Biometric Systems Authentication & Multi-Modal Biometric System
Harshil Joshi1 Chaitasee Pandya2
1M.E., Computer Science & Engineering
2B.Tech., Computer Science & Engineering

Abstract—This paper gives outline of different biometric technologies and biometric authentication process. A biometric system which relies on only a single biometric trait is often not able to meet the desired performance. In Multi-modal system more than one biometric traits are used to identify a person. The study of methods for uniquely recognizing based upon one or more intrinsic physical or behavioral. In this paper we present the use of multimodal biometric system to get the higher degree of security.

Keywords: Different Types of Biometric Technologies, Biometric Authentication Process, Multi-Modal Biometrics System, Applications of Multi-Modal Biometrics.

Introduction: This paper summarizes different technologies that are used for mobile payment systems. Types of biometric authentication process which is used for mobile payment systems. And, Multi-Modal Biometric systems and it's applications.

I. DIFFERENT TYPES OF BIOMETRIC TECHNOLOGIES

Following are the types of biometric technologies which can be used for mobile payments.

- Facial Recognition: This technology is used to identify people from still or video photograph image of their faces.[1]
- Fingerprint Identification: The technology that make authentication through fingerprint. A fingerprint is the pattern of ridges and furrows on the surface of fingertip. No two persons have exactly the same arrangement of patterns, and the patterns of any individual remains same throughout life.[2]
- Retinal Pattern Recognition: The technology to authenticate people through scanning their eyes. The retina is the innermost layer of the eye. The pattern formed by veins beneath the surface of the retina is unique to each individual. [3]
- Iris Based Identification: This technology authenticates with iris scanning. The colored part of the eye is iris. It lies at the front of the eye surrounding the pupil.[3]
- Voice Recognition or speaker recognition is a technology through which voice of a person is recorded. The biometric technology uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (i.e. shape and size of throat and mouth) and learned behavioral patterns (i.e. voice pitch, speaking style). [4,5]
- Signature Recognition: This technology is used to verify the signature of the individual.
- Signatures of people vary substantially. It is based on measuring dynamic signature features such as speed, pressure and angle used when a person signs a standard, recorded pattern (e.g. autograph). [4,5]

A. Biometric Authentication Process:

There are two processes in biometric authentication. Enrollment process and verification process.

1) Enrollment Process:
In this process the biometric template of the customer is captured and stored in biometric database. The typical steps in enrolment process are:

1) The customer is asked to enter a customer identity number (this could be a bank related number, a national ID or any other unique identity number).
2) The customer is then asked to present their biometric template on a scanner that then captures the images.
3) The enrolment system may ask the customer to present their biometric multiple times to ensure that the quality of image captured is good for verification.
4) An ISO 19794-2 template is derived from the captured images.
5) The template along with the raw image is stored in the biometric server against the customer identity number for later retrieval and verification.[6]

2) Verification Process:
In this process customer biometric template is verified to authenticate the payment. In verification process the customer enters their customer identity number into the verification system. The system then prompts the customer to present their live biometric on the scanner. The live biometric is then compared with the biometric template stored against the customer identity number in the biometric server. In case the verification is successful the payment transaction is considered authenticated and the transaction sent to the bank for processing. In case of a failure the customer may be asked to present the biometric template again up to a certain maximum number of tries. Implementing a biometric authenticated payment system requires three primary system elements to be put in place by a bank or acquirer. These are:

a) Enrollment System:
Used for enrolling customers on to the program and recording their biometric identity. In enrolment stage the biometric images of the different individuals to be verified are first processed by feature extraction module; the extracted features are stored as template in a database for later use.

b) Verification System:
Used at retail locations for verifying the live biometric template with the stored fingerprints for authenticating
Payments. The biometric image of the individual to be verified first processed by feature extraction modules; the extracted features are then fed to a matching module with his/her identity ID, which matches them against his/her templates in the database.

c) Biometric Server:
Used for storing the biometric template, extracting and verifying biometric template during a payment process and providing an interface to banks and acquirers for managing the customer data and reports. [8]

II. SECURE BIOMETRIC AUTHENTICATION:
Biometric data are not secret. We cannot expect that the biometric characteristics are not available to attackers. Therefore the knowledge and presentation of the data subject's biometric data should not directly lead to a successful authentication. This is why remote biometric authentication does not work (is not secure) in most cases (despite of some broad framework specifications [7]). Locally we can try to verify so called liveness (also called liveliness) to make sure we are processing the fresh biometric data originating from the person being authenticated. Liveness tests are specific for a particular biometric modality and can be roughly divided into two categories. Static tests measure some physiological characteristics (like the finger temperature or conductivity) that should discriminate between the living human and an artificial fake. Therefore, secrecy of biometric data and the need for liveness testing. For secure authentication the biometric system must be convinced that the presented biometric measurements are coming from a trusted and unmodified input device and are fresh. The biometric system should verify the liveness, otherwise the system could be cheated with copies of biometric characteristics. Sometimes the liveness test can be replaced with a human guard, it is however questionable whether a human guard can protect against more advanced biometric fakes (like a thin silicon layer at the fingerprint). If the authentication is done on-device, the device itself should be trustworthy. If the authentication is done off-device, then the operating environment of the software and the communication link between the software and the device have to be secured. For example, in a client-server application, if the client workstation is not trusted, then there is no point authenticating the person using that workstation. If one chooses to run the authentication software at the server side, then the communication link between the server and the device itself (not just the client workstation) has to be secured. Otherwise, a malicious party or even the workstation itself may intercept the communication and replay recorded biometric data. One way to defeat replay attacks is to put a separate secret key in the device and to use challenge/response protocol with this key. Obviously, the device has to be trustworthy. One possible solution would be to use a tunneling protocol with mandatory authentication of both parties. To protect the keys and to avoid modification of the liveness test the device must be tamper-resistant or physically secured. As we have already mentioned, remote biometric authentication is mostly not secure. There is no sense to send a fingerprint scanner to log-in to a web server if the fingerprint scanner is not trusted by the web server. And to be trusted can imply to have a reliable liveness test, to have a secret key to support data authenticity and to be tamper resistant (to protect the keys and to protect against modification of the liveness test or direct injection of attacker’s data – the device is fully in the hands of users and potential attackers). It is quite difficult to make a small smartcard tamper resistant. To design a tamper resistant fingerprint scanner is a real challenge. The raw biometric sample or templates need to be supplied for comparisons. Hashing the biometric data by a cryptographic hash function and sending only the hash [9] for comparison does not work (unlike for passwords). Biometric measurements never yield the same values, therefore cannot be directly compared in hashed or encrypted domain. There are some efforts of how to avoid the transmission of the full sensitive biometric data [8] and we discuss relevant issues below.

III. MULTI-MODAL BIOMETRICS SYSTEM:
The Multimodal biometric systems are providing identification and human security over last few decades. Due to this reason multimodal biometrics systems are adapted to many fields of applications. Some of these multimodal systems are human computer dialog interaction based systems where the user interacts with the PC through voice or vision or any other pointing device in order to complete a specific task. Multimodal biometric systems are those which utilize, or are capable of utilizing, more than one physiological or behavioral characteristic for enrollment, verification, or identification. A biometric system is essentially a pattern recognition system. This system measures and analyzes human body physiological characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements for authentication purposes or behavioral characteristics. The biometric identifiers cannot be misplaced. In spite of inherent advantages, unimodal biometric solutions also have limitations in terms of accuracy, enrollment rates, and susceptibility to spoofing. This limitation occurs in several application domains, example is face recognition. The accuracy of face recognition is affected by illumination and facial expressions. The biometric system cannot eliminate spoof attacks. In spite of using unimodal biometric system that have poor performance and accuracy, we study and propose a new approach to the multimodal biometric system. This new Multimodal biometric systems perform better than unimodal biometric systems and are popular even more complex. Multimodal biometric systems utilize more than one physiological or behavioral characteristic for enrollment, verification or identification. The reason to combine different modalities is to improve recognition rate. The aim of multi biometrics is to reduce one or more of the following:

- False accept Rate (FAR)
- False Reject Rate (FRR)
- Failure to Enroll Rate (FTR)
- Susceptibility to Artifacts

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
voice and fingerprint recognition would be considered “multimodal” even if the “OR” rule was being applied, allowing users to be verified using either of the modalities.

C. Law enforcement

An Automated Fingerprint Identification System, or AFIS, is designed to enable a fingerprint to be matched extremely quickly against a large number of records in a criminal database. To do this effectively it will almost always hold encodings of all ten fingers. Law enforcement agencies have achieved significant success with facial recognition, matching the mug shot (or even composite drawing) of a suspect against a database of offenders. This is particularly useful where the individual has refused to give his name, or has given a false name.

V. Conclusion

In this paper different biometric technologies are discussed. The primary advantage of biometric authentication methods over other methods of user authentication is that they really do what they should, i.e., they do authenticate the user. They do not rely on objects the user carries or something the user has remembered. Biometric authentication methods use the real human physiological or behavioral characteristics to authenticate users. These characteristics should not be duplicable, but it is unfortunately often possible to create a copy that is accepted by the biometric system as a true sample. Well-known investigations [10,11] confirmed our earlier findings that attacks may be much easier than generally accepted. The biometric authentication also has some other advantages. Most biometric techniques are based on something that cannot be lost or forgotten. This is an advantage for users as well as for system administrators because the management of lost, reissued or temporarily issued tokens/cards/passwords can be avoided. So why do not we use biometrics everywhere instead of passwords or tokens? Nothing is perfect and biometric authentication methods also have their own shortcomings. First of all the performance of biometric systems is not ideal (yet?). Getting the result is quite clear and quick when comparing two passwords. Comparing two sets of biometric characteristics is not so straightforward. Biometric systems still need to be improved in the terms of accuracy (and sometimes also speed). The fail to enroll rate (FTE) brings another important problem. Not all users can use any given biometric system. People without hands cannot use fingerprint or hand-based systems. Visually impaired people have difficulties using iris or retina based techniques. Even enrolled users can have difficulties using a biometric system. Biometric data are not secret and the security of a biometric system cannot be based solely on the secrecy of the biometric characteristics. The server cannot authenticate the person just after receiving her correct biometric characteristics. User authentication can be successful only when the person’s characteristics are fresh and have been collected from the person being authenticated. This implies that the biometric input device must be trusted. Its authenticity should be verified (unless the device and the link are physically secure) and the liveness should be checked. We believe that the biometric authentication is a good additional authentication method. Even cheap and simple biometric solutions can often increase the overall system security if used on top of existing traditional
authentication methods. Replacing a current traditional authentication method with a biometric one, on the other hand, may be risky and requires deeper analyses. Biometric authentication systems often replace traditional authentication systems not because of their higher security but because of higher comfort and ease of use. Biometric key generation is far from mature. The high false rejection rate and short key length are the common shortcomings of most current systems, yet the first practically usable implementations are appearing. However, the use of biometric keys has to cope with the fact that biometric data are not (fully) secret. This makes the use of directly derived biometric keys very problematic, but also biometrically locked cryptographic keys have to take into account that compromise of the biometric data implies easier access to the locked keys – and prudent implementers will protect the secrecy of the locked keys by additional means. Multimodal biometrics system has been presented. By combining multiple biometric traits, the performance of biometric system can be improved. Various applications of multimodal biometrics system and different levels of fusion are discussed. The multimodal biometrics is very popular in these days due to its performance and advance level of security. Though some complexity also exists in multimodal system which reduces its acceptability in many areas.

REFERENCES