ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Volume 2, Special Issue 19, October 2016

BIOMETRICS IMAGE SIGNAL AND VIDEO PROCESSING

K.MohamedSayeed Khan
II M.Sc. Computer science
Sadakathullahappacollege
Tirunelveli

V.Uma Devi M.Sc.M.Phil.,
Assistant Professor
Sadakathullahappa college
Tirunelveli

Abstract

Biometrics is seen by many as a solution to a lot of the user identification and security problems in todayUs networks. Password abuse and misuse, intentional and inadvertent is a gaping hole in network security. This results mainly from human error, carelessness and in some cases maliciousness. Biometrics removes human error from the security equation.

Our project will examine all the technological and feasibility aspects as well as the practical applications. We will look at many different biometric methods of identifying the user.

1. INTRODUCTION

A biometric system is a recognition system, which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the

user. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons:

- The person to be identified is required to be physically present at the point of identification.
- Identification based on biometric techniques eliminates the need to remember a password or carry an identity.

Depending on the context on which a biometric system works, it can be
Either classified as an identification system or a verification (authentication) system identification involves in establishing a person's identify whereas in verification involves confirming or denying a person's claiming identity.

2. MULTIBIOMETRICS

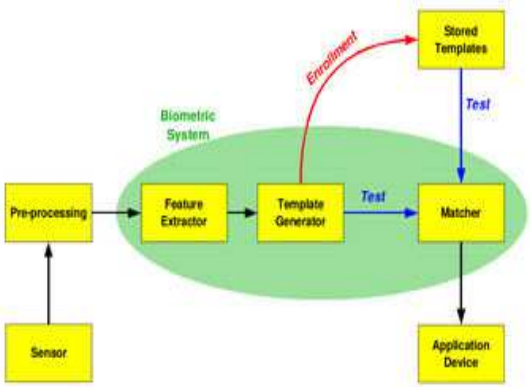
A multi-biometrics system is obtained by the integration of multiple individual biometrics models. A numbers of models integrating hand geometry, keystroke dynamics, face and iris

recognition system have flooded the markets in recent years.

Here we present a multimodal system that can be embedded in a mobile phone, which integrates fingerprint, voice and facial scanning. It shuts down the problem of high False Rejection Rate of facial scanners, eliminates the fooling of fingerprint scanners and overshadows the disadvantage of voice recognition models.

3.BIOMETRICS FUNCTIONALITY

The block diagram illustrates the two basic modes of a biometric system.First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be.



Three steps are involved in the verification of a person.In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison.Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using same identity".

Second, in identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be".The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

The first time an individual uses a biometric system is called *enrollment*. During the enrollment, biometric

information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a *template*. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the filesize and to protect the identity of the enrollee.

During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements.We should consider Performance, Acceptability, Circumvention, Robustness, Population coverage, Size, Identity theft deterrence in selecting a particular biometric. Selection of biometric based on user requirement considers Sensor availability, Device availability, Computational time and reliability, Cost, Sensor area and power consumption

4. APPLICATIONS

FORENSIC

The use of biometric in the law enforcement and forensic is more known and from long date, it is used mainly for identification of criminals. In particular, the AFIS (automatic fingerprint identification system) has been used for this purpose. Lately the facial-scan technology (mug shots) is being also used for identification of suspects. Another possible application is the verification of persons of home arrest, a voice-scan is an attractive solution for this problem. The typical application are:

- **Identification of criminals-** collecting the evidence in the scene of crime (e.g., fingerprints) it is possible to compare with data of suspects or make a search in the database of criminals.
- **Surveillance -**-using cameras one can monitor the very busy places such as stadiums, airports, meetings, etc. Looking in the crowds for suspect, based on the face recognition biometric, using a images (e.g., mug shots) database of wanted persons or criminals. Since the events of September 11, 2001, the interest in biometric surveillance has increased dramatically, especially for air travel applications. Currently there are many cameras monitoring crowds at airports for detecting wanted terrorists.
- **Corrections -**This refers to the treatment of offenders (criminals) through a system of penal incarceration, rehabilitation, probation, and parole, or the administrative system by which these are effectuated. Is this cases a biometric system can avoid the possibility of accidentally releasing the wrong prisoner, or to ensure that people leaving the facilities are really visitors and not inmates.
- **Probation and home arrest -** biometric can also be used for post-release programs (conditional released) to ensure the fulfillment of the probation, parole and home detention terms.

5. COMMERCIAL

Banking and financial services represent enormous growth areas for biometric technology, with many deployments currently functioning and pilot project announced frequently. Some applications in this sector are:

- **Account access -** The use of biometric for the access to the account in the bank allows to keep definitive and auditable records of account access by employees and customers. Using biometry the the customers can access accounts and employees can log into their workstations.
- **ATMs -** the use of biometric in the ATM transaction allows more security,
- **Expanded Service Kiosks -** A more receptive market for biometrics may be special purpose kiosks, using biometric verification to allow a greater variety of financial transaction than are currently available though standard ATMs.

- **Online banking -** Internet based account access is already widely used in many places, the inclusion of biometric will make more secure this type of transactions from home. Currently, there are many pilot programs using biometric in home banking.
- **Telephony transaction -** Voice-scan biometric can be used to make more secure the telephone-based transactions. In this type of application, when the costumer calls to make a transaction, a biometric system will authenticate the customer's identity based on his or her voice with no need of any additional device.
- **PC/Network access -** The use of biometric log-in to local PCs or remotely through network increase the security of the overall system keeping more protected the valuable information.
- **Physical access -** the biometric is widely used for controlling the access to building or restricted areas.
- **E-commerce -** biometric e-commerce is the use of biometrics to verify of identity of the individual conduction remote transaction for goods or services
- **Time and attendance monitoring -** In this sector the biometrics is used for controlling the presence of the individuals in a determine area. For example for controlling the time sheet of the employees or the presence of students at the classroom

6.BIOMETRICS IN MOBILE PHONES

Nowadays, shopping through the internet has become very popular and surely, a WAP enabled mobile phone provides the facilities to consumers to shop online. Credit cards continue to be an efficient tool for online money transactions. But, on the other hand, credit card's number can be stolen on its way to its destination and can be misused by hackers. Thus, e-Business through a mobile phone becomes insecure.

7.FUTURE MOBILE PHONE

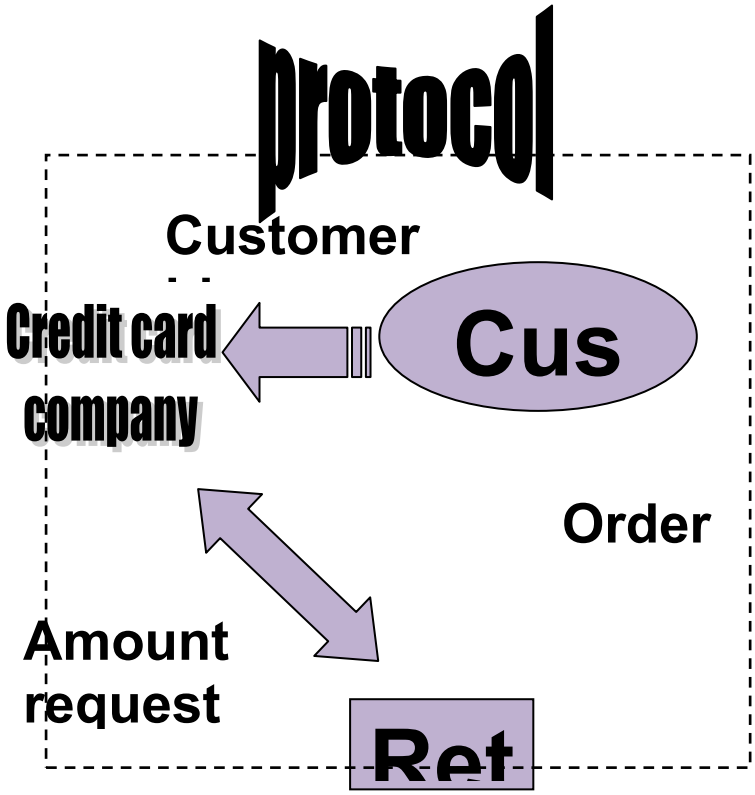
8.FACE RECOGNITION

Facial recognition is considered to be one of the most tedious among all scans. Further, difficulty in acquisition of face and cost of equipments make it more complex.

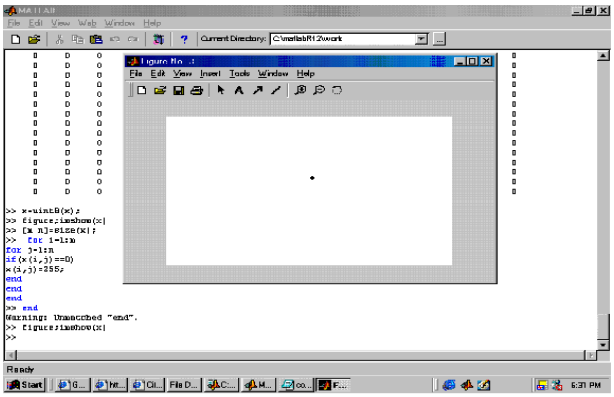
However, some WAP enabled phones like CX 400K and LG-SD1000 manufactured by LG electronics, have built in camera that can acquire images and can be transmitted over internet. This it is sent to the credit card company to verify the face received matches with the face in their database. If it matches, the goods are sent, else the order is rejected.

Figure1

Figure 2



We in our IMAGE PROCCESSING LAB took two faces with small differences (you see a small dot in the forehead of second face) and programmed MATLAB to find the difference between the two. The output is place below:



Difference between two images can be found by MATLAB.

The above simulations shows that even two persons having almost similar face with minute difference can also be differentiated.

Now, there arises a problem. A man, without bread, make as a transaction successfully .A week later he makes another transaction with some hair grown on his chin and go for acquiring images of

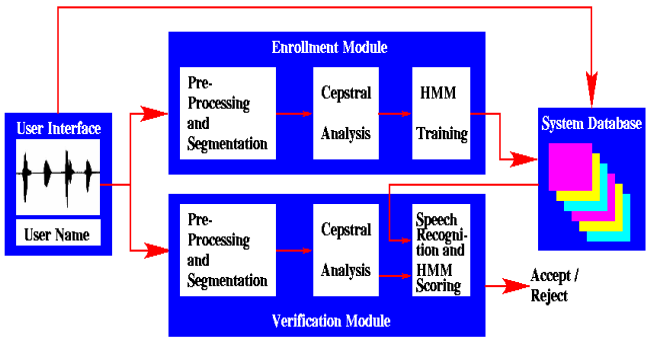
any part of the face like forehead, nose, ear etc.

Hence, this type of facial scanning system can be used as a part of the multi-biometric system we have presented above.

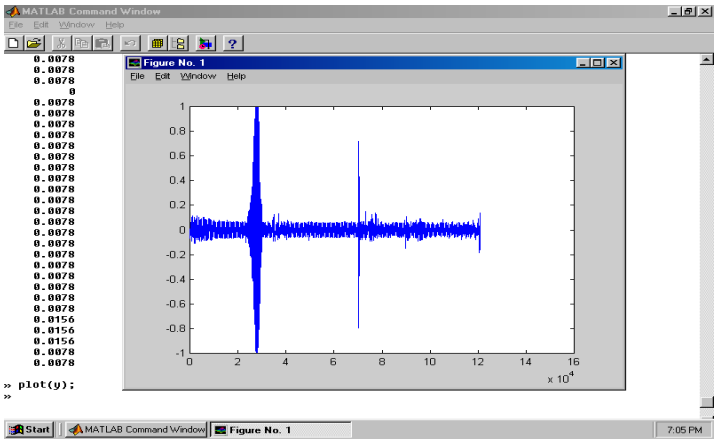
9. VOICE RECOGNITION

The speaker-specific characteristics of speech are due to difference in physiological and behavioral aspects of the speech production system in humans. The main physiological aspect of the human speech production system is the vocal tract shape. The vocal tract modifies the spectral content of an acoustic wave as it passes through it, thereby producing speech. Therefore, it is common in speaker verification systems to make use of features derived only from the vocal tract.

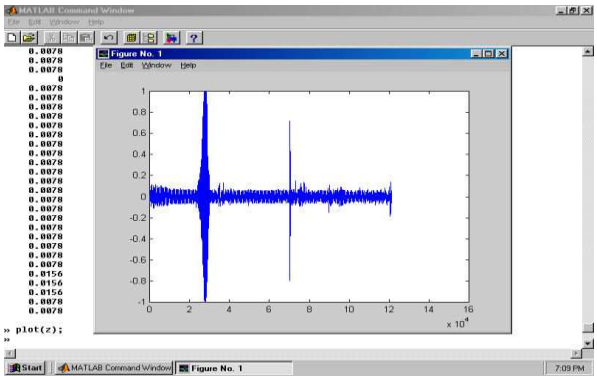
The microphone in the mobile phone captures the speech. Then, using cepstral analysis, an utterance may be represented as a sequence of feature vectors. Utterances, spoken by the same person but at difference times, result in similar yet a different sequence of features vectors. So, the irrespective of the mood of the consumer, his transaction is accepted or rejected. The following algorithm may be used in voice verification.

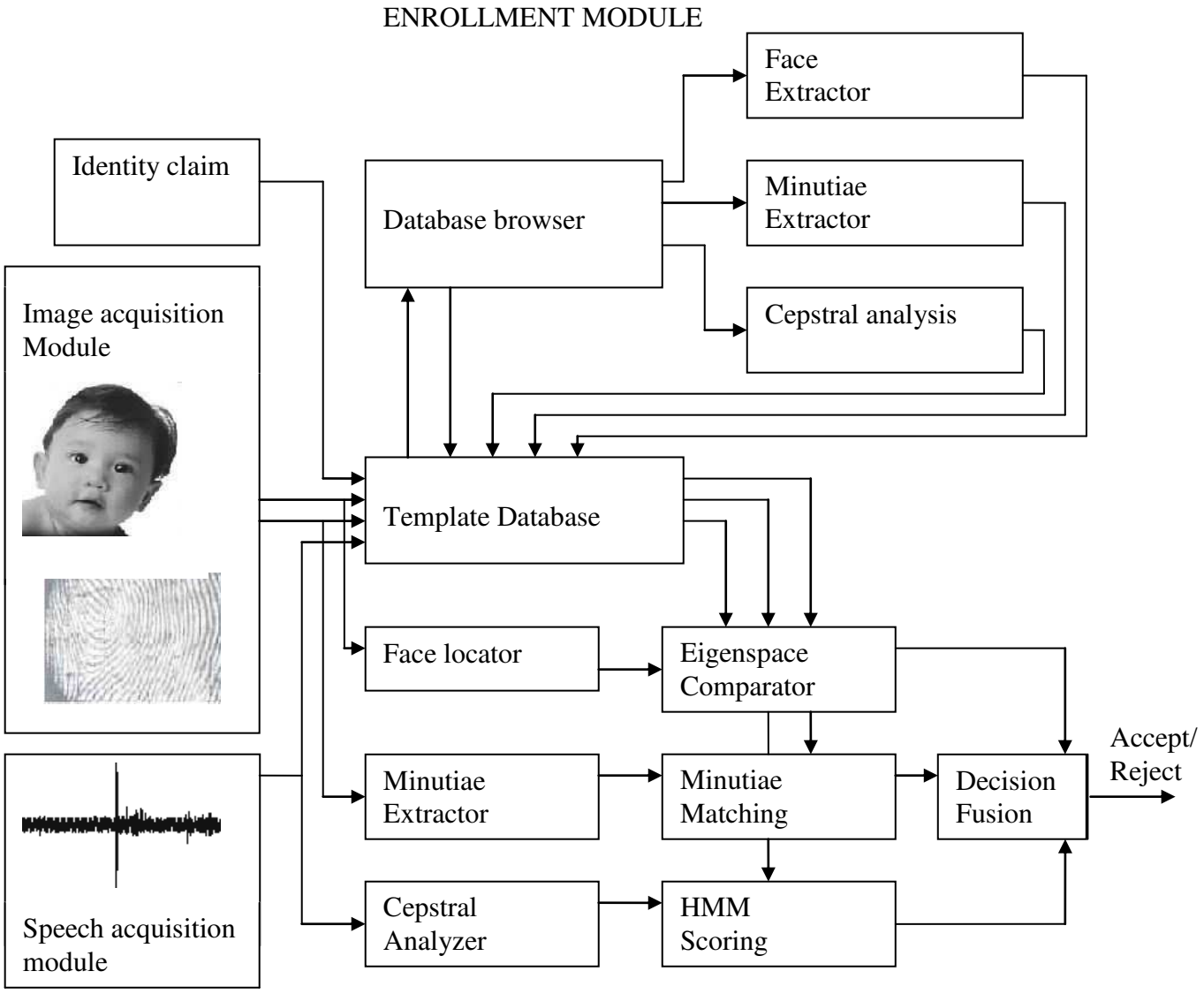


Flowchart for Voice verification



We recorded a person saying the letter ‘a’ directly into a sound recorder and plotted the graph1. This was simultaneously recorded in a tape recorder and Graph2 was plotted. The above graph shows some minute differences which prove that this system cannot be fooled by *imitation.*





As every mobile phone have an in-built microphone and some have video camera, the need for an extra hardware for the speech and image acquisition is eliminated. A proposal for
the display screen to act as a fingerprint acquisition is dealt later.

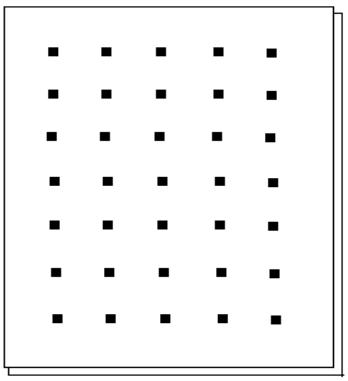
10.FINGERPRINT ACQUISITION:

Finger based scanning is one of the oldest methods used for verification. Fingerprints, unique and immunable for all are made of series of ridges and furrows on the surface of the finger. These ridges and furrows determine the uniqueness of the fingerprints. Apart from these, minute points (i.e. local ridge characteristics that occur at either a ridge bifurcation or a ridge ending also play role in fool-proofing this biometric technique.

To reduce the search time and the computational complexity, fingerprint classification is undertaken and thus fingerprints are classified as whorl, right loop, left loop, arch, and arch. Recently researchers and scientists achieved a great feat by improving the fingerprint classification to 94%.

In today's world, fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. In minutiae based technique, the minutiae points are found and their relative placement are mapped on the finger whereas in correlation based technique, the fingerprint acquired from the person is checked for certain points previously stored in the database. If both matches, the person

is given authentication, else he is denied permission.



Transaction scanner embedded above display screen

The scanner here is a transparent layer above the screen. The scanner consists of arrays of capacitors of the size of 0.03μm. capacitors with such a small size can be manufactured with MEMS technology. When the consumer places his thumb on the scanner, the points at which his fingerprint touches the screen get discharged whereas others remain charged. Thus the fingerprint is scanned and is then sent for further process.

11. CONCLUSION

Thus, this mobile multi-biometrics can be embedded in mobile phone. Phone is cost effective since no special hardware in required and is highly secured. Thus, this mobile phone becomes a reality will provide more e-Business and E-Transaction

REFERENCES

[I] Ani1 K. Jain, Ruud B o k , and Sharath Pankanti, ***Biometrics: Personal Identification in Networked Society*** Ed. **Kluwer** Academic Publishers, 2001.

[2] Ani1 K. Jain, **Arun Ross,** and Sharath Pankanti, **"A** Prototype Hand Geometly-based Verification System," **Proc.** of 2nd Int. Conf. on Audio- and Video-based Biometric Person Authentication, Washington D.C., pp.166-171, March 22-24, *1999.*

[3] C. M. Bishop, ***Neural Networks /or Pattern Recognition,*** Ed. Oxford University Press, 1995.

[4]**Ani1 K.** Jain , ***Fundamentals of Digitol Image Processing.*** **Prentice Hall.** 1989.

[5] ***S*** **.** Bow, ***Pattern Recognition and Image Preprocessing,*** Ed. Marcel Dekker, 1992.

(61 Biilent **Sankur,** Mehmet **Sezgin, "Image** thresholding **Techniques: A** survey **over** categories".(visited in **June** 2002) **h t t p : l l ~ . b u s i m . e e . b o u n . e d u . t r / - s a n k u**1**r**.do**C**