IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 12, December 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

Multimodal Biometric System Advantages over Unimodal Biometric System Authentication Technology

Shital Baghel[1], Thaneshwar Kumar Sahu[2], Dr.Kshitiz Varma[3]

[1]Assistant Professor, [2]Assistant Professor, [3]Project Officer

[1]Department of Biomedical Engineering and Bioinformatics
Chhattisgarh Swami Vivekanand Technical University,Bhilai
shital.baghel@gmail.com
[2]Department of Biomedical Engineering and Bioinformatics
Chhattisgarh Swami Vivekanand Technical University,Bhilai
thaneshwar.sahu@gmail.com
[3]TEQIP CELL, Chhattisgarh Swami Vivekanand Technical University,Bhilai
kshcsvtu@gmail.com

ABSTRACT

In daily life now a days authentication is needed everywhere. Humans do this verification by their eyes, touch, nose, etc. Computers uses programming algorithms or codings using its database to authenticate and verify. Whenever, wherever, whatever we do authentication and verification is needed. Biometric system is a unique and popular method of security design. It is a system which uses human features for security purposes like face recognition, finger print, gait, iris identification etc. This study presents advantages of multimodal biometric system over unimodal biometric system in terms of accuracy. Multimodal biometric system uses more than one feature for better accuracy as compare to unimodal biometric system which uses only single feature for verification.

KEYWORDS: Biometric, Unimodal biometric system, Multimodal biometric system, Face recognition, Fingerprint recognition.

1. INTRODUCTION

The number of activities which are related to the Internet has increased. This is the age of universal electronic connectivity i.e., the electronic world with its applications like e-banking, e-commerce, e-government, virtual shops, e-mail, etc. There are obstacles and some problems related to it like unauthorized access, hackers, viruses, computer theft, etc, which effect the productivity and prosperity of individual or group. Thus, security became necessary as well as important. The solution for this problem is Authentication meaning the verification of the message and of the user [1]. Therefore in complex society,necessity of personal identification in the e-world is increasing, and the authentication of the user is a challenge that must stop the fraud in advanced technologies. Gait , face, voice characteristics, etc had been used by humans for thousands of years to identify and recognize each other. The term biometrics is derived from the Greek words biomeaning “life” and metrics meaning “to measure”[2]. Any two persons should be sufficiently different in terms of the characteristic, in clear term ‘Distinctiveness’. For our use, biometrics refers to technologies for measuring and analysing a person's physiological or behavioural characteristics. These characteristics are unique to individuals hence can be used to verify or identify a person. Biometrics refers to the identification or verification of a person based on his/her physiological and/or behavioural characteristics. Several verification/identification based biometrics have evolved based on various unique aspects of human body, ease of acquiring the biometric, public acceptance and the degree of security required. This paper presents an overview of

various biometrics in use/proposed and their applicability to different activities.

Usually a classification of the biometric features is made as physiological (fingerprint, face shape, iris, retina etc.) and behavioral (voice, gait, writing style etc.). In practice, all biometric verifiers may be considered combinations of physiological and behavioral characteristics due to the interaction mode between the user and the system, which puts its mark over the characteristic. Any physiological or behavioral feature may be used as a biometric verifier as long as it satisfies the following requirements [3]:

• Universality – every person must own this characteristic
• Distinctiveness – two persons possessing the same characteristic do not exist.
• Permanence – the characteristic must be invariant for a time period as long as possible;
• Collectablility – indicates the fact that biometric may be quantitatively measured;

For practical systems, there are some additional requirements that must be fulfilled such as [3]:

• Performance – which refers to the accuracy of the tangible recognition, speed, robustness, as well as the prerequisites for touching a certain level of performance.
• Acceptability – indicates the degree in which the given biometric characteristic is accepted by the users.
• Resistance to circumvention – indicates the facility through which a system can avoid fraud.

2. HOW BIOMETRIC SYSTEM WORKS

In a, biometric systems a set of specific vectors are compared with a set of models from a database. It is a recognition systems which captures biometric features from a person based on a model and extracts vectors. There are four important elements in a common biometric system as shown in Fig.1.

- First one is Sensor module which captures the biometric data of an individual. An example is a camera that captures face of a user.
-Second is Feature extraction module in which feature values are extracted from the acquired data. The position and orientation of minutiae points in a face image would be extracted in the feature extraction module of a image processing system.
- Third one is the Matching module in which comparison is done between the feature values with those in the template by generating a matching score. For example, in this module, the number of matching minutiae points between the query and the template will be computed and treated as a matching score.
- Last one is the Decision module in which the user's identity is established or a claimed identity is either accepted or rejected based on the matching score generated in the matching module.

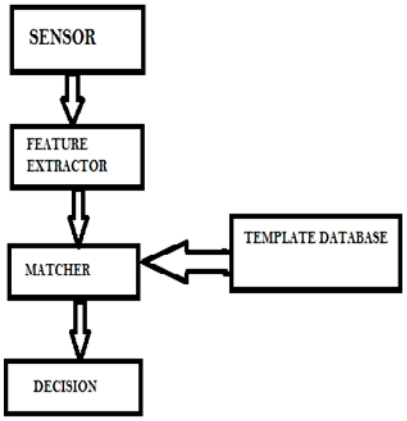

Fig 1 : A Biometric Authentication System

Depending on the application context, a biometric system can operate in the verification mode or in the identification one. First, biometric recognition implies the enrolment of the user in the system for creating the reference model in the database.

In verification mode, the assignation of the test model to the asserted person may be accepted or rejected; therefore only one comparison is made between the test model and the reference of the user that claims it. The verification problem may be presented consequently: being given a biometric vector XQ and the asserted identity I, establish if (I, XQ) belongs to the classes B1 or B2, where B1 indicates the fact that the demand is true, meaning that the vector XQ is authentic of the user I, and B2 indicates a false demand, that is the vector XQ belongs to an impostor. For taking the decision, the vector XQ is compared with XI, which represents the model of the user, I [3]. So,

(I, XQ)€ {B1 ,if S (XQ, XI) > p (1)
B2 otherwise,

Where S is a measure of the similarity between the biometric vectors XQ and XI, and p is a predefined threshold. S (XQ, XI) defines the similitude degree or the similarity score between the biometric vectors of the user and of the one who asserts the identity [4].

In identification mode, the system recognizes whom the tested biometric feature belongs to, meaning that it compares the test model with the reference models from the database (fig.1). From the formal point of view, the identification may be defined like this: being given a biometric vector XQ, determine the user's identity Ik, k Î{1,2…N+1} (to) whom the vector belongs to. The identities I1, I2….IN belong to the user's enrolment in the

system, and IN+1 indicates the situation of the rejection of the test vector.

$$XQ \in \{Ik, \text{if } \max\{S(XQ, XI\,k)\} > p,\ k=1,2,..N \quad (2)$$
$$IN+1 \text{ otherwise,}$$

Where XIk is the biometric model corresponding to the identity Ik and p is a predefined threshold [4]. In some application, a screening task is required to verify if some persons (suspects) are registered in the biometric database.

The features and the taxonomy of the biometric systems The global performance of a biometric system is appreciated taken into account different factors like: precision, speed and storage of the data, easiness of utilization and costs, factors that affect the system's efficiency. The architecture of the biometric recognition systems depends on the application. Any user, before he/she can be tested by the system, must be enlisted, meaning that he/she must pass through a stage where the biometric characteristics of that system are captured. The biometric recognition systems can operate in positive or negative mode. An application of positive recognition establishes if the person that claims his/her identity is indeed that person. The purpose of positive recognition is to prevent the situation when more users use the same identity. In this case, false acceptance favors fraud. The negative recognition proves that the user is not who he/she claims to be. The goal of negative identification is to prevent the situation when a person has more than one identity. For instance, the user X received certain facilities (rights in a system), but now he/she pretends to be someone else, the user Y, in order to profit by his/her rights too (double permission). The system will establish that "the user Y" is not who he/she claims to be. The traditional methods of authentication using passwords, PIN, keys can function for positive recognition, but the negative recognition can be realized only through biometric methods.

3. HOW MULTIMODAL BIOMETRIC SYSTEM WORKS

In a multimodal biometric system more than one feature of humans are first sensed by sensor and then its features are extracted and then it is matched by using database and then with the help of certain algorithm scores of matching from all of the features are added to get exact score and if this score becomes equal to or greater than the certain threshold level then the verification process becomes genuine and if score becomes less than the threshold then the result shows that it is an imposter or fraud. As shown in Fig.2 two traits i.e., face and finger is taken, first of all a sensor will sense face of object and then feature extractor unit will extract its feature and then its matched with the database, another sensor module will sense fingerprint trait and it will extract its feature and it will also be matched with the database and its score will be calculated. Then the scores from both the traits will be fused by certain algorithms and then it will give us final score. If this score is greater or equal to the threshold than the result will show us that the object is genuine, and if the score is less than the threshold than the result will show us that the object is fraud.Therfore we observe that in case of a single biometric feature there are chances of fraudrey but if we will fuse more than one feature then this chance get reduced. For example if a system is only based on fingerprint then very easily by means of certain techniques the fingerprint can be used by others for the verification, but if it get fused with face which have very different feature then the authentication and verification will be tough and imposter will fail so proper security can be achieved. The lack of universality of some characteristics (for instance, in the case of fingerprints, approximately 4% of people cannot enlist because of weak fingerprints, and this percent increases at 7% in the case of the iris),Noisy signals captured from the sensors due to the incorrect usage by the clients and due to the environmental conditions (humidity, dirt, dust etc.),the lack of the safety of the used sensors, the limitation of the discrimination of biometric systems due to a high in-class and low inter-class variability, the recognition performances of the systems are upper limited at a certain level, Unacceptable error rates for the unimodal biometric systems, the lack of permanence and variability in time of the biometric characteristics, the fraud possibility through voluntarily or involuntarily cloning (of) a biometric characteristic[5].

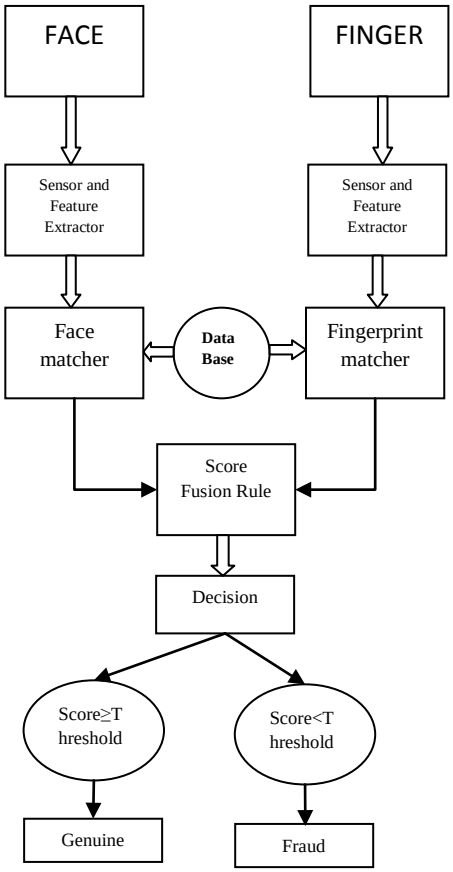

Fig 2 : A multimodal Biometric Authentication System

4. CONCLUSION

More security is better than less security, we can say that system based on biometric is not fully secure but we can improve security. In a unimodal biometric system it is affected by non-distinctiveness, noisy input, non universality and lack of invariant separation. Adding multiple traits can be useful to overcome disadvantages of unimodal biometric system. The score rate by fusion methods gives better accuracy, Chances of fraud becomes less, more than one sensor used gives less noisy input, Recognition performances gets increased, Variability in time issues gets reduced, voluntarily or involuntarily fraud through cloning gets reduce hence error rate gets reduced.

REFERENCES

[1] Eugen LUPU Petre G. POP.,(2008),"Multimodal Biometric System Overview", Technical University of Cluj-Napoca.
[2] A. Zahid., (2012), "Basic Structure of A Biometric System",Security Of Multimodal Biometric Systems Against Spoof Attacks, University Of Cagliari, Cagliari, Pp 12-13.
[3] Maltoni, D. Maio, A.K. Jain, S. Prabhakar Handbook of Fingerprint Recognition, Springer Verlag, NY, 2003.
[4] Arun Ross and Anil K. Jain, "Multimodal Biometrics: an overview", Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp.1221-1224, September 2004.
[5] Jain A., Mink A., Uludag U., Indovina M.,"Multimodal Biometric Authentication Methods: A COTS Approach", Proceedings of Workshop on Multimodal User Authentication, December, 2003

Authors

SHITAL BAGHEL received the Bachelors of Engineering degree in Electronics and Telecommunication Engineering from Chhatrapati Shivaji Institute of Technology,CSVTU, Bhilai, Chhattisgarh, India in 2009, and Masters of Technology in Electronics and Communication Engineering from Indian Institute Of Technology Kharagpur India in 2015.

THANESHWAR KUMAR SAHU received Bachelors of Engineering degree in Electronics and Telecommunication Engineering from Chhatrapati Shivaji Institute of Technology, Pt.R.S.U, Raipur, Chhattisgarh, India in 2006, and Masters of Technology in Instrumentation and Control Engineering from Bhilai Institute Of Technology Durg,C.G India in 2015.

Dr. Kshitiz Kumar Varma received Bachelors of Engineering degree in Electronics and Telecommunication Engineering from Rungta Institute of Technology, Pt.R.S.U, Raipur, Chhattisgarh, India in 2005, and Masters of Technolog,in VLSI from SSCET Bhilai, Phd in Electronics Engineering from CVRU BILASPUR ,C.G, India in 2016.