Volume 2, Issue 9, September 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Biometrics for Enhancement of Security Standards

Pooja Shelke
Institute of Forensic Science, Nagpur, India

Ashish Badiye*
Institute of Forensic Science, Nagpur, India

Abstract— Biometrics has found an important place in our day to day life. With growing concerns over security of individuals as well the data, there has been a step rise in the number and types of biometric devices and security. For enhancing the security standards of the Biometric devices some important features included in the system namely uniqueness of the data, permanent identification, Indispensability, preciseness, exclusiveness, simplicity, affordability, convenience, acceptance. But these measures are not totally efficient and sufficient in the prevention of damage to the user as well as the safe keeping of the database. When thieves cannot get access to secure properties, there is a chance that the thieves will stalk and assault the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property.
Sharing of database amongst various security agencies within a country and amongst other countries should be increased. Many countries, including the United States, are planning to share biometric data with other nations. There is an urgent need for the enhancement of the security standards in biometrics. This paper aims to explore the numerous underlying possibilities and effective ways to use the existing biometric systems and to develop new standard systems in the process which will help serve the world to make it a better place to exist.

Keywords— irreversible biometrics, biometric concepts, biometrics at global level, multimodal biometrics

I. INTRODUCTION

The word BIOMETRIC is derived from the Greek letters 'bios' and 'metric'; which means; life and measurement respectively, directly translates into "Life Measurements". Biometric authentication system works on two basics that are **Identification and Verification.** A biometric identifier relies on unique biological information about a person.

The history of biometrics can be traced back as far as the fourteenth century when it was used by merchants in China where thumbprints and other anatomy measurements were used as a method for identifying and keeping track of customers. (Hall 2008) In more recent times Bertillionage emerged from Paris in the latter part of the 19th Century. Developed by a police clerk called Alphonse Bertillion, Bertillionage was a new method of identifying people by taking measurements of their body. (Kaluszynski 2001) Although these techniques of measuring various dimensions of the body as identifying data were not the advanced technology we have come to think of as biometrics, it is easy to see that today's biometric technologies have evolved from the principles of these early techniques.

When a biometric is used to verify a person that verification is frequently referred to as "one-to-one" matching .Almost all systems can determine whether there is a match between the person's presented biometric and biometric templates in a database in fewer than one second. Identification, by contrast, is known as "one-to-many" matching. In identification, a person's presented biometric is compared with all of the biometric templates within a database. There are two types of identification systems positive and negative. Positive systems expect there to be a match between the biometric presented and the template. These systems are designed to make sure that a person is in the database. Negative systems are set up to make sure that a person is not in the system. Negative identification can also take the form of a watch list, where a match triggers a notice to the authority for action. Biometrics further having some advantages and disadvantages as follows-

A. *Privacy of Data*

It may possible that data obtained during biometric enrollment may be used in ways for which the enrolled individual has not consented. For example, biometric security that utilizes an employee's DNA profile could also be used to screen for various genetic diseases or other 'undesirable' traits.

B. *Security of Owners and Secured items*

When thieves cannot get access to secure properties, there is a chance that the thieves will stalk and assault the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. For example, in 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car. Universality of the biometric data and devices is also increasing.

C. *Irreversible Biometrics*

One advantage of passwords over biometrics is that they can be re-issued. If a password is lost or stolen, it can be cancelled and replaced by a newer version. This is not naturally available in biometrics. If someone's face is compromised from a database, they cannot cancel or reissue it. Irreversible biometrics is a way in which to incorporate protection and the replacement features into

biometrics. Although increasing the restrictions on the protection system, it makes the irreversible templates more accessible for available biometric technologies.

D. *Biometrics at global level.*

Many countries, including the United States, are planning to share biometric data with other nations. In testimony before the US House Appropriations Committee, Subcommittee on Homeland Security on "biometric identification" in 2009, Kathleen Kraninger and Robert A Mocny commented on international cooperation and collaboration with respect to biometric data, as follows:

"To ensure we can shut down terrorist networks before they ever get to the United States, we must also take the lead in driving international biometric standards. By developing compatible systems, we will be able to securely share terrorist information internationally to bolster our defenses. Just as we are improving the way we collaborate within the U.S. Government to identify and weed out terrorists and other dangerous people, we have the same obligation to work with our partners abroad to prevent terrorists from making any move undetected. Biometrics provides a new way to bring terrorists' true identities to light, stripping them of their greatest advantage—remaining unknown." (Siegel 2007)

AFIS (Automated Fingerprint Identification System) Technology was the first major use of automated biometrics, and the system will be familiar to any regular viewer of science fiction or crime television and film, but it has only existed since the late sixties. It was developed and implemented by the Federal Bureaux of Investigation as an automated computer system that could substitute the previously laborious manual task of matching fingerprints against a database. (Zhang, Jing and Yang 2006) The Henry Classification System, which identifies key distinguishing markers within fingerprints, formed part of the basis for the development of the AFIS software.

II. THE CHALLENGES OF ONLINE SECURITY

Security mechanisms exist to provide security services such as authentication, access control, data integrity, confidentiality and non repudiation and may include the mechanisms such as biometric authentication and/or security audit trails (Stallings, 2006).

On-line security is of particular importance especially for activities such as on-line banking or e-payments. Cyber attacks continue to increase and can take many forms. An example of this was the Banker Trojan which was created to copy passwords, credit card information and account numbers associated with on-line banking services from the user's PC.

In order for security mechanisms to work every link in the chain must work. This includes personal and/or resource passwords. People's habits or the security culture within organizations, such as sharing passwords or writing them down, or not logging off when they step away from the computer can break down most security systems. Often these habits are hard to monitor and prevent (Herath & Rao, 2009; Kraemera et al., 2009) yet in spite of this, text passwords remain popular as they are relatively easy to implement and still accepted by users. For the actual username–password method to be effective, it is essential that users generate and use (and remember) strong passwords that are resistant to guessing and cracking (Vu et al., 2007).

Biometric authentication cannot solve every problem with on-line security but it can be used to overcome some of these issues associated with passwords and system access. Biometric security can also provide a measure of continuous authentication when performing the actual transaction. The use of biometric security does not leave the user with something to remember or to write down. Dhamija and Dusseault (2008) suggest that users are more likely to accept a security system if it is simple to use.

Biometric applications may be categorized into three main groups:

1. Forensic applications, in criminal investigations, e.g., for corpse identification, parenthood determination, etc.
2. Government applications, including personal documents, such as passports, ID cards and driver's licenses; border and immigration control; social security and welfare-disbursement; voter registration and control during elections; e-Government.
3. Commercial applications, including physical access control; network logins; e-Commerce; ATMs; credit cards; device access to computers, mobile phones; PDAs; facial recognition software; e-Health.

This order generally reflects the emergence and use over time of biometric recognition systems. Initially found mainly in the field of criminology and forensics, biometrics underwent a market breakthrough when governments started to integrate biometric access control mechanisms in personal documents. While access control and authentication have remained the primary purpose, other fields of application are taking off.

Google's photo organizer software Picasa and social-networking site Facebook have integrated face recognition algorithms to make it easier to search and display all photos featuring a certain person. Picasa is available as an application for several operating systems, while its photo sharing web site (Picasa Web Albums) and Facebook provide face recognition online. Biometric systems embedded in cars of a vehicle fleet can help to identify the driver, adjust seat, rear mirrors, and steering wheel to meet individual preferences.

Commercial and government applications are likely to overlap in some fields. Future e-commerce, e-health and e-government services may require authentication with the help of biometric personal documents issued by governments, as soon as they are used by a large enough part of the population. Some developing countries have used biometrics for voter registration in the run-up to elections in order to avoid out-dated voter lists and election fraud.

Market forecasts on biometric spending are generally optimistic. Growth is expected especially in commercial and government applications, where the biometrics industry and the related smart card chip industry benefit from government decisions toward the adoption of electronic

III. BIOMETRICS AND INDIVIDUAL AUTHENTICATION

A. *Biometric Concepts*

Biometrics is described as the science of recognizing an individual based on his or her physical or behavioural traits (Jain et al., 2006). Since a biometric is either a physical or behavioural characteristic of the user it is almost impossible to copy or steal. The use of biometrics as a security measure offers many benefits such as increasing individual user accountability or decreasing number of Personal Identification Numbers (PINs) and passwords per user. This in turn allows stronger security measures for remaining PINs and passwords.

Biometric security has existed since the beginning of man – recognising someone by face or voice. Fingerprint biometrics dates back to ancient China. A formal approach for commercial use dates back to the 1960s and 1970s as is the case with fingerprint scanning, which has been around since the late 1960s (Dunstone, 2001).

Biometrics authentication refers to both verification and/or identification. In verification the subject claims to be a specific person and a one-to-one comparison is done. Whereas, with identification the applicant's data is matched against all the information stored or the entire database to determine his/her identity. This is a one-to-many task.

There are many applications of biometrics for both security and confidentiality. These include law enforcement and forensics, access control, and preventing/detecting fraud in organisations, educational institutions and electronic resources. Biometric Encryption also exists. This is the process of using a characteristic of the body as a method to code/encrypt/decrypt data. This can be used in asymmetric encryption to generate the private key.

Jain et al. (2004) outlined some characteristics of efficient biometric systems:

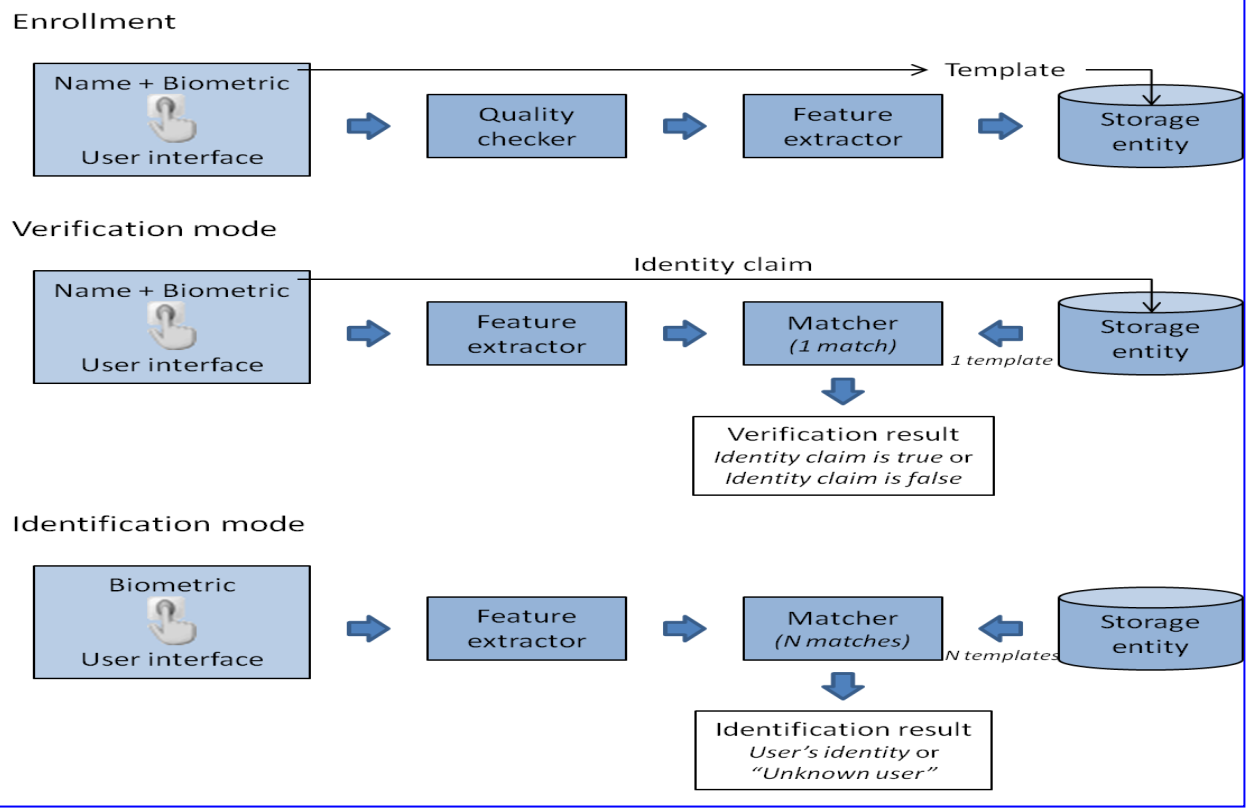
a. Universality — every person should have the characteristics.
b. Distinctiveness — no two persons should have the exact biometric characteristics.
c. Permanence — characteristics should be invariant with time.
d. Collectability —characteristics must be measurable quantitatively.
e. Performance — the biometric system accuracy, speed, consistency and robustness should be acceptable
f. Acceptability — users must be willing to accept and use the system.
g. Circumvention —fooling the system should be difficult.

B. *Biometric Techniques*

There are two types of biometric techniques – physiological and behavioral. Physiological techniques are based physical characteristics. Examples include fingerprint recognition, iris recognition, face recognition, hand geometry (finger lengths, finger widths, palm width, etc.), blood vessel pattern in the hand, DNA, palm print (apart from hand geometry), body odour, ear shape and fingernail bed (apart from fingerprints).

Behavioral techniques are based on the things you do (a trained act or skill that the person unconsciously does as a behavioral pattern). Examples include voice recognition, keystroke recognition (distinctive rhythms in the timing between keystrokes for certain pairs of characters), signature recognition (handwriting or character shapes, timing and pressure of the signature process). Gait

Figure 1: Block diagrams of Enrollment, Verification and Identification



recognition or the pattern of walking or locomotion is also used as a biometric measure (Ortega-Garcia et al., 2004).

C. *The Biometric Process*

The Biometric Process has two stages – enrolment and authentication. Each user must first be enrolled in the system. Here the aim is to capture data from the biometric device which can identify the uniqueness of each subject as it is essential to establish a 'true' identity. The key features for each user are then extracted from this data and stored in a database. These features could be common for all users or customized, either by weights assigned to show the importance of the feature or by selecting different features, for each user. Usually before feature extraction/selection there is some form of pre-processing in which the data is made more manageable for extraction. Some form of normalization or smoothing may be done at this stage. After the template is created for each user (during enrolment), a new sample is taken and compared to the template. This creates the genuine distance measure (Wayman, 2000). The average genuine distance for the whole sample population can be used as a common threshold or the threshold can be unique for each user.During the authentication (identification and/or verification) process new samples taken from the subject are compared to the

stored data and a match score is computed to determine the fit. The match score is compared to the threshold score and if it is greater that the threshold score this is not considered to be a fit. The general biometric process is shown in the figure below (Figure 1.). This is them summarized in the table which follows (Table 1).

Figure 1: Block Diagram of Enrollment, Verification & Identification

Stage of Process	Activity
Capture	A physical or behavioral sample is captured by the system during enrolment. (Data Collection); this is influenced by the technical characteristics of the sensor, the actual measure and the way the measure is presented.
Extraction	Unique data is extracted from the sample and a template is created. Distinctive and repeatable features are selected. Feature templates are stored in the database.
Comparison/ Classification	The new sample is then compared with the existing templates. Distance Measures (DM) are calculated and compared to threshold(s). DM Never zero because of variability due to human, sensor, presentation , environment
Decision-making	The system then decides if the features extracted from the new sample are a match or a non-match based on the threshold match score.

D. *Some Challenges with Biometric Authentication*

A biometric system cannot guarantee accuracy partly due to the variability in humans, the systems and the environment. Stress, general health, working and environmental conditions and time pressures all contribute to variable results (Roethenbaugh, 1997).

There are two main accuracy measures used: False Accept and False Reject. False Accept error occurs when an applicant, who should be rejected, is accepted. False Accept Rate (FAR) or Type II error rate is the percentage of applicants who should be rejected but are instead accepted. False Reject Rate (FRR) or Type I error rate is the percentage of legitimate users who are denied access or rejected. These two measures are also referred to as false match or false non-match rates respectively

IV. FACTORS AFFECTING THE ACCURACY OF BIOMETRIC MEASUREMENTS

The UK Government Test Protocol for Biometric Devices (Mansfield et al., 2001) is a standard protocol which could be used for commercially available biometric devices. It suggests some time lapse between the collections of trials for template creation (to cater for the aging or learning process). Two common system errors are Failure to enroll and Failure to Acquire. Failure to enroll occurs when the system is unable to generate repeatable templates for a given user. This may be because the person is unable to present the required feature. Failure to acquire occurs when the system is unable to capture and/or extract quality information from an observation. This may be due to device/software malfunction, environmental concerns and human anomalies.

The following diagrams sums up some of the possible errors within each stage of the process.

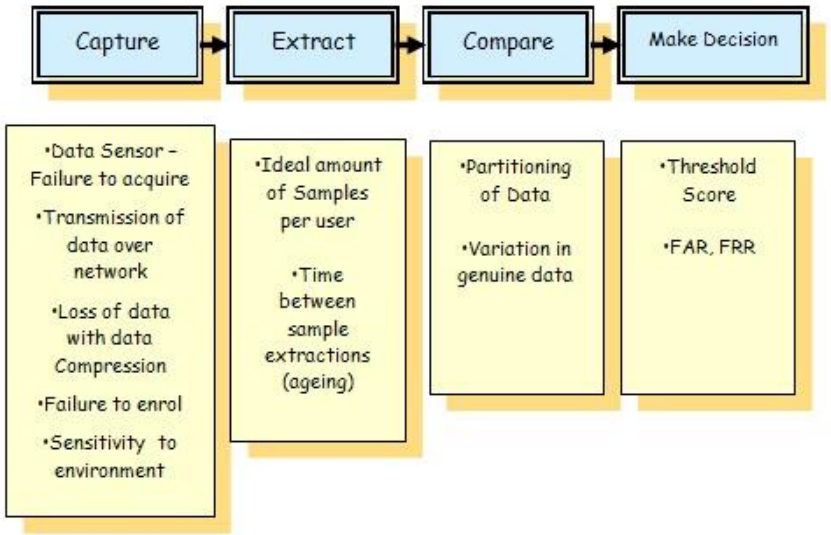


Figure 2. Some possible errors within the Biometric Process.

A. *Multimodal Biometrics*

A multimodal approach could be adopted to make a biometric system more secure. A layered or multimodal biometrics approach uses two or more independent systems or techniques to yield greater accuracy due to the statistical independence of the selected approaches. Therefore more than one identifier is used to compare the identity of the subject. This approach is also called multiple biometrics (Huang et al., 2008). Ortega-Garcia et al. (2004) refers to this as unimodal-fusion or monomodal-fusion.

B. *Dynamic Signature Verification: a form of Biometric Authentication*

Dynamic signature verification (DSV) can capture the shape of the image, as is done with static signature recognition, but also the space-time relationship created by the signature. Both static and dynamic signature verification are forms of biometric authentication.

To decrease processing time a simple comparison was done before the classification stage - this took the form of 'prehard' and 'presoft' classifiers. This was done by comparing the absolute value of writing time of the signature being tested minus the average writing time. With the presoft classifier if this value was below a certain level (.2) the data did not need to be normalised before extraction. For the prehard classifier if this value was too high the data was instantly rejected. They were able to achieve 0% FRR and 7%FAR.

Penagos et al (1996) also used customised feature selection – the weight assigned to each feature was adjusted for each feature of each user. The common features selected were the starting location, size, and total duration of the signature. As in Lee et al. (1996) the threshold was also customised for each user. The customised thresholds were adjusted, if needed, until either their signatures were accepted repeatedly, or the maximum threshold value was reached. The experiment was conducted with the use of a digitizing tablet to extract features such as shape of signature, pressure (measured with the stylus), speed and acceleration. Normalisation was done on the time, position and acceleration values. They were able to achieve an 8% FRR and 0%FAR.

Plamondon & Srihari (2000) presented a survey paper on on-line and off-line handwriting recognition and verification. It suggested that at the time of this article (2000), even if verification was being researched for about three decades, the level of accuracy was still not high enough for situations needing high level of accuracy such as banking. The survey listed several techniques used for user verification, they include neural networks, probabilistic classifiers, minimal distance classifiers, nearest neighbour, dynamic programming, time warping, and threshold based classifier. One point highlighted was that before recognition noise is removed by a smoothing algorithm, signal filtering.

Jain et al. (2002) used writer-dependent threshold scores for the classification stage. For their experiment, like the ones above, a digitising tablet was used. The features were separated into Global (properties of the whole signature e.g. total writing time) and Local (properties that refer to a position within the signature e.g. pressure at a point). Prior to the feature selection stage a Gaussian filter was used to smooth the signatures. Number of individual strokes and absolute speed normalized by the average signing speed were some of the features used. Dynamic Time Warping was used to compare strings. The experiment yielded a FRR of 2.8% and a FAR or 1.6%.

Some studies focus on the best selection of the features, for example Lei & Govindaraju, (2005). In this paper they compared the discriminative power of the biometric features. Here the position features were normalised by dividing by the maximum height or maximum width. The authors compared the mean or average consistency for each feature, the standard deviation over subjects, and EER of selected features. The authors highlighted the fact that a high standard deviation implies that this feature may not discriminate itself among users. Low mean consistency implies that this feature varies among one user. The results showed that some features such as the speed, the coordinate sequence, and the angle were consistent and reliable.

In most studies the features were first normalised to make them easier to select and compare. Dimauro et al. (2004) suggested that the data should be first filtered then normalised in time-duration and size domain. Faundez-Zanuy (2005) stated that length normalisation was used because different repetitions of signature from a given person could have different durations.

Feature such as 2D position and speed were common features selected. McCabe et al. (2008) used other features such as aspect ratio (This is the ratio of the writing length to the writing height). Number of "pen-ups" (This indicates the number of times the pen is lifted while signing after the first contact with the tablet and excluding the final pen-lift). Top Heaviness (This is a measure of the proportion of the signature that lies above the vertical midpoint i.e., the ratio of point density at the top half of the signature versus the density at the bottom half), and Area (This is the actual area of the handwritten word). They used a neural network for user verification. The FAR was as low as 1.1% with a 2.2% FRR.

Recently Eoff and Hammond (2009) obtained accuracy of 97.5% and 83.5% for two and ten users respectively. The study was used to identify different user strokes on a shared (collaborative) surface. Here the authors used pen tilt, pressure and speed to classify users. A Tablet PC was used to capture the strokes of users.

Unlike the other studies discussed, C Hook et al. (2003) did not use the digitizing tablet. They presented a study of a biometrical smart pen BiSP. In this study the pen itself was able to capture measures such as pressure and acceleration. This study took a multimodal approach - it also used fingerprint information as well as acoustic information for authentication. Results showed accuracy of up to 80% for user identification and 90% for user verification.

V. CONCLUSION

For enhancing the security standards of the Biometric devices some important features has to be included in the system namely uniqueness of the data, permanent identification, Indispensability, preciseness, exclusiveness, simplicity, affordability, convenience, acceptance. Biometric systems & databases pose a few unknown disadvantages. It is possible that data obtained during biometric enrollment may be used in ways for which the enrolled individual has not consented. Biometric security that utilizes an employee's DNA profile could also be used to screen for various genetic diseases or other 'undesirable' traits. When thieves cannot get access to secure properties, there is a chance that the thieves will assault the property owner to gain access. On the other hand, centralizing the database will help in many ways like many countries, including the United States, are planning to share biometric data with other nations. By developing compatible systems, we will be able to securely share terrorist information internationally to bolster our defense and to prevent terrorists from making any move undetected.

REFERENCES

[1] Ross A. K. Jain and Salil Prabhakar, "An Introduction to Biometric Recognition". *IEEE Transaction on Circuits and Systems for Video Technology*, 14, 2004, PP: 44–48.

[2] Debnath Bhattacharyya, 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, 2009 Sep.

[3] Dr.T.Kathikeyan and S.Prabhu, "Personal Identification and Verification based on biological trait", *Journal of Computer Science*, Vol.01, No.05, Mar-Apr 2006, PP: 399-403.

[4] Stelvio Cimato, Marco Gamassi, Vincenzo Piuri, Daniele Sana, Roberto Sassi, and Fabio Scotti, "Personal identification and verification using multimodal biometric data", CIHSPS 2006 - *IEEE International Conference on Computational Intelligence for Homeland Securityand Personal Safety.* Alexandria, VA, USA, Oct 2006, 16-17.

[5] Palaniappan, R: "A new method to identify individuals using VEP signals and neural network". *IEE Proceedings - Science, Measurement and Technology Journal*, Vol. 151, 2004, 16-20.

[6] R.Palaniappan and P.Raveendran, "Individual identification technique using visual potential signals", *Electronics Letters*, Vol.38, No.25, 2005.

[7] Nadia Feddaoui, Hela Mahersia and Kamel Hamrouni, "Improving Iris Recognition Performance Using Quality Measures", *Advanced Biometric technologies*, 2010, PP: 242-264.

[8] Ramasamy Palaniappan, Danilo P.Mandic, *"EEG Based Biometric Framework for Automatic Identity Verification", Journal of VLSI signal processing*, 49, 2007, PP: 243-250.

[9] Josef Kittler Giorgio Fumera Fabio Roli and Daniele Muntoni, "An experimental comparison of classifer fusion rules for multimodal personal identity verification system", *In SpringerBerlin/Heidelberg*, 2002.

[10] Dr.T.Karthikeyan "Efficient Bio Metric IRIS Recognition System Using Fuzzy Neural Network", *International Journal of Advanced Networking and Applications* Volume: 01,Issue: 06, 2010, PP: 371-376.

[11] Tieniu Tan Yuchun Fang and Yunhong Wang. Fusion of global and local features for face verification. *In 16th International Conference on Pattern recognition*, 2002.

[12] Raghavendra.R, Ashok Rao, Hemantha Kumar, Multisensor Biometric Evidence Fusion of Face and Palmprint for Person Authentication using Particle Swarm Optimization (PSO), *International Journal of Biometrics*, 2010, Vol.2, No.1,PP: 19–33.

