COMPARATIVE ANALYSIS OF MULTIMODAL BIOMETRIC SYSTEM

[1]Gagandeep Kaur , [2]Samandeep Singh , [3]Navneet kaur
[1]Research Scholar, [2] Assistant Professor, [3]Assistant Professor
[1]Department of Computer Science, G.I.M.E.T , Amritsar, Punjab, India
[2]Department Computer Science, G.I.M.E.T , Amritsar, Punjab, India
[3]Department of Computer Science, G.I.M.E.T , Amritsar, Punjab, India
[1]gillgagan563@gmail.com, [2]saman.singh@gmail.com, [3] navneetkaur299@gmail.com

ABSTRACT

Networked environment provides legion of resources but also causing uncertainties due to crimes like computer hacking, illegal access of ATM and cell phone, security is the prime requirement. To overcome this barrier, biometric techniques are used as authentication technique to prevent unauthorized access. Biometric system kind of a method to scrutinize exclusive physical or behavioural traits to determine individual's identity. In this study ,providing the review comparison multimodal biometric system which provide additional accuracy as compared to unimodal biometric systems. The system of concern takes the input either from single or multiple sources and verifies it against the historical information stored within the dataset. This technology uses more than one biometric identifier to compare the identity of the individual. Thus, the system uses three technologies i.e. face, mimic along voice and if any one of this technology is not able to identify, the system scan still use the other two to get accurate results. The main objective of this paper is to use fusion of these biometric techniques for performance enhancement, security , minimize the system error rates to achieve better results.

Keywords :- Biometric, Multimodal Biometric, Security, Sensors.

INTRODUCTION

The word “biometric” is taken from the Greek words “bios” and “metron” which means “life measurement”. So, the word [1] Biometric is referred as an automatic identification of individual’s identity from their physiological or behavioural features to verify his/her. So, Biometric is used to identify that “who you are”. Examples of biometrics include fingerprint, hand geometry, face and iris recognition etc. These samples are usually very accurate, and are the most common amongst biometric readers. But sometimes samples like voice and signature are less accurate but still useful, behavioural characteristics, is based upon the measurement of a person’s actions.[2] Biometrics is generally more secure and safer than keys or passwords that we use to secure data. Biometric system takes the input from the user through the sensors. Sensors grabs the related information by heat map and collect it within the buffer. The dataset information about the minutiae related to fingerprint is already present within the training set. Extracted information is matched against the collected information within the buffer. Region of interest is also analysed for similarity. In case match occurs, person is authenticated but in case match does not occur unauthorised access is determined and blocked. General structure of biometric system consisting of sensors , feature extractor and templates is shown in fig1.

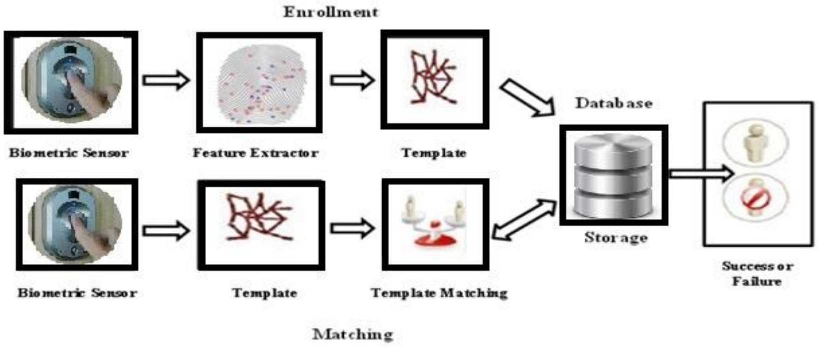

Fig 1: Biometric system

Components of Biometric System:

- Sensors collect the data from humans and convert it into digital format.
- Signal processing algorithm performs quality control activities and start developing the biometric template from those samples.
- Data storage keeps information from the sensors with which the new biometric template will be compared to.
- Matching algorithm then compares the new biometric template to one or more templates in stored data.
- Decision process makes a system level decision from the matching component to create result.

Problems in Biometric System

Biometric system receive signal from only one biometric system known as unimodal. But, each biometric has its own pros and cons so it is not difficult to steal a biometric, create a copy and use the fake trait to attack on biometric systems. This a serious issue because to enhance the network security people these days are using biometric. Furthermore, vulnerable [5] attacks can be put to break the security of networks like spoof attack, replay attack, substitution attack, Trojan horse attack and transmission attack etc. Different technologies have been applied to defeat these attacks like biometrics, but it is not secret so it cannot be protected like passwords. Without any awareness people leave their biometrics everywhere so that information can easily be captured, copied or forged. Another challenge in front of a biometric system is the speed i.e. the system must make an accurate decision in real time.

Biometrics contains two types of recognition errors: false accepts rate (FAR) and the false reject rate (FRR). A False Accept rate occurs when an unmatched set of biometric data is accepted wrongly as a match by the system and False Reject rate occurs when a matching set of biometric data is wrongly rejected by the system. If you overcome one of these errors by changing the value of threshold, then other error rate increases automatically. Therefore, a balance should be present, with in a decision threshold that can be specified to either minimize the risk of FAR, or to minimize the risk of FRR. While using biometrics some problems come in front of us which are given below:

- Noise in sensed data.
- Intra-class variation in the sample data.
- Inter-class similarity in the sample data.
- Spoof attacks.
- Distinctive Ability.

To overcome these problems of [8] unimodal biometrics multimodal biometrics system was introduced.

Multimodal biometrics

Multimodal biometrics is emerging choice to secure authentication of user. Multimodal biometric refers to merging of two or more biometric modalities for improving the performance of the individual systems, recognition rate and reliability. Generally, the term multimodal indicates the use of more than one biometric aspect (modality, sensor, instance and/or algorithm) and some time to combine these and make a specified biometric verification/identification decision. [7]

The main objective of multimodal is to reduce the following:

- False Accept Rate (FAR)
- False Reject Rate (FRR)
- Failure to Enroll Rate (FTE)
- Susceptibility to Artifacts or Mimics

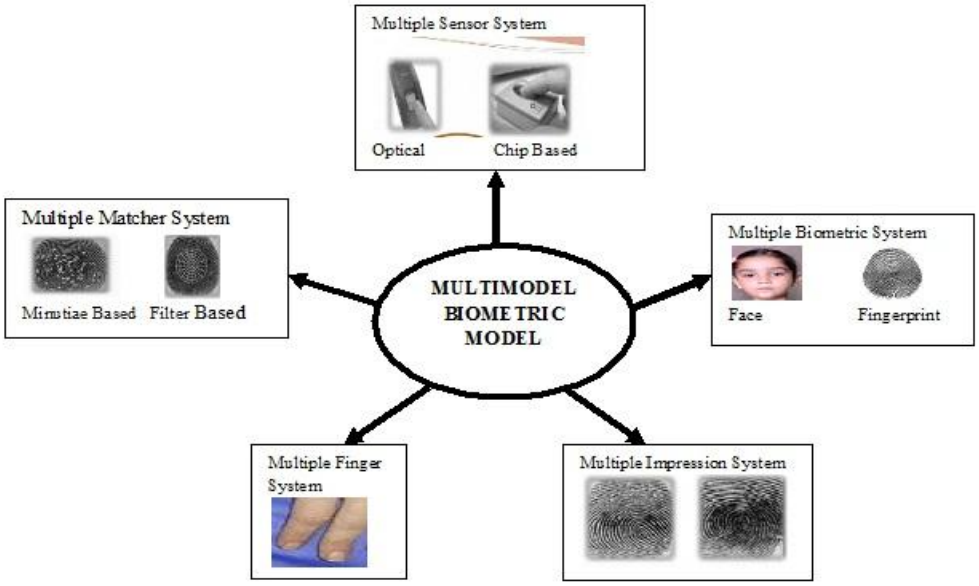

Fig2: Types of multimodal system

Multimodal are more vital to fraudulent technologies, because it is so difficult to forge multiple biometric characteristics than to forge a single biometric characteristic thus provide higher accuracy rate and higher protection from spoofing. [16] Multimodal system also provides the protection against the spoofing. Spoofing causes the identities of the users to be hacked. With biometric system identities are unified and scanning can detect the existence of unauthorised access. Furthermore, depending on the traits, [15] sensors and feature sets many different types of multimodal systems are given below:

- **Single biometric trait, multiple sensors**: The same biometric characteristics are recorded using multiple sensors. The data taken from various sensors are combined at the feature level or matcher score level to improve the performance of the system.
- **Multiple biometrics:** Multiple biometric traits combine any of two or more like fingerprints, voice, iris and face. Different sensors are used for capturing the sample of each biometric characteristic. A commercial product Bio ID uses voice, lip motion and face of a user to verify identity of the user.
- **Multiple units, single biometric traits:** Two or more than two fingers of a single user can be used as a [9] biometric trait and it’s an inexpensive way of improving system performance, as it doesn’t require multiple sensors or incorporating additional feature extraction or matching modules.
- **Multiple snapshots of single biometric:** In this more than one instance of the same biometric is used for the recognition like multiple impressions of the same finger or multiple samples of the voice are captured for authentication.
- **Multiple matching algorithms for the same biometric**: To extract the features and matching of the biometric characteristic different methods can be applied.

Modes of operation

A multimodal biometric system can work in three different modes which are given below:

- **Serial mode:** In the serial mode the output of one biometric characteristic is used to reduce the number of possible identities before the next characteristic is used for identification. So, because of this multiple source of information is not collected simultaneously.
- **Parallel mode:** In this mode the information from multiple characteristics is taken together to perform recognition.
- **Hierarchical mode:** In this mode individual classifiers are combined in a tree like structure and this mode is well suited where we have large number of classifiers.

RELATED WORK

Aggarwal & Verma, 2016 suggested multimodal biometric systems provides more accuracy as compared to unimodal biometric systems. Multimodal biometric systems capture input from single or multiple sensors and measures two or more different modalities of biometric characteristics. Multimodal biometric technology uses more than one biometric identifier to compare the identity of the individual person. The system can use three technologies i.e. face, mimic and voice. If one of the technologies is not able to give identity of the user, the system can still use another two to get accurate identify against user. This paper provides the study of various techniques used for performance enhancement, security and level of fusion in multimodal biometric along with various challenges in multimodal biometric. [3]

Ahuja & Chabbra, n.d. discussed a biometric technology was used to analyse human characteristics for the purpose of security. The fingerprint, hand, eye, face and voice are the most common physical biometrics patterns analyzed for security purposes. The main advantage of using biometrics is to verify a person's identity over using passwords or token. However, from the researches of past years it is concluded that the biometric technologies can be defeated with low–tech and cheap materials. So it gives a new challenge to people and encouraged them to use multimodal biometrics as a means to enhance network security. In this paper we have discussed multimodal biometrics to increase the security level and with the fusion of multiple biometrics we can minimize the system error rates.[4]

Gopal & Selvakumar, 2016 the development of recent technologies, a biometrics system has been the important affordable and more reliable system to provide network security to peoples. Biometric identification system is the automatic recognition of individual person based on their characteristics like voice, eyes retina, figure prints etc. Biometrics system is categorised in two broad areas namely unimodal biometric system and multimodal biometric system. In unimodal system only single biometric system is used as sample so it has some disadvantage due to its lack of non-universality and unacceptable error rate. But on the other hand multimodal is the better system for its two or three level of identification and verification. In this paper multimodal biometrics system characteristics are studied with its various biometrics traits and the comparison of different modalities is also processed to choose the best authentication mechanism. This paper performs multi biometrics system with its processing.[6]

Author Mane, n.d. proposed a biometric system to meet stringent performance requires high security applications. The fusion of multiple biometrics i.e. gathering of biometrics like figure prints, voice, iris helps in minimizing the system error rates. Fusion of multiple images causes difficulty for hackers to decrypt the information. More sophisticated methods are combined to scores from separate classifiers for each modality. This paper gives an overview of multimodal biometrics, the main research areas, challenges in the progress of multimodal biometrics and its applications to develop the security system for high security areas.[8]

Solution Proposed by Noorjahan Khatoon, 2013 involving biometric system combines the unique physical or behavioural traits to determine a person's identity. It is a pattern recognition system which includes feature extraction and comparison among these features against the template set in a database. Multimodal biometric systems gather more than one trait for person recognition. These systems offer more accurate results in comparison to the unimodal systems so they are more popular, even though they are complex than unimodal system. In this paper an overview of the different multimodal biometrics system and the fusion techniques associated with them are explained. Discussion part also include design issues, challenges and advantage of such systems over unimodal biometric system[10].

In proposed Panchal, 2013 paper security becomes a big requirement due to increase in crimes like computer hacking, illegal access of ATM & cell phone but security breaches in govt. and private buildings. These flaws become the advantage for criminals to break the security systems. For this biometric recognition system are used for personal identification of every individual on the network. Biometrics of individual can`t be broken or hacked easily as compares to password, personal identification number, smart card etc. As advancement Multimodal system combines any number of independent biometrics and overcome some of the cons of unimodal biometrics. With the fusion of multiple biometrics system error rates can be minimized. This paper present overview of multimodal biometrics, challenges faced by multimodal biometric system, applications to develop the security system for high security areas and application of biometric systems and their advantage over unimodal biometric system. [12]

Author Shaikh, 2016 this age of digital impersonation, to prevent unauthorized access biometric techniques are being used increasingly for authentication technique. The authentication through biometrics is done using individual's biological identities, and offer true proof of identity. The issues related to biometrics include security, forensics and remote managing. In this paper, unimodal, multimodal and fusion techniques are reviewed for authentication and extensive research has been conducted in this area with different techniques.[13,14]

COMPARISON TABLE

Author	Title	Method	Advantages	Disadvantages
Ahuja et. al.[2]	A survey of multimodal biometrics	Fingerprint, hand, eyes, voice analyze	Increase the security level using multimodal biometrics, System error rate minimizes	Biometrics is vulnerable to attacks such as transmission, replay and spoofing.
Aggarwal et. al.[3]	Multimodal Biometric Systems– A Survey	Face, mimic and voice are used as biometric	More accuracy as compared to unimodal system	Improvement in matching performance is required
Gopal et. al.[6]	Multimodal Biometric Identification System An Overview	Comparison of different modalities	Improve matching performance of different samples	Lack of non universality and unacceptable error rate.
Mane et. al.[9]	Review of Multimodal Biometrics: Applications, challenges	Fusion method	Integration of multiple sensors , optimal data is deliver	For more accuracy multimodal is used

	and Research Areas			
Noorjahan et. al.[11]	Multimodal Biometrics: A Review	Fingerprint, voice, DNA , Face, Iris used for biometrics	Combines various modalities for identification and verification	Complex than unimodal
Panchal et. al.[12]	Multimodal Biometric System	Fusion of multiple biometrics	Minimizes error rate	Provides unmanned access control
Shaikh et. al.[13]	Review of Hand Feature of Unimodal and Multimodal Biometric System	Fusion techniques and review the different palm print & finger print techniques	Increase accuracy and reliability	False error rate can occur

CONCLUSION AND FUTURE WORK

Biometric technology adds a new layer of security by providing secure identification and authentication. This technology flourishing very rapidly, but biometric authentication doesn’t give perfect results. To overcome this issues biometric authentication method has been reviewed from above discussion that there are two types of biometric authentication technique i.e. unimodal & multimodal. To increase accuracy and the reliability of biometric authentication, multimodal biometric can be used. This paper also reviews various security broken attacks, various modes of data transfer and errors like FAR, FRR, FTE that comes during data capturing. In future to enhance the multimodal system we can merge more than one or two biometric samples to get better response.

REFERENCES

[1] This, P. (n.d.). Chapter 5 Genetic Algorithm (Ga) for Facial Biometric Security System (Bss), 79–109.

[2] Hotta, K., Member, S., & Mishima, T. (2001). Scale Invariant Face Detection and Classification Method Using Shift Invariant Features Extracted from Log-Polar. IEEE Transactions on Information Systems, E84-D(7), 867–878.

[3] Aggarwal, A.,&Verma, M.K.(2016).Multimodal Biometric Systems – A Survey. International Journal of Advanced Research in Computer Science and Software Engineering, 6(3), 437–441.

[4] Ahuja, M. S., & Chabbra, S. (n.d.). A Survey of Multimodal Biometrics. International Journal of Computer Science and Its Applications, 157–160.

[5] Anwar, R. W., Bakhtiari, M., Zainal, A., Abdullah, A. H., Qureshi, K. N., Computing, F., & Bahru, J. (2014). Security Issues and Attacks in Wireless Sensor Network. World Applied Sciences Journal, 30(10), 1224–1227. http://doi.org/10.5829/idosi.wasj.2014.30.10.334

[6] Gopal, N., & Selvakumar, R. K. (2016). Multimodal Biometric Identification System - An Overview. International Journal of Engineering Trends and Technology (IJETT), 33(7), 351–355.

[7] Jabbar, M. A., Deekshatulu, B. L., & Chandra, P. (2013). Classification of Heart Disease Using K- Nearest Neighbor and Genetic Algorithm. Procedia Technology, 10, 85–94. http://doi.org/10.1016/j.protcy.2013.12.340

[8] Karaboga, D., Aslan, S., & Ò, Ü. Ñ. Ò. Ö. Ò. Ü. Ñ. Ü. Ü. Ñ. (n.d.). A New Emigrant Creation Strategy for Parallel Artifissscial Bee Colony Algorithm ØÒ ××, 689–694.

[9] Mane, P. V. M. (n.d.). Review of Multimodal Biometrics : Applications , challenges and Research Areas, 3(5), 90–95.

[10] National Science and Technology Council Subcommittee on Biometrics. (2006). Face Recognition.

[11] Noorjahan Khatoon, M. K. G. (2013). Multimodal Biometrics: A Review. IRACST - International Journal of Computer Science and Information Technology & Security(IJCSITS), ISSN: 2249-9555 Vol. 3, No.3, June 2013, 3(3), 230–236.

[12] Panchal, T. (2013). Multimodal Biometric System. International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), 1360–1363.

[13] Shaikh, J. (2016). Review of Hand Feature of Unimodal and Multimodal Biometric System. International Journal of Computer Applications, 133(5), 19–24[

14] Meenakshi sharma and Dr. Himanshu Aggarwal,"EHR Adoption in India: Potential and the Challenges", Indian Journal of Science and Technology,2016.

[15] Tashtarian, F., Yaghmaee Moghaddam, M. H., Sohraby, K., & Effati, S. (2015). On Maximizing the Lifetime of Wireless Sensor Networks in Event-Driven Applications With Mobile Sinks. IEEE Transactions on Vehicular Technology, 64(7), 3177–3189. http://doi.org/10.1109/TVT.2014.2354338

[16] Yang, X., & Hossein Gandomi, A. (2012). Bat algorithm: a novel approach for global engineering optimization. Engineering Computations, 29(5), 464–483. http://doi.org/10.1108/02644401211235834