IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Network Security In Multimodal Biometrics

UMASANKARI. N
Dept. of Computer Science and Engineering, Vel tech Engineering
Avadi, Chennai -600 050, Tamil Nadu, India.

Abstract

The most reliable user authentication is becoming an important task in the web-enabled world. The consequence of an insecure authentication system in a corporate or enterprise environment can be catastrophic. Authentication and security have been major issues right from the beginning of the computer age. Password abuse and misuse, intentional and inadvertent is a gaping hole in network security.

One of the emerging and efficient techniques for implementing security is multimodal biometrics technology that strives towards authenticating the identity of a living person based on a biological key. The physiological biometrics is hand geometry, fingerprints, facial characteristics, retina and iris. The behavioral characteristics are signature, keystroke and voice.

The pattern recognition system that establishes the authenticity and possessed by a user and integrated into a database provide a new dimension of protection against fraud, falsification and duplication.

The encryption is an important process and Biometric devices eliminate the problems like lost cards, lost keys, forgotten PINs and unauthorized access. In this paper we described the different methodologies, its applications, future developments, and the hardware and software useful for this biometrics.

Keywords: *Biometrics, Multimodal, Face, Fingerprint, Iris, Signature, Fusion*

Synopsis

1. Introduction:

The term "Biometrics" is derived from “Greek” Bio means life and metric means measure. Biometrics is the science of verifying a person’s identity based on unique personal characteristics, such as voice, face, eye, or fingerprint. These can be captured, analyzed and stored as "Bioprints" in database, smart card in an embedded chip.

Biometrics is the development of statistical and mathematical methods applicable to data analysis problems in the biological sciences. A Biometrics system is basically a pattern recognition system, including all the hardware and associated software and the interconnecting infrastructure, enabling identification by matching a live sample to a stored pattern in a database. Logically a biometric system can be divided into two stages:

- The enrollment module
- The identification module

The enrollment module is responsible for training the system to identify a given person. In the identification module, the biometric sensors capture the characteristics of the person to be identified and convert it into the same digital format as the template.

1.1 History

At first the biometrics was practiced in China in the 14th century, explorer Joao de Barros reported it. He wrote that the Chinese merchants were stamping children's palm prints and footprints on paper with ink to distinguish the young children from one another.

Afterwards in 1890s, an anthropologist named Alphonse Bertillion, developed 'Bertillonage', a method of bodily measurement, which got named after him. Bertillion realized that even if names changed, even if a person cut his hair or put on weight, certain elements of the body remained fixed, such as the size of the skull or the length of their fingers.

Police authorities used finger printing, which was implemented by Richard Edward Henry of Scotland Yard. This method paved the way for the further developments.

1. Methodologies in Use:

- Fingerprint recognition
- Face recognition
- Optical recognition

- Signature verification
- Hand geometry
- Voice verification
- Keystroke recognition

1.1  Fingerprint Recognition:

Fingerprints are a distinctive feature and remain invariant over the lifetime of a subject, except for cuts and bruises. Fingerprints are one of the most mature biometrics technologies used in forensic division for criminal investigation.

Steps:

- A fingerprint impression is acquired using an inkless scanner.
- The digital image of the fingerprint includes unique features like ridge bifurcations and ridge endings termed as minutiae.
- The next step is to locate these features in the fingerprint image using an automatic feature extraction algorithm.
- Due to the sensor noise and other variability on the imaging process, the feature extraction stage may miss some minutiae and also due to the elasticity of the human skin, the minutiae may be disported from one impression to the next.
- In the final stage, the matcher subsystems attempts to arrive at a degree of similarity between the two sets of features.

Comments:

- It is a good choice to use this in the house security systems.
- It is low cost and very ease to integrate in the fingerprint authentication devices.

1.2  Face Recognition:

An image of a person's face is stored digitally when the person opens an account. At each transaction, a tiny camera feeds a live image of the person to the database, which compares the image to the one stored and to the account figure.

Steps:

- The system collects a database of face images.
- It generates a set of eigenfaces by performing Principal Component Analysis.
- On the face images, approximately hundred Eigen vectors are enough for a large database of faces.
- The system then represents each face image as a linear combination of the eigenfaces.

Comments:

- Majority of face recognition are Sensitive to variations in illuminations.
- Changing facial positions can also have an effect on performance.

1.1  Optical Recognition:

A retina based biometric involves analyzing the layer of blood vessels situated at he back of the eye. It needs a low intensity light source through an optical coupler to scan the unique pattern of the retina. The iris code is calculated using eight circular bands that are adjusted to confirm the iris and pupil boundaries and byte code is generated. Iris codes derived from this process are compared with previously generated ones. The difference between two iris codes is expressed in terms of hamming distance. It is zero for identical ones and one for the different ones.

Steps:

- A user has to stand one to three feet from the system which contains three video cameras.
- The system determines the position of eyes.
- Two wide-angle cameras image user's torso.
- The third camera focuses on an eye and captures a single black and white digital image.
- The system looks at the patterns of light and dark iris areas and generates the byte code for that person.
- The system checks the bar code against the version stored in a computer database.

Comments:

- These devices found very difficult in reading images of those people who are blind or have cataracts**.**

1.2  Voice Verification:

Vector quantification is used to classify the audio sequence. From each voice pattern, a matrix is created and the vector quantifier combines these matrices into one matrix. This matrix serves as a prototype that displays the reference voice pattern. Voice recognition is of two types, text dependant and

text independent. In text dependant recognition, the speaker says a predetermined phrase. This technology enhances recognition performance, but requires co-operative user. In text independent recognition, the speaker need not say a predetermined phrase and need not co-operate or even be aware of the system.

Comments:

- Different people can have similar voice and voice can vary because of changes in health, emotional state and age.
- Poor quality can affect verification.

1.1. Signature Recognition:

Signature verification analyzes the way a user signs his/her name. The important ***signing*** *features are* ***speed, velocity*** and ***pressure***. It operates in a ***three dimensional environment*** where height***, width*** *and* ***depth*** of ***pen stroke*** is ***measured***.

Comments:

- The different biometrics systems can be integrated at multi-classifier and multi-modality level to improve the performance of the verification system.
- One drawback is that people always do not sign in the same manner. The angle in which they sign may be different due to their sitting position or due to writing placement on writing surface.

1.3 Keystroke Recognition:

This technology adds an extra dimension of keystroke dynamics. By simply knowing the password the intruder, cannot enter into the system, but they must also be able to replicate the rate of typing and intervals between letters to gain access to the information. It is not possible for the intruder to, type it with the proper rhythm unless they have had the ability to hear and memorize the correct user's keystrokes. This is one of the most least secure new biometric technologies.

2.6. Hand Geometry:

It is concerned with measuring the physical characteristics of the hand and fingers. It may be suitable for users who access the systems infrequently and may therefore be less disciplined in their use of the systems.

2. Multi-Modal Biometrics:

This multimodal biometric system integrates fingerprint recognition, face recognition and signature recognition in making a personal identification. It can be used to overcome some of the limitations of single biometrics.

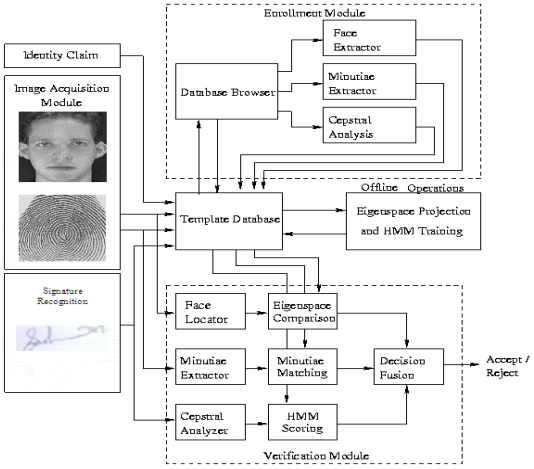


Fig. 3.1

4. Software and Hardware:

4.1. Software:

4.1.1. Secure Touch-n-PayRVS:

ScureTouch-n-PayRVS is provides finger image authentication for sales transactions. By matching the finger image provided during the sale to a master template already on file in Secure Touch-n-Pay, customers are protected from unauthorized sales transactions and retail stores are protected against fraud.

4.1.2. SecureTouchPAL:

SecureTouchPAL is helpful for the user to logon into the system by making use of the fingerprint authentication. It is compatible with Windows 95/98/ME operating systems. There is no limit for the numbers users to be enrolled.

4.1.3. SecureTouchGINA:

SecureTouchGINA is similar to the SecureTouchPAL software. It is compatible with Windows NT/2000 operating systems.

4.2. Hardware:

4.2.1. Secure Touch PC:

SecureTouch PC is a low cost, easy to use finger image reader that provides enhanced security for computer and network access control.

Unlike passwords, which can be lost, stolen or forgotten, finger image authentication assures that only authorized individuals gain access to the computer and network. SecureTouch PC is available in a Parallel Port model and a USB model.

4.2.2. Secure Touch PC Development Toolkit:

SecureTouch PC Development Toolkit enables us to add finger image security to our applications. This includes a Secure Touch PC unit, all standard SecureTouch software, plus three APIs, ("C", ActiveX, and Java) documentation, sample code and access to technical support.

5. Advantages Over Cards and PINs

Personal Identification Numbers were one of the first identifiers to offer automated recognition. This automation implies recognition of the PIN, not necessarily of the person providing it.

Likewise, a system may easily recognize cards and other tokens, but they could have been presented by anybody. Using a PIN and card together provides a slightly higher confidence level, but the security of such a system is still easily compromised.

Multi Modal Biometrics is not easily transferred between individuals. Verifying an individual's identity can become both more streamlined and considerably more accurate as biometric devices cannot be easily fooled.

6. Applications:

In Airport Security:

Biometrics is helpful in replacing the poorly trained, underpaid, and often incompetent airport security guards. Some fingerprint biometric systems are being installed at airports. Now the facial recognition systems are in use. The cameras are helpful to scan a crowd, matching faces against a database of known terrorists and criminals. One of the advantages of facial recognition systems is that a database of 1.1 billion facial images in identification databases already exists around the world.

- In border control biometrics can be used to bypass long immigration queues.
- Voting systems where eligible voters are required to verify their identity. This is intended to stop 'proxy' voting.
- It is being widely used in forensics for criminal identification.
- In automobiles, biometrics can replace keys with key-less entry devices.
- To prevent the drivers from having multiple licenses or swapped licenses among themselves when crossing state lines or national borders.
- In prison visitors systems, the visitors undergo verification so that identifiers are not swapped during the visit.
- Biometric techniques can potentially prevent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks.

7. Implementations in Biometrics:

In this paper we are implementing the project using MULTI MODAL BIOMETRICS by Java for the reputed institution. In this paper we will show the two modules from our whole project. This Model will check and compare the Finger Prints as well as Face Recognition System.

7.1. Java Technology Card:

This paper intention is to propose an efficient and universal Smart Card System to be implemented for banking applications over the Internet to support the fast growing Electronics Commerce Industry.

The project describes how smart card is being integrated with other Authentication specification to provide secure transactions over a distributed network such as the Internet. Using modern day technology, a 56-bit DES encryption algorithm can be broken into, just 2.3 DAYS using the EFF DES CRACKER. A simple PIN code verification is no longer sufficient. Hence, the paper has looked into the possibility of using biometrics as a mean of authentication.

The project recommends a new generation of Smart Card known as the Java Card. Implementing biometrics verification inside a smart card is notoriously difficult since the template tends to occupy a large part of the card memory.

8. Overview of Project:

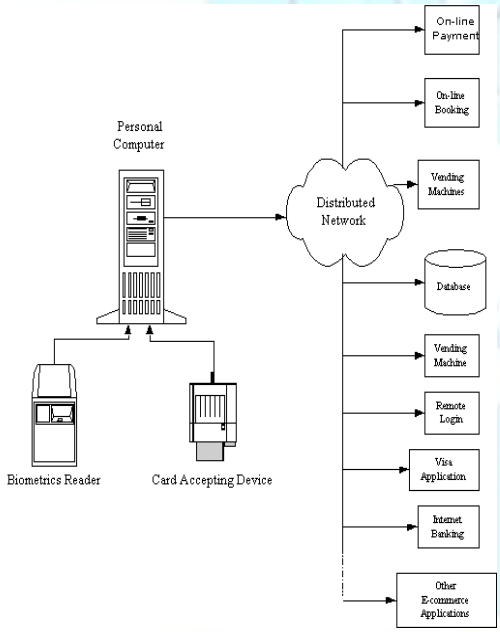
Finger Print Recognition, Face Recognition and Signature Verification System:

Our project aims to provide a reliable and universal smart card system for business applications over the Internet. Whenever a person purchases the java card, his fingerprint is saved within the Java card. The saved information is known as Template. As a

user wants to use the Java card his fingerprint is got in the real-time. It is then compared with the stored template [1]. If there is a match, he is authenticated. Thus it provides high security

since the fingerprint is a unique physical trait of a person. The java card and the card-accepting device are very expensive. So, we have used java card simulator and the scanner and web cam to take a face image respectively. Hence we couldn't do the fingerprint verification as well as face recognition described above. Here, we have saved the fingerprint of every individual in separate files and captured face image is also. Then, the fingerprint is got in real-time and saved in a file. Then calculate signature velocity.

Then all the file contents are compared to find a match of finger print and signature, also the face images are capturing through web camera. Then the face images are capturing during the runtime and compare the face images for the existing system.



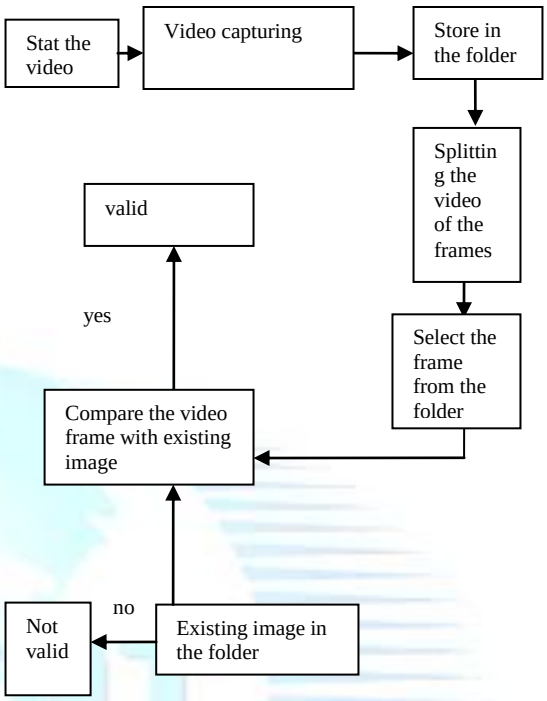


Fig. 8 .2

Its not match this system is give an alert to make a message is send to corresponding mail id and mobile number.

8.1. Signature Verification:

In multimodal biometrics terminology, the signature is a behavioral characteristic of a person and can be used to identify/verify a person's identity.

The signature recognition algorithm consists of three major modules i.e., Preprocessing and noise removal, feature extraction and computation of Euclidean distance. Offline signature acquisition is carried out statically.

Online signature acquisition, by capturing the signature image using a high resolution scanner. A scanned signature image may require morphological operations like normalization, noise removal by eliminating extra dots from the image, conversion to grayscale, thinning and extraction of high pressure region.

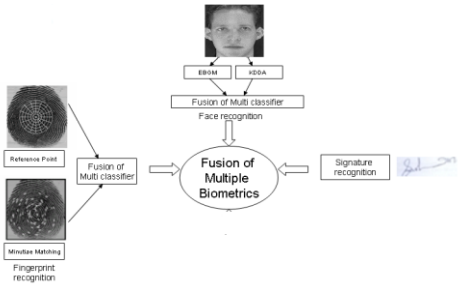


Fig. 8 .1.1.

9. Conclusion

This rapidly expanding market offers the opportunity to provide value-added services and differentiate services for their customer. It creates a potentially huge market for Java Card applications.

Smart cards with the Java Card API represent a relatively new set of technologies with a great deal of promise. The introduction of Java Card in this rapidly expanding market offers operators, equipment manufacturers and service providers the opportunity to provide value-added services and differentiate services for their customer.

The word multi modal biometrics will be heard more often everywhere in the future. It will surely make our world secure and safer to lead the life. This field is developing tremendously; it will play a critical role in future computers and especially in electronic commerce (i.e) e-com.

Multi Modal Biometrics is surely to move from the specialized applications to areas that impact our everyday lives. Public awareness and acceptance of biometrics is steadily increasing. Multi Modal Biometrics has been gaining recognition as a security solution that can improve the collective safety of society.

We all want the peace of mind safety for our family security for our business.

This is made to be possible with the help of Multi Modal Biometrics.

Multi Modal Biometrics provides greater protection to our personal information and financial assets, which is now more essential than ever before. Recent advances have made biometrics more reliable, accurate and cost-effective. These future proposals will surely come into our real life. The achievement is not so far.

Acknowledgement:

I express my profound thanks to the Chairman **Mr. Vel.Shri.Dr.R.RANGARAJAN. B.E(Elec.), B.E(Mech.), M.S. (Auto.), D.Sc.** and the Chair Person **Dr.Mrs.R.MAHALAKSHMI.B.E, M.B.A**. and the Director **Mr. K V D KISHORE KUMAR**. **B.E, M.B.A**.

I express my respectful and sincere thanks to Principal **Mr.Dr.K.RAJAN Ph.D**. and my friends for their encouragement and interest shown on me to complete my journal presentation work successfully.

I proudly thank to my father **Mr. S. NATARAJAN,** and my husband **Mr.SIVAKADHIR**, and my Brothers providing a great opportunity to pursue this paper study.

Finally the biggest of all the giants is my mother **Mrs. T. KOUSALYA**, who I cannot thank enough for the opportunities she has given me, the constant encouragement he provides and for always being there for me.

References:

Websites:

- www.biometrics.org
- www.biometricscatalog.org
- www.biom.cornell.edu
- www.biometrics.org
- www.biosmartcards.edu

Books:

[1] Sun Microsystems, Inc.: Java Card 2.0 Language Subset and Virtual Machine Specification, October 13, 1997.

[2] Sun Microsystems, Inc.: Java Card Applet Developer's Guide, July 17, 1998.

[3] CSI Communications –MAR 2002

[4] IBM Systems Journal Vol-40 No 3 2001