ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

# Survey on Multimodal Biometric System

Mrs. W. Ancy Breen[1], Praveen Kumar.D[2], Gothandan.G[3], Meganathan.D[4]
[1]Associate Professor, Veltech High-tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai, Tamil Nadu.
[2, 3, 4] UG Scholar, Veltech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai, Tamil Nadu.
ancybreen@velhightech.com[1] praveenkumarcse140695@gmail.com[2] gggothandan@gmail.com[3]
meganathanmac@gmail.com[4]

## *Abstract*

*This report focuses on offline signature verification, characterized by the usage of static (scanned) pictures of signatures, where the objective is to discriminate if a given signature is real (produced by the claimed individual), or a forgery (produced by an impostor). In this paper, a new approach for feature selection is projected for writer-independent (WI) off-line SV. First, one or more pre-existing techniques are utilized to extract options at totally different scales. The signature of a person is a crucial biometric attribute of a person's being which might be wont to demonstrate human identity. The proposed feature set describes the form of a signature in terms of abstraction distribution of black components around a candidate pixel (on the signature). It also provides a live of texture through the correlation among signature components in the neighborhood of that candidate pixel. . To reduce the spatial property of facial image and improve the popularity rate, a face recognition system based on curve let rework and Least sq. Support Vector Machine (LS-SVM) has been developed during this paper, which uses curve let rework to extract options from facial pictures initial, and then uses LS-SVM to classify facial images supported options.*

***Index Terms-*** *Signature verification, Write-independent, Biometrics*

## 1. INTRODUCTION

Biometrics technology is used today in an exceedingly wide selection of security applications. The aim of such systems is to recognize someone supported physiological or activity traits. In the first case, the recognition is predicated on measurements of biological traits, such as the fingerprint, face, iris, etc. The latter case is concerned with activity traits like voice and therefore the written signature [1].

Biometric systems can perform 2 tasks: verification and identification. In the first case, a user of the system claims to be a particular person, and provides the biometric sample. The role of the verification system is to check if the user is indeed United Nations agency he or she claims to be. In the identification case, a user of the system provides a biometric sample, and the objective is to spot, among all the people listed in the system, who the person is.

The handwritten signature is a significantly vital sort of biometric attribute, mainly due to its omnipresent use to verify a person's identity in legal, financial and administrative areas. One of the explanations for its widespread use is that the method to gather handwritten signatures is non-invasive, and people area unit acquainted with the employment of signatures in their way of life [2].

Biometric systems provide 3 recognition functions: identification, screening, and verification. Identification seeks to establish a person's identity by matching his biometric sample against all user templates within the system database. Screening discreetly determines whether the bio- metric sample of associate individual whose enrollment procedure isn't usually well-defined matches any of the system's watch list of identities. Forgeries are sometimes divided into 3 types—random, simple, and simulated. A random forgery occurs once the forger will not understand each the writer's name and therefore the signature's morphology. It can additionally happen once a real signature conferred to the system is illegal to a different user. When the forger is aware of the writer's name however not the signature's morphology, the forger can solely manufacture a straightforward forgery employing a form of writing of his feeling.

Within the field of human classification, the procedure of biometrics is nascent as a result of of its distinctive properties like hand pure mathematics, iris scan, fingerprints or DNA. The use of signatures has been one amongst the more opportune strategies for the popularity and verification of people in general. A signature may be termed a activity biometric, as it can modify reckoning on several necessities such as: frame of mind, exhaustion, etc. The exigent aspects of automated signature recognition and verification are, for a long time, a true impetus for

researchers. Research into signature verification has been energetically pursued for a range of years and remains being explored (especially within the off-line mode) . Christo Ananth et al. [4] proposed a method in which the minimization is per-formed in a sequential manner by the fusion move algorithm that uses the QPBO min-cut algorithm. Multi-shape GCs are proven to be more beneficial than single-shape GCs. Hence, the segmentation methods are validated by calculating statistical measures. The false positive (FP) is reduced and sensitivity and specificity improved by multiple MTANN.

Signature is one of the oldest biometric hallmarks used for authentication of a personal or a document. Even in the modern digital era, signature remains one of the favored means for the authentication of official documents like bank checks, credit card transactions, certificates, contracts and bonds. An automatic signature verification system aims to verify the identity of AN individual supported the analysis of his or her signature.

Depending on the signature acquisition technique used, automatic signature verification systems can be classified into 2 groups: on-line (dynamic) and offline (static). A static signature image, generally scanned at a high resolution, is the only input to offline systems.

This paper presents the state of the art in automatic signature verification, with specific attention to the most recent advancements. Following an introduction of the phases of the signature verification method, the main contributions of research activities in recent year's square measure delineated and also the most promising trends square measure mentioned. Specifically, Section II presents the main aspects associated with data acquisition and preprocessing and Section III discusses the feature extraction section.

Compared to other biometric techniques requiring cooperative subjects such as fingerprint recognition and iris recognition, face recognition might not have a superior level of accuracy, but operating with faces definitely has clear blessings of being natural and passive. Face recognition has drawn increasing attention because of its potential applications in several fields, such as identity authentication, information security, surveillance, human-computer interface, and so on.

## 2. BIOMETRICS OVERVIEW

Biometrics is a technology used to identify, analyze, and measure an individual's physical and behavioral characteristics. A biometric system is a technology which takes an individual's physiological, behavioral, or both traits as input, analyzes it, and identifies the individual as a genuine or malicious user. Each human being is unique in terms of characteristics, which make him or her different from all others. The physical attributes such as finger prints, color of iris, color of hair, hand geometry, and behavioral characteristics such as tone and accent of speech, signature, or the way of typing keys of computer keyboard etc., make a person stand separate from the rest.

In the 19th century, an Anthropologist named Alphonse Bertillion developed a method (named Bertillionage) of taking body measurements of persons to identify them. He had realized that even if some features of human body are changed, such as length of hair, weight, etc., some physical traits of body remain unchanged, such as length of fingers. This method diminished quickly as it was found that the persons with same body measurements alone can be falsely taken as one. Subsequently, Richard Edward Henry from Scotland Yard developed a method for fingerprinting.

The idea of retinal identification was conceived by Dr. Carleton Simon and Dr. Isadore Goldstein in 1935. In 1976, a research and development effort was put in at EyeDentify Inc. The first commercial retina scanning system was made available in 1981.

In 2001, Biometrics Automated Toolset (BAT) was introduced in Kosovo, which provided a concrete identification means. Today, biometric has come up as an independent field of study with precise technologies of establishing personal identities

ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

## 3. USES OF BIOMETRICS

With increasing use of Information Technology in the field of banking, science, medication, etc., there is an immense need to protect the systems and data from unauthorized users. Biometrics is used for authenticating and authorizing a person. Though these terms are often coupled; they mean different.

### 3.1 Authentication (Identification)

This process tries to find out answer of question, "Are you the same who you are claiming to be?", or, "Do I know you?" This is one-to-many matching and comparison of a person's biometrics with the whole database. The first type of authentication is accepting proof of identity given by a credible person who has first-hand evidence that the identity is genuine. When authentication is required of art or physical objects, this proof could be a friend, family member or colleague attesting to the item's provenance, perhaps by having witnessed the item in its creator's possession. With autographed sports memorabilia, this could involve someone attesting that they witnessed the object being signed.

The second type of authentication is comparing the attributes of the object itself to what is known about objects of that origin. For example, an art expert might look for similarities in the style of painting, check the location and form of a signature, or compare the object to an old photograph. An archaeologist, on the other hand, might use carbon dating to verify the age of an artifact, do a chemical and spectroscopic analysis of the materials used, or compare the style of construction or decoration to other artifacts of similar origin

### 3.2. Verification

This is the one-to-one process of matching where live sample entered by the candidate is compared with a previously stored template in the database. If both are matching with more than 70% agreeable similarity, then the verification is successful.

### 3.3. Authorization

It is the process of assigning access rights to the authenticated or verified users. It tries to find out the answer for the question, "Are you eligible to have certain rights to access this resource?"

The function of specifying access rights to resources related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define an access policy. For example, human resources staff is normally authorized to access employee records and this policy is usually formalized as access control rules in a computer system. During operation, the system uses the access control rules to decide whether access requests from (authenticated) consumers shall be approved (granted) or disapproved (rejected). Resources include individual files or an item's data, computer programs, computer devices and functionality provided by computer applications. Examples of consumers are computer users, computer Software and other Hardware on the computer.

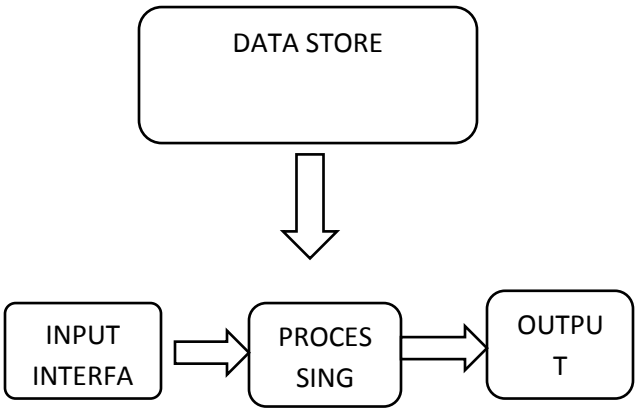
ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

# 4. BIOMETRIC SYSTEM

**Basic Components of a Biometric System**

In general, Biometric system is divided into four components,




### 4.1 Input Interface (Sensors)

It is the sensing component of a biometrics system that converts human biological data into digital form. For example, A Metal Oxide Semiconductor (CMOS) imager or a Charge Coupled Device (CCD) in the case of face recognition, handprint recognition, or iris/retinal recognition systems. An optical sensor in case of fingerprint systems. A microphone in case of voice recognition systems.

### 4.2 Processing Unit

The processing component is a microprocessor, Digital Signal Processor (DSP), or computer that processes the data captured from the sensors. The processing of the biometric sample involves −Sample image enhancement, Sample image normalization, Feature extraction. Comparison of the biometric sample with all stored samples in database.

### 4.3 Database Store

The database stores the enrolled sample, which is recalled to perform a match at the time of authentication. For identification, there can be any memory from Random Access Memory (RAM), flash EPROM, or a data server. For verification, a removable storage element like a contact or contactless smart card is used.

### 4.4 Output Interface

The output interface communicates the decision of the biometric system to enable the access to the user. This can be a simple serial communication protocol RS232, or the higher bandwidth USB protocol. It could also be TCP/IP protocol, Radio Frequency Identification (RFID), Bluetooth, or one of the many cellular protocol.

# 5. PATTERN RECOGNITION

Pattern recognition deals with identifying a pattern and confirming it again. In general, a pattern can be a fingerprint image, a handwritten cursive word, a human face, a speech signal, a bar code, or a web page on the Internet. The individual patterns are often grouped into various categories based on their properties. When the

patterns of same properties are grouped together, the resultant group is also a pattern, which is often called a pattern class.

Pattern recognition is the science for observing, distinguishing the patterns of interest, and making correct decisions about the patterns or pattern classes. Thus, a biometric system applies pattern recognition to identify and classify the individuals, by comparing it with the stored templates.

**Pattern Recognition in Biometrics**

The pattern recognition technique conducts the following tasks –

**Classification** is identifying handwritten characters, CAPTCHAs, distinguishing humans from computers.

**Segmentation** is detecting text regions or face regions in images.

**Syntactic Pattern Recognition** is determining how a group of math symbols or operators are related, and how they form a meaningful expression.

**Popular Algorithms in Pattern Recognition**

The most popular pattern generation algorithms are −

**Nearest Neighbor Algorithm**

You need to take the unknown individual's vector and compute its distance from all the patterns in the database. The smallest distance gives the best match.

**Back-Propagation (Back prop) Algorithm**

It is a bit complex but very useful algorithm that involves a lot of mathematical computations.

## 6. BIOMETRICS SYSTEM SECURITY

A number of solutions are proposed to address the biometric system security issue. Biometric templates are never stored in the raw form. They are encrypted; sometimes even twice. In the case of biometrics, there are various resources involved such as humans (subjects or candidates), entities (system components or processes), and biometric data (information). The security requirements of confidentiality, integrity, authenticity, non-repudiation, and availability are essential in biometrics. Let us go through them briefly.

### 6.1 Authenticity

It is the quality or the state of being pure, genuine, or original, rather than being reproduced. Information is authentic when it is in the same state and quality when it was created, stored, or transferred.

There are two authenticities in a biometric system − entity authenticity and data origin authenticity. Entity authenticity confirms that all entities involved in the overall processing are the ones they claim to be. Data origin authenticity ensures genuineness and originality of data. For example, the biometrics data is captured with sensor devices. The captured data that came from a genuine sensor is not spoofed from a previous recording.

### 6.2 Confidentiality

It is limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized people. In cases of a biometric system, it mainly refers to biometric and related authentication information when it is captured and stored, which needs to be kept secret from unauthorized entities. The biometric information should only be accessible completely to the person it belongs. During identification and variation, the accessing candidate needs to be restricted with appropriate security measures.

### 6.3 Integrity

It is the condition of being complete and unaltered that refers to its consistency, accuracy, and correctness. For a biometric system, the integrity should be high. Any malicious manipulations during operation and storage should be kept away or detected earliest by including its notification and correction.

### 6.4 Non-repudiation

It is identification of involved resources such as entities and components. It is also seen as accountability. For example, it prohibits a sender or a recipient of biometric information from denying having sent or received biometric information.

### 6.5 Availability

A resource has the property of availability with respect to a set of entities if all members of the set can access the resource. An aspect called reachability ensures that the humans or system processes either can or cannot be contacted, depending on user interests. Attackers can make the system unusable for genuine users, thus preventing them from using authenticated applications. These attackers target the availability of the information.

## 7. CONCLUSION

Biometrics can only be limited by limiting one's imagination. Biometric technology is now being used in almost every area. Not only that, but various types of biometric systems are being used to achieve various functionalities. We have short listed a few highly popular applications of biometrics technology. Although this list is no way complete it is simply an effort to list a few of the more popular biometric applications

## .9. REFERENCES

[1] Prabhakar,S.,Kittler,J.,Maltoni,D.,O'Gorman,L.,Tan,T.:Intro- duction to the special issue on biometrics: progress and direc- tions.IEEETran.PatternAnal.Mach.Intell.29(4),513–516(2007)

[2] S. Chen, and S. Srihari, "Use of Exterior Contour and Shape Features in Off-line Signature Verification", 8th International Conference on Document Analysis and Recognition (ICDAR '05), 2005, pp. 1280-1284.

[3] J. Coetzer. Off-line signature verification. PhD thesis, Uni- versity of Stellenbosch, South Africa, 2005. 2

[4] Christo Ananth, G.Gayathri, M.Majitha Barvin, N.Juki Parsana, M.Parvin Banu, "Image Segmentation by Multi-shape GC-OAAM", American Journal of Sustainable Cities and Society (AJSCS), Vol. 1, Issue 3, January 2014, pp 274-280

[5] K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," Circuits and Systems for Video Technology, IEEE Transactions on, vol. 14, no. 1, pp. 4–20, 2004.

[6] Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biomet- ric recognition. IEEE Trans. Circuits Syst. Video Technol. 14(1), 4–20 (2004).

[7] R. Plamondon and S. N. Srihari, "Online and off-line handwriting recognition: a comprehen- sive survey," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 22, no. 1, pp. 63–84, 2000.

[8] C.AllgroveandM.C.Fairhurst,"Majorityvotingforimprovedsignature verification,"in Proc. Inst. Elect. E Colloq. Vis. Biometrics,London, U.K., 2000, pp. 9-1–9-4

[9] C. J. C. Burges. A tutorial on support vector machines for pattern recognition. Data Min. Knowl. Discov., 2:121–167, June 1998. 4.

[10] K. Han, and I.K. Sethi, "Handwritten Signature Retrieval and Identification", Pattern Recognition 17, 1996, pp. 83-90.