A REVIEW ON MULTIMODAL BIOMETRIC SYSTEMS

[1]A.Kavitha
Assistant Professor of Computer Science,
Aditanar College of Arts and Science, Tiruchendur.

Abstract: In the digital era of information technology, there is a need to implement authentication and authorization techniques for security of resources. Nowadays Biometric authentication provides reliable, robust and user-friendly authentication with a high level of accuracy. We have seen that the growth of biometric technology throughout the world for many reasons but mostly due to the fact that personal identification is considered more and more important. Multimodal biometric systems are very difficult to spoof as compared to unimodal systems. Even if one biometric modality could be spoofed, the individual can still be authenticated using the other biometric identifier. This paper provides an overview of multi modal biometric systems.
Keywords: authentication, security, biometrics, unimodal biometrics, multimodal biometrics, fusion

I. INTRODUCTION

In our day to day life, the identification of a person is very important task to access sensitive data. That's why we can use a new modern way to identify a person is biometric authentication. Biometric technology is based on the principle of measuring and examining the biological traits of individuals, extracting the unique features from this acquired data and then comparing it with the template set stored in the biometric templates database. The biometric modalities fall under two types- Physiological and Behavioral [1][2].

Physiological modalities are based on the direct measurement of parts of human body such as iris, retina, face, fingerprint etc., Behavioral modalities include voice, signature, keystroke etc.,

II. UNIMODAL AND MULTIMODAL BIOMETRIC SYSTEMS

Biometric identification systems which use a single biometric trait of the individual for identification and verification are called unimodal systems. Biometric identification systems which use or are capable of using a combination of two or more biometric modalities to identify an individual are called multimodal biometric systems [3].

In the real world, unimodal is used in Biometric systems applications. They depend on the evidence of a one source of information for authentication. These systems have to deal with variety of problems such as Noise in the sensed data, Intra-class variation, Inter-class similarities, Non-Universality and Spoof Attack. Not all but some of the limitations of the unimodal can be overcome by including multiple source of information for identification. These types of system are called as Multimodal Biometric Systems. These systems are more reliable due to the presence of multiple, independent biometrics. Some common multimodal biometrics are face and fingerprint, face and iris, iris and fingerprint etc.

III. MODULES OF MULTI MODAL BIOMETRIC SYSTEM

A multimodal biometric system consists of the following four modules

- Sensor Modules
- Feature Extraction Modules
- Matching Module
- Decision-Making Module

In multimodal biometric systems fusion is achieved by running two or more biometric traits against two or more different algorithms which is then used to arrive at a decision.

IV. TYPES OF MULTIMODAL BIOMETRIC SYSTEMS

The various types of multimodal biometric systems are

Multi-algorithmic biometric system:

This type of system takes a single biometric sample from a single sensor and then processes it using two or more different algorithms.

Multi-instance biometric system:

This type of system use one or more sensors to capture samples of two or more different samples of the same biometric trait. For example a system capturing images of multiple fingers.

Multi-sensorial biometric system:

This type of system use two or more different sensors to capture the same instance of a biometric trait. These captured samples are then processed using a single algorithm or a combination of algorithms [4].

V. FUSION IN MULTIMODAL BIOMETRIC SYSTEMS

We use more than one biometric modality in multimodal biometric systems and hence we have more than one decision channels. Thus arises the need to design a mechanism which can combine the classification outcome from each biometric channel and this mechanism is known as biometric fusion. This fusion combines the measurements from different biometric attributes to enhance the strengths and decrease the weaknesses of the individual measurements. Fusion can be used to address a number of issues faced in implementation of biometric systems such as accuracy, efficiency, robustness, applicability and universality. There

are various levels of fusing the biometric traits which can be used to increase robustness of the multimodal biometric system. They are sensor level fusion, feature level fusion, matching score level fusion and decision level fusion.

Sensor level fusion:

In sensor level fusion, we fuse the biometric traits coming from different sensors such as fingerprint scanner, iris scanner, video camera etc. to form a merged biometric trait and process.

Feature level fusion:

In feature level fusion, signals coming from different biometric channels are first processed after which the feature vectors are extracted separately from each biometric trait. The feature vectors are then combined to form a composite feature vector using a specific fusion algorithm and then used for further classification. In feature level fusion, some reduction techniques need to be used in order to select only the useful features.

Features contain richer information of biometric traits as compared to matching score or decision of matcher and thus fusion at the feature level provides better recognition results. It has also been observed that feature level fusion provides more accuracy when the features of different biometric modalities are compatible with each other.

Matching score level fusion:

In this fusion level, the feature vectors are processed separately rather than combining them. Then an individual matching score is found and based on the accuracy of each biometric channel, we then fuse the matching level to find a composite matching score which will be used for classification. We can use various techniques such as logistic regression, highest rank, Bayes rule, mean fusion etc. to combine match scores. In addition to this, another important aspect of this fusion is the normalization of scores acquired from different modalities. We can use techniques such as Min-max, z-score etc. to achieve normalization of the match scores. Matching score level fusion has lesser complexity than the other fusion levels and hence it is widely used.

Decision level fusion:

In decision level fusion, each biometric trait is first pre-classified separately. The individual biometric trait is first captured and then features are extracted from the captured trait. The traits are classified as either accept or reject based on these extracted features. The final classification is obtained by combining the outputs of different modalities [4][5][6][7][8][9].

VI. CONCLUSION

In this paper we reviewed the multimodal biometric systems. Our world has been thoroughly transformed by digital technology. An accurate personal authentication is very important for the operation of our electronically interconnected information society. Unimodal biometrics has several problems. On account of the limitations raised by the unimodal biometric system many users resorted to multimodal biometric system in order to provide maximum level of accurate authentication. Effective utilization of the advantages of multiple biometric traits is applied to enhance the performance in many aspects including accuracy, noise resistance, and universality, spoof attacks, and reduce performance degradation in huge database applications. Nowadays, new algorithms and applications of multi-modal biometrics are emerging tremendously. We have discussed the features of both unimodal and multimodal biometric systems. We see that multimodal biometric systems are more robust, reliable and accurate as compared to the unimodal systems. Multimodal systems overcome the various limitations of unimodal systems and hence are suitable to many industries such as healthcare, civil id and financial industries.

REFERENCES

[1] Sushma Jaiswal, Dr.Sarita Singh Bhadauria, Dr.Rakesh Singh Jadon, Journal of Global Research in Computer Science, Volume 2 , No.10, October 2011, Biometric : Case Study

[2] Information security An Overview, PHI 2004. pp. 117

[3]https://WWW.bayometric.com/ unimodal-vs-multimodal

[4] Waleed Dahea, HS Fadewar, International Journal of Research in Advanced Engineering and Technology , Volume 4; Issue 1; January 2018; Page No. 25-31, Multimodal biometric system: A review

[5]https://www.scribd.com/document/350486967/A-Review-on-Unimodal-and-Multi modal-Biometric-Systems

[6]Kunal Kumar, Mohammed Farik, International Journal Of Scientific &Technology Research Volume 5 , Issue 12, December 2016, A Review Of Multimodal Biometric Authentication Systems

[7]https://docplayer.net/15735225-A-comparative-study-on-atm-security-with-multimodal- biometric-system.html

[8]https://www.tutorialspoint.com/ biometrics/multimodal_biometric_systems.htm

[9]https://www.semanticscholar.org/paper/ A-Review-Of-Multimodal-Biometric-Authentication- Kumar Farik/