Blind Authentication: A Secure Crypto-Biometric Verification Protocol

Afshan Jabeen
Department of Computer Science & Engineering
Jhulelal Institute of Technology
Nagpur,India

Professor Nisha Balani
Department of Computer Science & Engineering
Jhulelal Institute of Technology
Nagpur,India

Abstract:- **Blind authentication biometric protocol, to concerns of user's privacy and trust issue. The protocol is blind in the sense that its the identity, no additional information about the biometric to the authenticating server. the protocol is based on asymmetric encryption of the biometric data, captures advantages of biometric authentication is the security of public key. The authentication protocol can run over provide nonrepudiable identity verification. The encryption provides template protection the ability revoke enrolled templates and alleviates the concerns on privacy in widespread use in biometrics. This approach makes no restrictive assumptions on applicable to multiple biometrics. a protocol has significant advantages over existing biometric cryptosystems use a biometric to secure a secret key, which is used for authentication.**

Keywords: ***biometric security system, recognition methods, identification, facial recognition, fingerprint, voice recognition, iris/retinal recognition, vein recognition, DNA recognition, privacy.***

1 INTRODUCTION

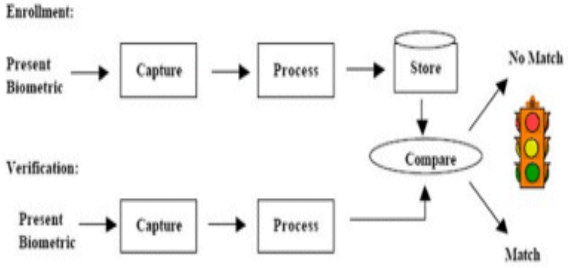
Biometrics is defined as the unique logical characteristics of human body, These characteristics are used to identify each human. Any details of the human body, differs from one human to another will be used as unique biometric data to serve that person unique (ID), such as, retinal, fingerprint palm print and Biometric systems to collect and store this data in order to use for verifying personal identity. Biometrics is the method of recognizing a person based on physiological characteristic. Biometric technology are becoming the foundation of extensive array of secure identification and personal verification solution.

Biometric technology should be considered and evaluated giving consideration to the following characteristics:

- **Universality**: Every person should have the characteristic. People who are without a fingerprint will need to be accommodated in some way.
- **Uniqueness:** Generally no two people have identical characteristic. However, identical twins are hard to distinguished.
- **Permanence:** The characteristic should not vary time. A person's face for example, may change with age.
- **Collectibility**: The characteristic must be easily measurable.
- **Performance**: The method to deliver accurate results under varied environmental circumstance.
- **Acceptability:** The general public accept the sample collection routines.
- **Circumvention**: This technology should be difficult to deceive.

Biometric authentication require comparing a enrolled biometric sample against newly captured biometric sample **Enrollment** a sample of the biometric is captured processed by computer, & stored for later comparison.

Biometric recognition can be used in **ID** mode, the biometric system identifies a person from entire enrolled population by searching a database for a match based on the biometric. For example, an entire database can searched to verify a person has not applied for benefits under two different names. This is sometimes called "one-to-many". A system can also be used **Verification** mode, where the biometric system authenticate a person claimed identity from their previous enrolled pattern. This is also called as "one-to-one" matching. In most computer access and verification mode be used. A user an account users name inserts a token as a smart card but instead of enter a password.



Biometric based authentication application include

workstations and network access, sign-on, application log on, protection, remote access resource, transaction security and Web security. The promises through the utilization strong personal authentication procedure. Secure electronic banking investing and other financial transaction, sales, law, health and social services are already benefit from these technology.

2 BIOMETRICS SOLUTION

2.1-Facial Recognition Detector

The human face is one of the easiest characteristics which can be used in biometric security system to ID a user. Face recognition technology is very popular and used more widely because it does not require any kind of contact between the user and device. Camera scan the user face and match it to a database for verification. it is easy to install and does not require any expensive hardware, facial recognition technologies are used widely in a variety of security systems such as, physical access control computer user account, it is still not as unique as its counterpart such as retinal, DNA. it is normally used with other characteristics in the system. the other hand, time is most negative affective factor with face recognition technology because the user will change over time Biometric face recognition system will collect data from the user face and store in a database for future use. It will measure overall structure shape and proportion of features on the user face such as distance between eyes, nose, ears, jaw, size of eyes, mouth and others expression. Facial expression is also counted as one of the factor to change during a user facial recognition processes. Example, include smiling, crying and wrinkles on the face.

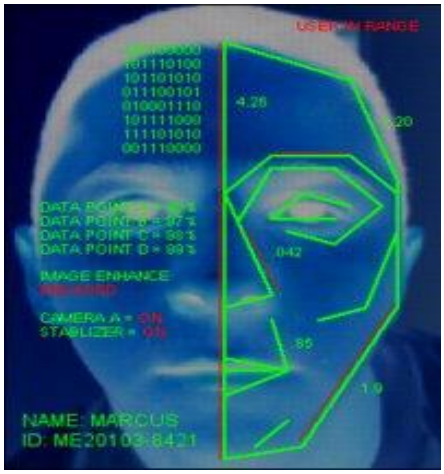


Figure - Example of face recognition scan

2.2-Fingerprint reader

Our fingerprint is made of a number of ridges and valley of finger that are unique each human. Ridges are the upper skin layer segments of the finger and valleys are low segment, The ridge form two points ridge ending where the ridges end ridge where the ridges split into two, The uniqueness of a fingerprints can be the different pattern of the ridges and furrows as well as the minutiae point. There are five basic pattern which make up the fingerprint: the arch such as tented and plain arch cover 5% of fingerprint; left and right loop cover 60% of fingerprint cover 34% of fingerprints and accidental cover 1% of fingerprint, 3 of 10 To capture the surface of fingerprint for verification the id of user, new technology are design with tools such as, optical and ultrasound. There are two algorithm are used to recognize fingerprint, matching and pattern matching. matching will compare the details of the extract to identify the difference between one user fingerprint as compared to other. When users register with the system, they will record images of location and direction on finger surface. users use fingerprint recognition system to verify their identification a image is brought out and compareand provided at the time of access. Pattern matching will compare all the surface of the finger instead of one point. It will concentrates in thickness curvature and density of fingers surface. The image of the fingers surface for this method will the area around a minutiae point area with low radius or areas with unusual combination of ridge, There are several benefit of using fingerprint recognition system. This system is easy to install. It requires cheap equipment which generally low power consumptions. there are some disadvantages of the system. If the surface of the finger get damaged and one or more marks it identification become increase hard. the system require the user finger surface to have a point of pattern in order to have matching image. This will be a limitations.

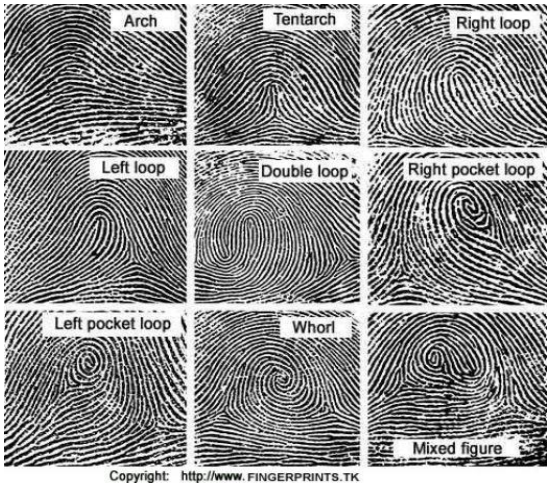


Figure - Fingerprint types [Lazaroff, 2004].

2.3-Voice Recognition

There are two factor which make a person voice unique. Firstly, the physiological component which is known as voice tract. Secondly a behavioral component which is known as voice accent. By combining both of these factor, it is impossible to another person voice exactly. Taking advantage of these characteristic, biometrics technology created voice recognitions system to verify each person identification using only voice. The voice recognition will focus on the tract because is a unique characteristics of a logical trait. It work perfectly in access control for users.

2.4-Iris Scanner & Recognition

The human iris is a thin circular structure in the eye which is responsible for control the diameter and size of the pupil. It also control the amount of light which is allowed through to retinal order to protect the retina. Iris color is also a different to each person depending upon their gene. Iris color will decide eye color for each individual. There are several color for iris such as, brown, green, blue, grey, hazel (the combination of brown, green and gold), violet.. The iris also has its own pattern from eye to eye & person to person, make up to uniqueness for each individual. .
Iris recognition system will scan the different ways. It will analyze over 200 point of the iris including: rings, furrows, freckles and others characteristic.
It will save the information in database, for future use comparing every time a user want to access the system. recognition security system are considered as one of the most accurate security system nowaday. Its unique and easy to identify a user. Even the system require installation equipment and expensive fee it is the easiest and fastest method to identifies a user. There should be no physical contact between the user and system during, the verification process. the verification process, if the user are wearing accessories such as glasses and contact lenses the system will work normal because it doesn't change any characteristic of the user iris.

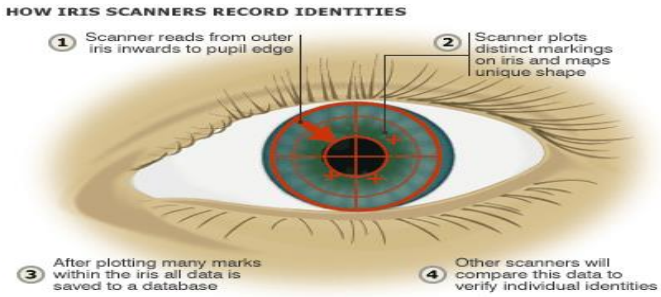


Figure - How Iris Scanners Record Identities

2.5-Veins Recognition

One of the recent biometric technology invented is the vein recognition. blood vessels that carry blood to the heart. persons vein have unique physical trait. Taking advantage of the biometric characteristics of the vein as a method to identify to the user. Vein recognition system mainly focus on the vein in the users hands. finger on humans hand has veins which connect directly with the heart and its own physical trait. Compared to the other biometric system. the user veins are located inside human body. the recognition system will capture image of the vein pattern inside of user finger by applying light transmission to each finger. For more details it works by passing near infrared light through finger, this way a camera can record vein patterns recognition system are getting more attention from expert because it has many other function which other biometric technology, It has a higher level of security which protect information, access control better. The level of accuracy used in vein recognition systems is impressive and reliable by the comparison of recorded database to the current data.

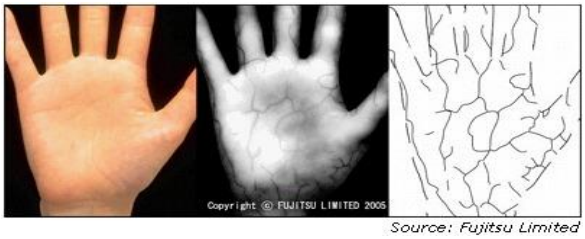


Figure - One example of vein scanning

2.6-DNA Biometrics System

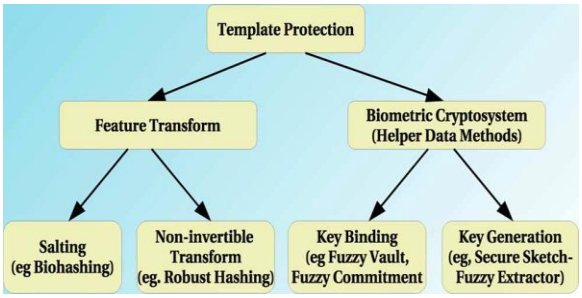
One of biometric technologies it is used in security systems recently is DNA biometric. It is impossible to fake this characteristics because each person DNA is unique. Each person DNA contain some trait from her parents. Each cell in the human body contain a copy of this DNA. profiling will decide the amount of which repeat at a number of distinctive loci.

2.7-2D Barcode Scanner

2-D barcode biometric technology is a 2-dimesional method of security information which is provided by the biometric technologies system. 2-D barcode is normally applied during the identification of item rather than users. its application is still used to verify the identification of user. By combining 2-D barcode and biometric, it will create a better security level can be accessed easily and faster. By using method, security level of system cannot be easily penetrated by the unauthorized users. It provide a more effective and efficient security, for 2-D barcode biometric technology have been used for a certain time but it is not user have not the benefit identifying user.

3. RELATED WORK

System and Detail, The previous work in the area of encryption security of biometric template tend to model the problem that of building a classification system separate the impostor sample in the encrypted domain. a strong encryption mechanism destroy patterns in the data which adversely affect the accuracy of verification, Hence, such matching mechanisms necessarily makes compromise between template security and accuracy.



4. CONCLUSION

The advantage of the proposed approach is that are able to achieve classification of a strongly encrypted feature vector using generic classifier, The authentication server need not

the specific biometric trait that is used by a particular user, which can even vary across user. Once a trusted enrollment server encrypts classifier for a specific biometric of a person, authentication server is verify the identity of a user to that encryption. The real identity of the person is hence not revealed the server making the protocol, completely blind. This allows one to revoke enrolled template by change the encryption key use multiple key across different server to avoid being tracked leading to privacy. The proposed blind authentication is extremely secure variety of attacks can be used with a wide variety of biometric trait. Protocol are designed to keep the interaction between the user and the server.

5. FUTURE ENHANCEMENTS

The verification can be done in real-time, with the help of available hardware this approach is practical in many application. The use of smart card to hold encryption enables application such as, biometric ATMs, access of services from public terminals. Possible extension to work include secure enrollment protocols and encryption method to reduce computation. This methods to do dynamic warping-based matching of variable length feature vectors can further enhancement utility of the approach. Biometric future will include e-commerce application for extra security on the page, biometrics will guard against unauthorized access, to car and cell phones. In the future, biometric technology will further develope 3-D infrared facial recognition access control, facial recognition and visitor management authentication system. Multilevel recognition can be made in authentication.

REFERENCES

[1] S. Abe, Support Vector Machines for Pattern Classification. New York: Springer, 2005.
[2] Anastasios Texas, Constantine Kotropoulos, Ioannis Pitas," Using Support Vector Machines to Enhance the Performance of Elastic Graph Matching for Frontal Face Authentication", IEEE transactions on pattern analysis and machine intelligence, vol. 23, no. 7, 2001 [Reid, 2011]
[3] Paul Reid, "Biometrics for network security", Pearson Education Inc., 2004, ISBN 0131015494 [Schuckers, 2001]
[4] Michael E. Schuckers, "Some Statistical Aspects of Biometric Identification Device Performance", 2001 [Tistarelli, 2009]
[5] Massimo Tistarelli and Marks Nixon, "Advances In Biometrics", Springer-Verlag Berlin Heidelberg 2009, ISBN 03029743