Emphasizing On Multimodal Biometric System : Survey

Achal Sancheti, Paridhi Nahar

Abstract— **Authentication is a key requirement of security. Authentication can be performed by highly complex and secured method or by simpler one. The factors of authentication fall into three categories: something the user knows, something the user has, and something the user is. This paper focuses on the authentication schemes that are still to be overcome even after the use of any of these existing passwords, smart card schemes or single biometric system considering the solutions prevailing to adopt the multimodal biometric system.**

Index Terms— **Authentication, identification, monomodal, multimodal biometric.**

I. Introduction

The process of identifying an individual usually based on username and password is authentication.

Authentication ensures that illegal users do not obtain system’s resources fraudulently. It also provides the legal users to use the resources of the system.

For effective results, the following factors should be considered:

1. **Knowledge Factors** are the factors that are **known to users** such as password, pattern, PIN, and so on.
2. **Ownership Factors** are the factors that the **user has** such as wristband, ID card, and so on.
3. **Inherence Factors** are the factors that **user is or does** such as finger print, signature, face, voice, and so on.

The knowledge factors authentication is the simplest and most commonly used method. Another scheme that provides the identification and authentication is ownership factors. But as the security is becoming more important as technology is increasing, authentication becomes a key requirement for security.

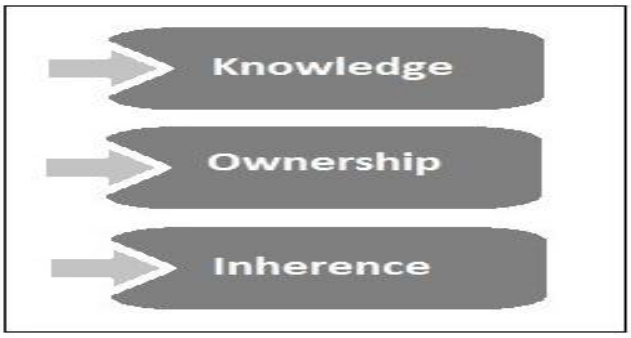


Figure 1.1: Factors of Authentication

Manuscript received November 13, 2014.

Achal Sancheti, Student of Swami Vivekanand College of Engineering, Indore, Rajiv Gandhi Technical University, Bhopal, India

Paridhi Nahar, Student of Swami Vivekanand College of Engineering, Indore, Rajiv Gandhi Technical University, Bhopal, India

The strongest security can be possessed by recognizing a person based on his/her own physiological or behavioral properties. This can be done by inherence factors like face, signature, finger print, hand geometry, iris, retinal, voice etc. This is referred as biometric system.

Biometric technologies are becoming the foundation of an extensive array of highly secure identification and a personal verification technology is becoming apparent. [1]

II. PROBLEM DOMAIN

Traditional password authentication scheme is not secure. It can easily be hacked and is at the verse of increasing target for hackers via spyware and key loggers.

In fact, a study of 272 large corporations by Intrusion.com found that 13% of users did not need passwords, 82% weren't required to change their password and 44% weren't required to use sufficiently long passwords. Furthermore, 16% of user accounts were inactive, allowing undetected entry.

Smart cards are generally used with the user specified passwords for authentication as a two-factor authentication. The point is about not to discuss what the smart card is, but rather to talk about what to do for a specific problem involving smartcard. Smart cards have also been the targets of security attacks.

Study ensures that, another problem with the smart cards is the lack of standards for functionality and security. To address this problem, The Berlin Group launched the ERIDANE Project to propose "a new functional and security framework for smart-card based Point of Interaction (POI) equipment".

In the fraud cases, the passwords can be hacked or changed and the new smart cards can be requested against security. However, the finger print impression, iris, voice cannot be changed, even though biometric system is not secured. The users always left their impression wherever he/she touched. The artist can modulate their voice, which may occur a serious issue against the authentication as well as security.

Biometric products provide improved security over traditional methods of authentication. The combination of biometric data systems and biometrics recognition identification technologies creates the biometric security systems. Since biometric identifiers are unique to individuals, they are more reliable in verifying an individual. With reference of study, the biometric industry revenues in the past few years is shown in the following graph: [2]

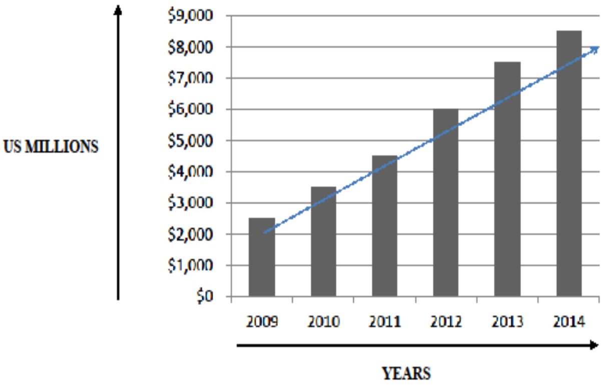
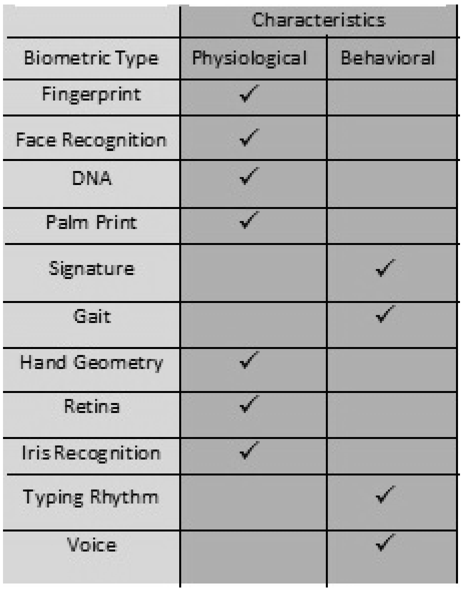


Figure 1.2: Biometric Industry Revenues

A biometric system is a technology that uses physiological or behavioral information to identify the person. For effective results, it relies on specific data about unique biological traits.



	Characteristics	
Biometric Type	Physiological	Behavioral
Fingerprint	✓	
Face Recognition	✓	
DNA	✓	
Palm Print	✓	
Signature		✓
Gait		✓
Hand Geometry	✓	
Retina	✓	
Iris Recognition	✓	
Typing Rhythm		✓
Voice		✓

Figure 1.3: Biometric Characteristics

Widespread adoptions of biometrics have given rise to a new generation of authentication. However, there are also several drawbacks with monomodal biometric systems.

Fingerprint authentication is not possible for people who have had a limb or limbs amputated. Biometric systems can only operate when backed by huge databases. The cost of developing biometric authentication systems and operating their databases is considerably higher than the cost of currently used systems. [3]

Another issue with the single biometric system is that everyone cannot use it. Disabled people, people having congenital defects cannot use this system.

The another issue is that in the case of frauds, users can change passwords or can request new smart card but the biometric system features like finger print, iris, DNA, hand geometry, and so on cannot be changed by user. [4]

Limitations of Monomodal Biometric System:

•Non-universality

• Noise in sensed data

• Reliability of the sensor used

• Limited discriminability

• Lack of permanence

• Spoofing. [5]

III. RELATED WORK

To address the limitations of monomodal biometric system, the multimodal biometric system was proposed. To make the biometric system more efficient, a multimodal biometric system is preferred because there are some drawbacks with each of the feature of biometric system.

Consider the example that user can't give proper finger prints due to cut, dryness of finger, etc. In case of noisy surrounding, voice can't be preferred as suitable biometric indicator.

In multimodal biometric systems, different biometric sources of evidence are used to overcome the limitations of monomodal systems.

Multimodal biometric systems may be: -

- Multi-sensor system for the same biometric (e.g. optical, capacitive, based on chip fingerprint sensor etc.)

- Multi-method system – this uses multiple methods to compare the test arrays with the references (e.g. multiple fingerprint matchers based on minutiae or filtering, multiple face matchers like PCA and LDA).

- Multi-characteristic system – (e.g., it uses the fingerprints from several fingers, left and right iris images).

- Multi-capture/instance system – it acquires samples from the same biometric characteristic (e.g. the same fingerprint will be sampled for more than one time).

- Multi-verifier system – it uses more than one biometric verifier (fingerprint, face, hand, voice etc. [6]

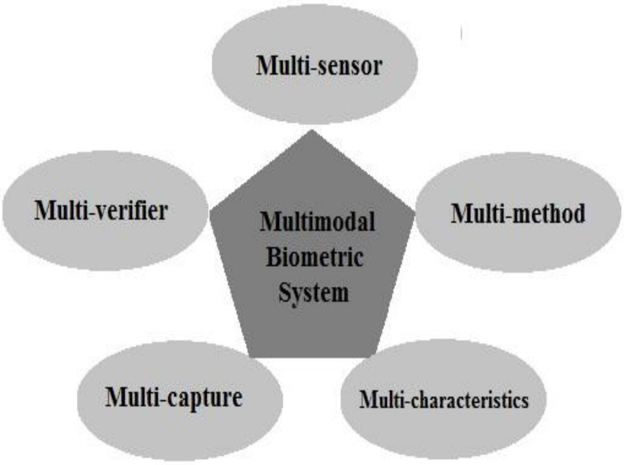


Figure 1.4: Multimodal biometric system

Multimodal biometric systems utilize more than one physiological or behavioral characteristic for identification or verification.

In many situations, the user might find one form of biometric identification is not good enough for authentication. This can be the case with fingerprints, where at least 10% of the population have worn, cut or unrecognizable prints. Multimodal biometric technology uses more then one biometric identifier to compare the identity of the person. Therefore in the case of a system using say three technologies i.e. iris, fingerprints and hand geometry. If one of the

technologies is unable to identify, the system can still use the other two to accurately identify the person. Since 1998, multimodal technologies have been in use commercially. [7]
The multimodal biometric verification systems are more reliable than monomodal biometric system. Multimodal biometric system performs person recognition based on a multiple source of biometric information. The following block diagram illustrates the general process of multimodal biometric system:

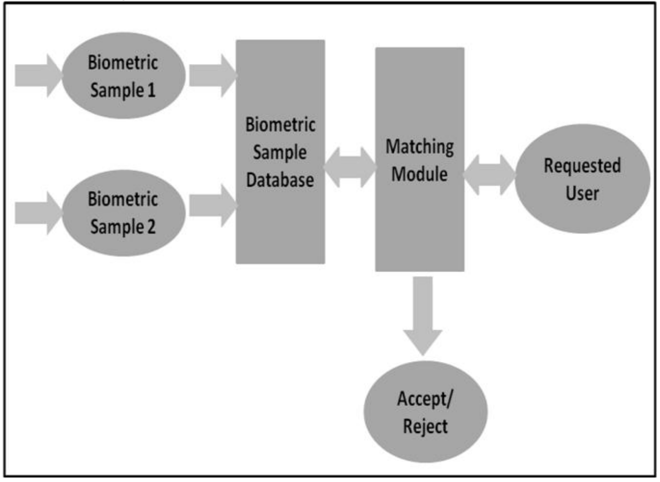
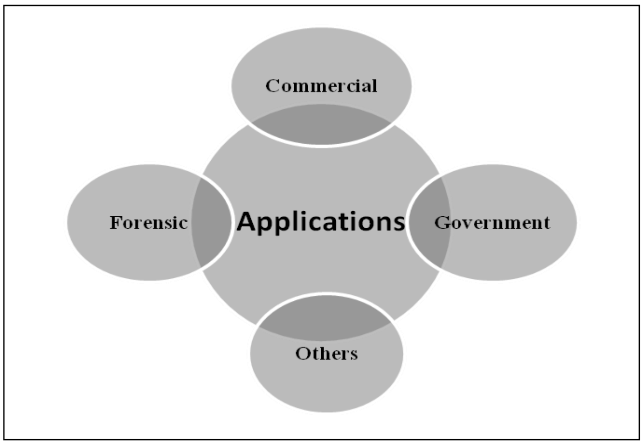


Figure 1.5: Working Module

Some work on the multimodal biometric system has already been proposed.
The NIST report recommends a system employing multiple biometrics in a layered approach. [8] The reason to combine different modalities is to improve recognition rate.
In literature it has been discussed a multimodal biometric system using face and fingerprint and proposed various levels of combinations of the fusion. [9]

All the proposed suited fusion of biometric features has some drawbacks. The improper fingerprint impression, noise or throat defect in voice recognition, cluttered background in face recognition, varying speed of keystrokes, etc results inefficient identification and authentication of justified user.



IV. APPLICATIONS

The **applications** of biometrics can be divided into the following three main groups:

Commercial applications: such as computer network login, electronic data security, ecommerce, Internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, and so on.

Government applications: such as national ID card, correctional facility, driver's license, social security, welfare-disbursement, border control, passport control, etc.

Figure 1.6: Application area of biometrics

Forensic applications: such as corpse identification, criminal
investigation, terrorist, identification, parenthood determination, missing children, etc. [10]
The other application of multi-biometric system includes door lock security systems that are based on finger print and iris recognition, for attendance purpose in the collages as well as multi-national companies. The use of multimodal biometric system eliminates the risk of losing keys, hijacking of passwords, stealing of smart cards, etc.
Therefore, these systems may provide high secured and authentication access. [11]

V. CONCLUSION

In this paper, we illustrated the study of the need of multimodal biometric system over the traditional schemes and monomodal biometric systems in order to make the efficient authentication in the favour of security. The multimodal biometric systems can ensure the working of large organisations more securely in coming era. These systems can be effectively use at the server side also along with the client side. With rapid growth of technology, its security must be grown with it. And, for the security, authentication is first and foremost necessity. It can be provided by the "multimodal biometric systems."

REFERENCES

[1] 'Introduction of biometric authentication' available at "http://www.tns.com/biometrics.asp" accessed on 26/12/13.

[2] 'Biometric industry revenues' available at "https://www.acuity-mi.com/FOB_Report.php&h=309&w=433&tbnid=ognnN9jaFBml_M:&zoom=1&docid=3QMDo9W_qiWgOM&hl=en&ei=61AxVPb5LpOiugS_5oLQAw&tbm=isch" accessed on 23/01/2014.

[3] 'Disadvantages of biometric authentication' available at "http://www.ehow.com/info_8233313_disadvantages-biometric-authentication.html" accessed on 05/01/14.

[4] 'Drawbacks of biometric authentication' available at "https://www.google.co.in/?gws_rd=cr&ei=--njUuLVGYGTrgfM3YH4AQ#q=drawbacks%20of%20biometric%20authentication" accessed on 09/01/14.

[5] 'Multimodal biometric system' available at "http://ftp.rta.nato.int/public/PubFullText/RTO/MP/RTO-MP-IST-044/MP-IST-044-16-PPT.pdf" accessed on 11/01/2014.

[6] 'Multimodal biometric system' available at "http://users.utcluj.ro/~atn/papers/ATN_3_2008_8.pdf" accessed on 15/01/14.

[7] 'All combination in multimodal biometric system' "http://www.biometricnewsportal.com/multimodal-biometrics.asp"accessed on 15/01/14

[8] 'Multimodal biometric system' available at "http://arxiv.org/ftp/arxiv/papers/1011/1011.6220.pdf" accessed on 16/01/14.

[9] 'Multimodal biometric system' available at http://arxiv.org/ftp/arxiv/papers/1011/1011.6220.pdf accessed on 20/01/14.

[10] 'Application of biometric system' available at "http://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0406.pdf" accessed on 25/01/14.

[11] 'Application of multimodal biometric system' available at "http://arxiv.org/abs/1210.2971" accessed on 25/01/14.