in many cases not evaluated in practice.

In the case of a verification system, two error rates are evaluated which vary in opposite directions: the false rejection rate FRR (rejection of a legitimate user called “the client”) and the false acceptance rate FAR (acceptance of an impostor). The decision of acceptance or rejection of a person is thus taken by comparing the answer of the system to a threshold (called the decision threshold). The values of FAR and FRR are thus dependent on this threshold which can be chosen so as to reduce the global error of the system. The decision threshold must be adjusted according to the desired characteristics for the application considered. High security applications require a low FAR which has the effect of increasing the FRR, while Low security applications are less demanding in terms of FAR. EER denotes Equal Error Rate (FAR=FRR). This threshold must be calculated afresh for each application, to adapt it to the specific population concerned. This is done in general using a small database recorded for this purpose.

Different biometric application types make different trade-offs between the false match rate and false non-match rate (FMR and FNMR). Lack of understanding of the error rates is a primary source of confusion in assessing system accuracy in vendor and user communities alike. Performance capabilities have been traditionally shown in the form of ROC (receiver- or relative-operating characteristic) plots, in which the probability of a false-acceptance is plotted versus the probability of a false-rejection for varying decision thresholds. Unfortunately, with ROC plots, curves corresponding to well-performing systems tend to bunch together near the

lower left corner, impeding a clear visualization of competitive systems. More recently, a variant of an ROC plot, the detection error tradeoff (DET) plot has been used, which plots the same tradeoff using a normal deviate scale.

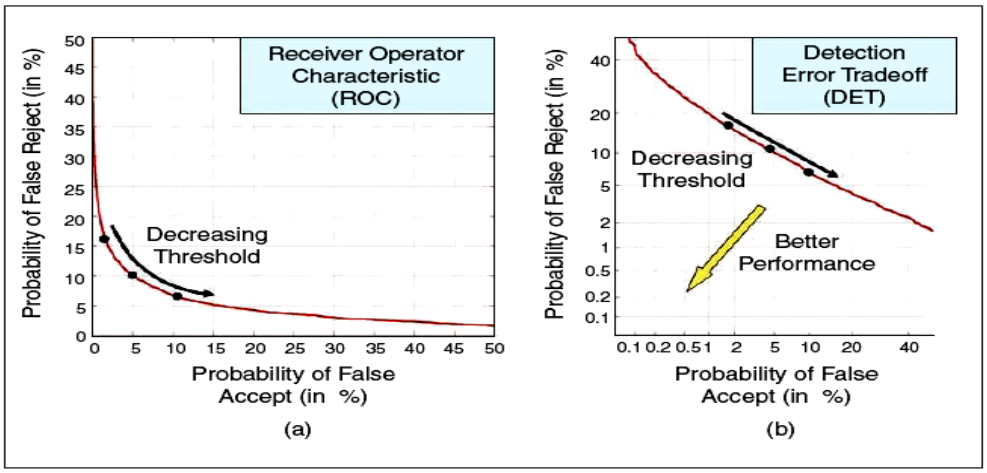

Figure 3. Example of Verification Performance Comparison for Same Hypothetical Systems, A and B, for both (a) ROC and (b) DET plots

Although the complete DET curve is needed to fully describe system error tradeoffs, it is desirable to report performance using a single number. Often the equal-error-rate (EER), the point on the DET curve where the FA rate and FR rate are equal, is used as this single summary number. However, the suitability of any system or techniques for an application must be determined by taking into account the various costs and impacts of the errors and other factors such as implementations and lifetime support costs and end-user acceptance issues. There is a tradeoff between the probability of correct detect and identify rate and the false alarm rate. If we increase the probability of correct detect and identify rate, the false alarm rate will increase. A Watch list Receiver Operating Characteristic curve is used to show the relationship between the probabilities of correct detects and identify rate and the false alarm rate. In practice, most applications that operate in the watch list task can be grouped into five operational areas:

a) **Extremely low false alarm:** In this application, any alarm requires immediate action. This could lead to public disturbance and confusion. An alarm and subsequent action may give away the fact that surveillance is being performed and how, and may minimize the possibility of catching a future suspect.
b) **Extremely high probability of detect and identify**: In this application, we are mostly concerned with detecting someone on the

watch list; false alarms are a secondary concern and will be dealt with according to pre-defined procedures.

c) **Low false alarm and detect/identify:** In this application we are more concerned with lower false alarms and can deal with low detect/identify.

d) **High false alarm and detect/identify:** In this application we are more concerned with higher detect/identify performance and can deal with a high false alarm rate as well.

e) **No threshold:** User wants all results with confidence measures on each for investigation case building.

7. CONCLUSION

A Multimodal Biometrics technique, which combines multiple biometrics in making a personal identification, can be used to overcome the limitations of individual biometrics. We developed a multimodal biometrics system which integrates decisions made by Face recognition, Iris recognition, Fingerprint verification, Palm print verification. Multi-biometric systems alleviate a few of the problems observed in uni-modal biometric systems. Besides improving matching performance, they also address the problems of non-universality and spoofing.With the widespread deployment of biometric systems in several civilian and government applications, it is only a matter of time before multimodal bio-metric systems begin to impact the way in which identity is established in the 21st century. Multiple Biometric technologies could make a huge positive impact into society, if it is correctly utilized to increase the robustness of security systems across the world. This would help to cope with the rising levels of fraud, crime and terrorism.

REFERENCES

[1] John Daugman, "*How iris recognition works*" IEEE Transactions on Circuits and Systems for Video Technology, 14(1):21–30, 2004. Page No. 103-109.

[2] Chang, "*New multi-biometric approaches for improved person identification*," PhD Dissertation, Department of Computer Science and Engineering, University of Notre Dame, 2004. Page No. 153-159.

[3] C.Hesher, A.Srivastava, G.Erlebacher, *"A novel technique for face recognition using range images"* in the Proceedings of Seventh International Symposium on Signal Processing and Its Application, 2003. Page No. 58-69.

[4] Barral and A. Tria, "*Fake fingers in fingerprint recognition: Glycerin supersedes gelatin*", In Formal to Practical Security. Springer, 2009. Page No. 83-92.

[5] Bergman, "*Multi-biometric match-on-card alliance formed*" Biometric Technology Today, vol. 13, no. 5, 2005. Page No. 1-9.

[6] F. YANG, M. Baofeng, "*Two Models Multimodal Biometric Fusion Based on Fingerprint, Palm-print and Hand-Geometry*",DOI-1-4244-1120-3/07, IEEE,2007.

[7] Teddy Ko, "*Multimodal Biometric Identification for Large User Population Using Fingerprint, Face and Iris Recognition*", Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop (AIPR05) ,2005.

[8] A.K.Jain, R.Bolle, *"Biometrics-personal identification in networked society"* Norwell, 1999, Page No. 23-36.

[9] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy and B.V.K. V. Kumar, "*Biometric Encryption, Enrollment and Verification Procedures*", Proc. SPIE 3386, 24-35, 1998.