**Dr. AMBEDKAR INSTITUTE OF TECHNOLOGY**

**An Autonomous Institute Affiliated to VTU, Belgaum and Aided by Government of Karnataka Near Janna Bharathi Campus Bangalore 560056**  

**SYNOPSIS OF**

**MINI PROJECT WORK**

**ON**

**“OFFLINE SIGNATURE AUTHENTICATION**

**USING HORIZONTAL AND VERTICAL PROJECTIONS”**

**Submitted in partial fulfilment of the requirement for the Award of the Degree of**

**BACHELOR OF ENGINEERING**

**IN**

**ELECTRONICS AND TELECOMMUNICATION ENGINEERING**

**SUBMITTED BY**

**Pallavi S 1DA19ET040**

**Santhosh BC 1DA19ET043**

**Shreyas S 1DA19ET044**

**Ullas J Naik 1DA19ET048**

**Under the guidance of**

**Dr. PRASHANTH C.R**

**PROFESSOR**

**Department of Electronics and Telecommunication Engineering, Dr. AIT**

**OFFLINE SIGNATURE AUTHENTICATION USING HORIZONTAL AND VERTICAL PROJECTIONS**

**1. ABSTRACT**

Authentication is the key process to speak the truth of an attribute claimed by the real entity. There are several ways to make authentication more robust and biometrics is one among them. From past decade, Biometric technology is widely adopted and accepted everywhere to authenticate an individual’s identity. Biometrics overcomes the limitations faced by the traditional authentication process such as knowledge-based issues including password and token for the authentication of an individual. Signature is the most widely accepted biometric to identify verification. As signatures continue to play an important role in financial, commercial and legal transactions, truly secured authentication becomes more and more crucial. A signature by an authorized person is considered to be the “seal of approval” and remains the most preferred means of authentication. An image of a signature is fed to the signature verification software and is compared with the signature image from the database, to authenticate whether the signature is genuine or forged.

**2. INTRODUCTION**

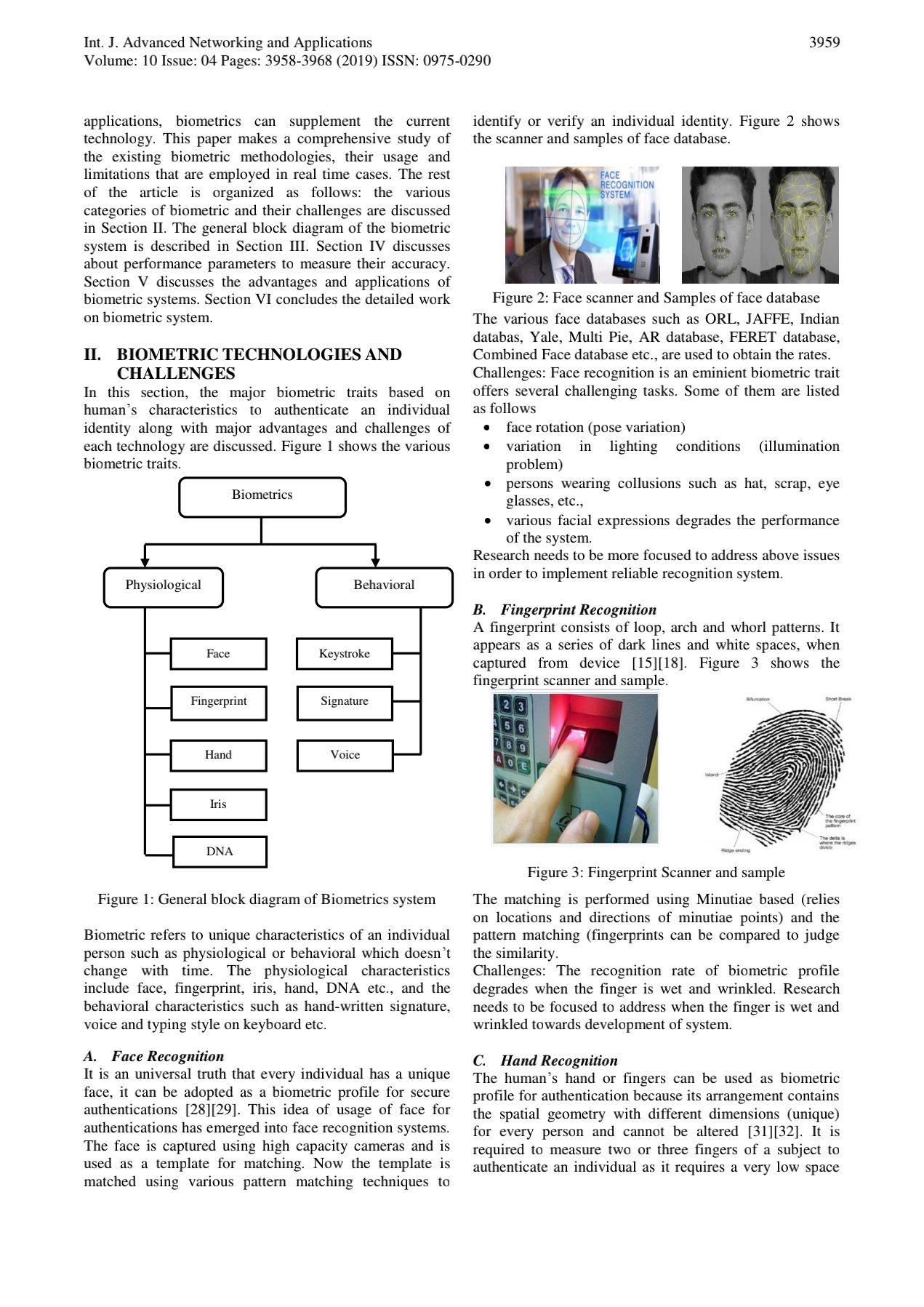
A signature is a person's name written in a distinctive way as a form of identification in authorizing a cheque or document or concluding a letter. Signatures are widely used as a means of personal identification and verification. Many documents like bank cheques and legal transactions require signature verification.

Traditional identity verification methods such as tokens, passwords, pins etc, suffer from some fatal flaws and are incapable to satisfy the security necessities. Password-based logins are problematic because passwords are easily forgotten and inherently insecure. Token-based authentication is also failing to meet the mark as a modern form of verification. An obvious drawback is that tokens must be carried at all times and are non-transferable — a characteristic that’s outdated in today’s user experience-focused world. Signature-based verification of a large number of documents is a very difficult and time-consuming task.

The vital need for the security enhancement is being realised by leading companies, from industries like financial services, healthcare, travel, entertainment and gaming. Modern businesses are understanding that in light of cybercrime, the dark web and the global nature of online fraud, they need to dispense with traditional, insecure and unreliable methods of authentication, and adopt modern biometric-based methods.

Biometrics is measure of biological or behavioural features which are used for identification of individuals. Most of these features are inherited and cannot be guessed or stolen.

A biometric system is the latest technology which helps in recognizing a user's physiological, behavioural or both characters as input, verifies it, and identifies the individual as a unique user. The various biometric traits are shown below.



The difference between using physiological and behavioural biometrics when authenticating users is that physiological biometrics can definitely improve security in certain circumstances. It requires input from specific sensors depending on the trait is being measured. Most techniques are used to verify that a person is physically present and alive.

Behavioural biometrics, on the other hand, checks for patterns of behaviour that are virtually impossible to spoof. Behavioural biometrics applications can analyse the way we interact with things in the world around us, such as how we type or swipe on a phone, and they can be considered tolerant of changes in individual patterns of behaviour.

Signatures are basically used to authenticate documents, transactions and other paper/manual-based instruments. Signature on any paper/document implies that the signer approves the responsibility of the data of the document. The traditional method of signing the process required a signer in person to sign and verify a particular document. It was more popular because of its distinctive property of handwritten and styling pattern which was difficult to imitate.

Biometric Signature is analyzing and recording people’s physical characteristics. These characteristics are encrypted, stored securely and embedded in the signed document. The biometric data is unique to every individual and therefore is used to identify an individual as well as link a particular document or data to him.

As signature is the primary mechanism both for authentication and authorization in legal transactions, the need for efficient auto-mated solutions for signature verification has increased. Unlike a password, PIN, PKI or key cards, identification data that can be forgotten, lost, stolen or shared the captured values of the handwritten signature are unique to an individual and virtually impossible to duplicate. Signature verification is natural and intuitive. The technology is easy to explain and trust.

A signature verification system and the techniques used to solve this problem can be divided into two classes Online and Off-line. On-line approach uses an electronic tablet and a stylus connected to a computer to extract information about a signature and takes dynamic information like pressure, velocity, speed of writing etc, for verification purpose. Off-line signature verification involves less electronic control and uses signature images captured by scanner or camera. An off-line signature verification system uses features extracted from scanned signature image. The features used for offline signature verification are much simpler. In this, only the pixel image needs to be evaluated. The verification process has to wholly rely on the features that can be extracted from the trace of the static signature images only.

The main objective is to verify offline handwritten signatures, which include characters, words, lines, paragraph etc. The approach is to validate whether the signatures are a match to the ones in the database and whether or not they are fraud.

**3. RELATED WORKS**

A handwritten signature is the result of a complex process depending on the psychophysical state of the signer and the conditions under which the signing process occurs. Although complex theories have been proposed to model the psychophysical mechanisms underlying handwriting and the ink processes, signature verification is still an open challenge since a signature is usually judged to be genuine or a forgery on the basis of only a few reference specimens [1]. The biggest limitation of off-line signature verification methods is the absence of temporal information. While on-line signature verifiers are able to compare the different features as a function of time, off-line verifiers are limited to the comparison of two-dimensional images; therefore, they often try to compare global features like size of the signature or similarities of the contour [2] [3] [4]. To get a tractable abstraction of the two-dimensional images, these methods often involve some image transformation, like the Houghor Radon transformations [5] or work on the density models of the signatures [6].

**4. PROPOSED MODEL**

To validate the signatures, our model consists of input, pre-processing, feature extraction and verification(output).

Input

Pre-processing

Feature Extraction

Verification

**4.1 INPUT**

The input to the system is the signature that is only available as a static image, typically obtained after it has been written on paper using a variety of writing instruments, with no reference to the sequence and timing of the pen strokes, which created the signature.

This step also includes the creation of the database. The database includes the collection of genuine and few test signatures.

**4.2 PREPROCESSING**

Pre-processing is the set of subsequent operations applied for the improvement of quality of signature image. This improvement in quality of image increases the accuracy of further steps involved in processing without losing relevant information. The various sub processes involved in pre-processing are cropping, filtering, conversion of color image to gray scale, binarization, thinning, rotation, resizing.

**4.2.1 Cropping**

The image is cropped, to the bounding rectangle of the signature.

**4.2.2 Filtering**

A noise reduction filter is applied to the image for eliminating single black pixels on white background.

**4.2.3 Conversion of color image to gray scale**

The luminance of pixel value of a grayscale image ranges from 0 to 255. The conversion of a color image to a grayscale image is converting the RGB values (24 bit) into grayscale value (8 bit).

**4.2.4 Binarization of grey scale image**

Binarization is the method of converting any grayscale image into black and white image.

**4.2.5 Thinning**

The goal of thinning is to eliminate the thickness differences of pen by making the image one pixel thick.

**4.2.6 Rotation for skew correction**

The skewness of the image is corrected by rotating at a particular angle.

**4.2.7 Resizing**

This process allows to make the image smaller or larger without cutting anything out. This is done to reduce the size of large files to make them easier for verification.

**4.3 FEATURE EXTRACTION**

Each person’s signature has different style. When someone tries to copy other’s signatures then they basically try to maintain the shape. But some important features can make a signature difficult to be copied. Now these features are analyzed and are used in this proposed method to differentiate genuine from forge one.

The following features are extracted from the processed image:

* **Normalized Signature Area**

It is the total number of black signature pixels in the signature image. Signature area gives information about the signature density. If in a signature image, total number of signature pixels (or black pixels if foreground image is black) is indicated as B, and total number of pixels in the whole image is indicated as P,

then normalized signature area = B/P

* **Aspect Ratio** (signature width to height ratio)

This is ratio of signature width to signature height of a cropped signature.

The aspect ratio of the processed image = width/height.

* **Maximum Horizontal Projection**

Horizontal projection is found by counting the number of signature image pixels in each row in a signature image and plotting it horizontally with a line. The row with maximum value gives the maximum horizontal projection.

* **Maximum Vertical Projection**

Counting and plotting signature pixels in vertical direction for every column, gives maximum vertical projection.

* **Centre of gravity or Centroid**

In a binary image signature image with black signature pixels, Centre of gravity or Centroid is the average coordinate point of all black pixels.

**4.4 VERIFICATION**

The features are extracted from the preprocessed signature image and then the image is compared with the signature image in the database to find whether or not the input signature image is genuine.

**5. OUTCOMES**

The output of the system gives the threshold value, False Acceptance Ratio (FAR) and False Rejection Ratio (FRR). The code is written in MATLAB that distinguishes between genuine and forged signatures.

**8. SOFTWARE USED**

MATLAB (R2022a)

MATLAB is a programming and numeric computing platform used to analyze data, develop algorithms, and create models.

**9. ADVANTAGES**

* Signature verification systems are user friendly and well accepted socially and legally.
* The most significant benefit of signature recognition is that it is highly resistant to impostors. although it is quite easy to forge the actual signature, it is very difficult to mimicthe behavioral patterns which are inherent in the process of signing.
* Enrollment is intuitive and fast.
* Non-intrusive and non-invasive.
* Signature verification in general has a fast response and low storage requirement.
* The signature verification system is independent of the native language user.
* Little time of verification.

**10. APPLICATIONS**

* **Indian Patent Office**

The Indian Patent Office used to process patent, copyrights and trademark applications manually. However, the system was inefficient with instances of corruption rife. In order to make the system streamlined the Patent Office modified its application process making it online dispensing with the need of any human intervention. According to the new system, the applications can be filed from anywhere in the world and all the applications are digitally signed.

* **Directorate General of Foreign Trade**

The DGFT processes request and issues import and export licenses. With hundreds of licenses issued daily; the manual process was rife with corruption and abuse. In order to make the processing of licenses more streamlined an online system was implemented which enabled the users to file the applications online under different schemes like DEPB, EPCG leading to better MIS, audit and accountability. Under this system applications were filed online.

* **E-Procurement**

Procurement tenders has been increasing in complexity for some time with the increase in the number of cartels, rigging and leakage of information. In order to remove these advantages an online system of tendering was devised which sought to reduce the human interface as much as possible by allowing the vendors to provide information and quote online. The reliability of the documentation was achieved through a system of digital signatures that was implemented with the help of electronic signature software.

**11. REFERENCES**

[1] D. Impedovo and G. Pirlo, “Automatic signature verification: The state of the art,” IEEE Trans. Syst. Man Cybern.—Part C: Applications Rev., vol. 38, no. 5, pp. 609–635, Sep. 2008.

[2] E. Frias-Martinez, A. Sanchez, and J. Velez, "Support vector machines versus multi-layer perceptrons for efficient off-line signature recognition," Engineering Applications of Artificial Intelligence, no. 19, p. 693– 704, 2006, Teszt adatok generálása.

[3] M. A. Ferrer, J. B. Alonso, and C. M. Travisco, "Offline geometric parameters for automatic signature verification using fixed point arithmetic," IEEE Transactions on Pattern Analyisis and Machine Intelligence, vol. 27, no. 6, pp. 993-997, Jun. 2005.

[4] R. Sabourin, J. P. Drouhard, and E. S. Wah, "Shape matrices as mixed shape factor for off-line signature verification," Fourth International Conference on Document Analysis and Machine Intelligence, vol. 22, no. 9, pp. 938-949, Sep. 2000.

[5] H. A. S. Touj and N. B. Amara, "Global feature extraction of offline arabic handwriting," IEEE SMC, vol. 2, no. 4, 2003.

[6] J. Mahmud and C. M. Rahman, "On the power of feature analyser for signature verification," Proceedings of the Digital Image Computing, Techniques and Applications, 2005