The International Journal of Engineering and Science (IJES)
|| Volume || 7 || Issue || 7 Ver. II|| Pages || PP 56-66 || 2018 ||
ISSN (e): 2319 – 1813 ISSN (p): 23-19 – 1805

Handwritten Dynamic Signature Biometric Verification Using Plainarised Region of Interest [Proi] Method

Benson-Emenike, Mercy E., Igwe, Agu Felix
Department of Computer Science,Abia State Polytechnic, Aba
Department of Computer Engineering,Abia State Polytechnic, Aba
Corresponding Author: Benson-Emenike

--***ABSTRACT***--

The technological advancement, experienced in our society today, necessitates a dependable and unswerving authorization and verification of persons; and this has become an indispensible application s in fostering authenticity and reliability in medical, travel and immigration, access control, financial and business transactions etc. biometric authentication has drastically eradicated risk of fraud, theft of personal data and theft of identity which were paramount in the traditional individual identification and verification. Dynamic or online signature verification involves capturing a person's signature as he writes it using special devices such as tablet and digitizer pen or stylus.Plainarised Region Of Interest **[***PROI] is a special pre-processing method used in this work. It involves processes involving Signature Size Normalization, Thinning, Denoising and Filtering, Binarization, and Width Normalisation; and gives high rate and accurate verification.*

Keywords: *Digital, Signature, Biometrics, Verification, PROI.*

Date of Submission: 09-07-2018 Date of acceptance: 23-07-2018

I. INTRODUCTION

Biometrics is a division of science that uses computer knowledge to establish human identification or authentication, based on a person's behavioural or physical characteristics. Biometrics is a constituent of two Greek words, 'bio' and 'metrics'. 'Bio' in the word biometrics has to do with natural life and refers to the quantifiable physical or biological traits while 'metrics' literally means 'to measure' and refers to the quantitative or measurable analysis for accurate authentication of a person [1]. It has been observed from the definition of biometrics that the use of biometrics in person's authentication yields better results than traditional methods.

The two old-fashioned methods of human identification were the Knowledge-based technique, in which identification is done based on what a person can remember e.g. secret code or somebody's ID and Token-based technique, in which personal identification is based on what a person has e.g. car driver's permit, passport, identity card, credit card, or keys [2].

These traditional methods have some shortcomings such as one could forget, misplace, lose or steal tokens, since they are not based on natural traits [3]. They cannot be adequately used to distinguish between an authorized person and an impostor hence guarantees insufficient security demands [2]. There is another method of identification or authentication known as biometrics; which has been proved to be stronger, more secure and dependable. Also, the use of encryption to protect templates is generally expensive because the matching algorithms require that such encrypted templates be decrypted prior to matching. This exposes the decrypted templates to potential hacker attacks. Therefore, our handwritten dynamic signature biometric verification using Plainarised Region Of Interest [PROI] method is the answer to all these limiting factors.

A signature is a handwritten name, sobriquet, a draw or just a mark that is stylized to be unique to an individual. They are used to authenticate or approve documents, transactions and other paper-based instruments.When an individual's signature is affixed to a document, it simply means that the signatory bears the responsibility of the content of the document.

II. OVERVIEW OF BIOMETRIC TECHNOLOGIES

There are various biometric technologies, as seen in Fig.1, and the choice of each of them depends on the process to be achieved. Biometric technologies have both advantages and disadvantages. The following is a brief introduction of the commonly used biometric technologies:

- **Face Biometrics:**Face biometrics is the most natural way of human identification. It works even when an individual is not putting into cognizance that he is being scanned. Face identification is an active and manageable research area with varied applications [4].

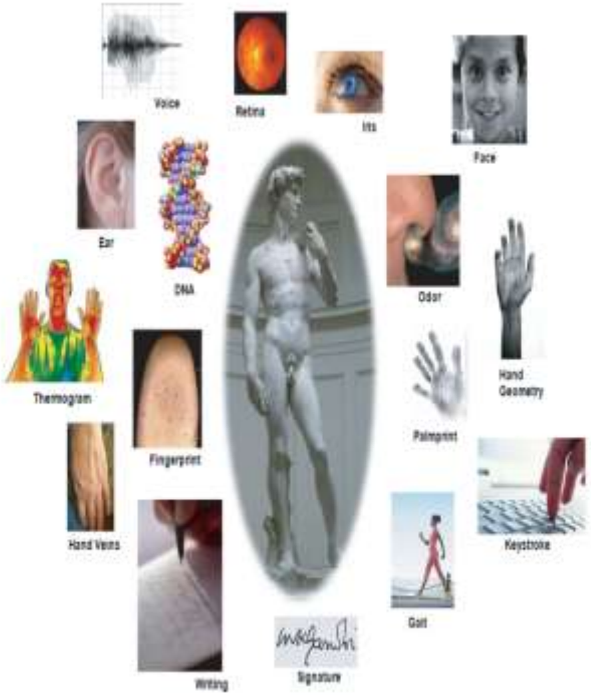


Figure 1: Biometric Features

(Source: Virginia, [5])

- **Facial Thermogram:**When heat is applied to a facial tissue, the human face vascular system releases a facial symbol which can be obtained using an infrared camera (Prakash, 2010). The resultant image is known as a facial thermogram. The uniqueness of an individual's facial thermogram is so distinct that even plastic surgery does not alter it as long as the flow of blood through the veins is not restructured. Infrared sensors used for facial thermogram is so expensive that the technology is hardly used.

- **Fingerprint Biometrics:**The fingerprint of a fetus becomes clear and at its seventh month. Human fingerprints are not the same; even identical twins have different fingerprints. Secretions from fingerprints can be used for forensic purposes. The use of fingerprint for personal identification has been for centuries and its authenticity has been clearly established [6].British researchers, in 2008, discovered means of identifying users of cocaine, marijuana and methadone from their fingerprint residues. This approach can be used to identify people who are addicted to cannabis, heavy coffee, and various other drugs [7]

- **Hand Geometry-Based Biometrics:**Measurements of the human hand, such as its shape, lengths and widths of fingers can be used as biometric characteristics [8]. Hand Geometry is the measurement of the thickness of the palm, the length and breadth of the fingers and other hand characteristics.

- **Palm Vein Biometrics:**A palm has a broad and complex blood vein pattern which is unique to every individual. It does not vary as long as the person lives. It cannot be spoofed since they are embedded under the skin. Infrared light is used for the data capture.
- **Palm Print Biometrics:**A palm print is the captured pattern or image of a palm; which is naturally endowed with distinctive ridges and valleys for every human being. This image can be offline i.e. taken with ink and paper or on-line i.e. taken by a Charge-Coupled Device (CCD) or a scanner[9].

- **Retinal Pattern Biometrics:**Retina scan is a capture of the retina blood vessel pattern of the eye. It is stable and unique. Retina is hidden and as such requires an infrared light to illuminate it for better extraction of the pattern. Retina image acquisition cannot be done from a distance hence enrollee's cooperation is highly needed.

- **Iris Biometrics:**The iris is a distinctive and sophisticated section of the eye which is bordered by the pupil and the white region of the eye known as the sclera. It has some useful features which can be used for person's identification.
- **Keystroke Biometrics:**Keystroke biometrics is a behavioral biometrics which measures the time lapse between the depressing and releasing a key on a keyboard. However, it suffers from high degree of dissimilarities.
- **Speech Biometrics**: This is a behavioral biometrics that involves the conversion of an audio signal captured by a telephone or microphone to a set of words. The variation in the size and shape of the mouth, nasal cavities, lips and vocal tracts, creating the sound, brings about variations in the way people speak.
- **Ear Biometrics:**The distance of salient points of the ear are used in ear biometrics for recognition. Ear growth becomes distinct after the first four months of birth; but there could be ear elongating due to gravity [10]. Several methods are used for this biometric although none of them can be trusted in terms of performance reliability.
- **DNA Biometrics:**Every individual has a distinctive Deoxyribo Nucleic Acid (DNA); however, identical twins have the same identical DNA patterns. Every human being has 23 pairs of chromosomes containing DNA. One chromosomal pair is paternal while the other is maternal. One of the constituents of a cell is its DNA. DNA is currently used in Forensic applications for individual recognition but has some serious drawbacks such as difficulty in obtaining a biometric sample, vulnerable to spoofing, not all stages of comparison are automated and extraction method requires complex chemical methods.
- **Gait Biometrics:**Gait is harmonized specific patterned motion resulting in human movement. Here, the eyes and the brain are maximally engaged. Since, everyone can observe how one walks, it becomes very difficult for this biometric to be spoofed.
- **Odor Biometrics:**Human beings emit chemicals which the body releases as body odor. It is practically unique and can conveniently distinguish an individual from the crowd. Human beings have different immunity genes which determine their body odors. A body odor, which is a mixture of about thirty different smell molecules (sweet-smelling or offensive), can be distinctively used for recognition purposes. However, this method has low recognition accuracy because human odors cannot be quickly captured and process result can be altered with perfumes or deodorants.
- Voice Biometrics: A voice biometric is a unique numeric interpretation of the sound, rhythm, pitch, tone, frequency, pattern and other characteristics that make up a person's vocal sound. It can also be used as an individual distinguishable trait. Voice biometrics guarantees a higher recognition accuracy and security particularly to applications using telephones, microphones, etc.
- RFID (Radio Frequency Identification): RFID (radio frequency identification) is a technology that uses radio waves to transmit a person's or object's identity wirelessly in the form of a unique serial number; using devices consisting of elements such as a chip, antenna, reader, and a database. It has the advantage of scanning a person even when he is unaware that he is being scanned.
- Writing: Writing is a behavioral biometrics that is easy to capture and can be easily changed over time. A sizeable amount of text must be captured in order to have a good recognition and cannot be effectively used in some applications(e.g. forensic).

III. REVIEW OF RELATED LITERATURE

Many techniques have been developed in the field of signature-based biometric authentication. Some examples of biometric verification and identification approaches and optimised schemes are discussed below:

Bromme, in his study showed that every person has both behavioural and physiological biometric characteristics which are static and dynamic. These characteristics are actually used for the recognition of individuals. He majored on the classification of biometric signatures[11].

Rabasse et al., described a method for the generation of synthetic handwritten signatures, in the form of sequences of time-stamped pen data channels, for use in online signature verification experiment. The method presents modelled variability within the generated data based on variation that is naturally found within genuine source data [12].

Yeung et al., 2004 used SVC2004 dataset and a commercial signature verification engine to show that the synthesized data achieves comparative verification performance to the use of genuine data. The method uses two seed signatures from a signer with captured data in the form of time stamped vectors [13].

Pascual et al., 2012proposed score normalization in biometric signature recognition based on client threshold prediction [14]. The use of score normalization in biometric based recognition system is a very important part, particularly in those based on behavioural traits, such as written signature. The score normalization techniques can be classified as: i) Test dependent and ii) Target dependent. The first is used mainly in speaker verification, while the second approachis used for signature verification techniques.

Kumar et al., presented Biometric security system based on signature verification using neural networks as a classifier for the authentication of a signature.The global and grid features are combined to generate new set of features for the verification of signature. Random, unskilled and skilled signature forgeries along with genuine signatures were considered for performance analysis of the system. Some common global features such as Aspect Ratio, Signature Height, Image Area, Pure Width and Pure Height were considered [15].

Maiorana et al., proposed a signature-based biometric authentication system, where water marking techniques have been used to embed some dynamic signature features in a static representation of the signature itself. A multi-level verification scheme, which is able to provide two different levels of security, has been obtained. These proposed watermarking techniques are based on the properties of the Radontransform which well fits to the signature images [16].

Maiorana et al., discusses a protected on-line signature-based biometric authentication system, where the biometrics considered are secured by means of noninvertible alterations, able to produce templates from which retrieving the original information is computationally as hard as random guessing it. The benefits of using a protection technique based on non-invertible transforms are exploited by presenting three different matching strategies in the converted domain, and by suggesting a multi-biometrics method based on score-level fusion to improve the performances ofthe considered system. The

experiments were evaluated on the public MCYT signature database[17].

Maiorana et al., presented an on-line signature-based biometric authenticationsystem in which non-invertible transformations are applied to the acquired signature functions, creating impossible to derive the original biometrics from the kept templates, while keeping the same recognition performances of an unprotected method. Specifically, the possibility of producing cancellable templates from the same original dataset, thus offering a proper solution to privacy concerns and security issues, is intensely explored [18]. Nagasundara et al., presented an authentication approach based on hand geometry, palmprint and signature. The aim of that paper is to exploit the best possible combinations of hand geometry, palmprint and static signatures for multimodal biometric systems by integrating the information at score level fusion. Primarily, Zernike moments are extracted for each biometric trait of a person and study the identification accurateness. Consequently, the effect of identification accuracy using score level fusion of multiple traits of a person is investigated. Experimentations are accompanied on GPDS hand geometry dataset, PolyU two dimensional palmprint dataset and UOM offline signature database to assess the actual advantage of the fusion of multiple biometric traits performed at score level fusion[19].

In Mhatre and Maniroja’s method, a signature based authentication using two different algorithms was introduced [20]. Before extracting different features from the signature, some pre-processing of the signature is performed. In pre-processing, the signature is colour normalized and scaled into a standard format. The process is pretty different and it deals with extraction of features based on moment, standard deviation and mean. The process uses Euclidean distance classifier for comparing test signature with database. The algorithm has shown promising results while dealing with random forgeries and simple forgeries; also it gives good recognition rate. Maiorana et al., introduced a set of noninvertible conversions, which can be employed to any biometrics whose template can be represented by a set of sequences, in order to produce multiple transformed versions of the template [21]. Once the transformation is made, recovering the original data from the transformed template is computationally as hard as random guessing. As a proof of perception, the suggested method is applied to an on-line signature recognition scheme, where a hidden Markov model-based matching approach is applied. The performance of a secured on-line signature recognition system employing the proposed BioConvolving approach is calculated, both in terms of verification rates and renewability capacity, employing the MCYT signature dataset. The reported extensive set of experimentations showed that protected and renewable biometric templates can be properly generated and used for recognition.

IV. BIOMETRICSIGNATURE

Every human being has a distinct writing style and that makes it useful for biometric authentication. However, a person’s signature may vary due to the person’s physical and emotional state as well as the force applied to the surface and the rapidity of motion of the pointer across the sensor.The process of signing signatures involves some biomechanical processes which takes place in the brain. To sign a signature, a signal is sent from the spinal cord to the particular muscles required for the signature especially the arm muscles. Then by the movement of the fingers on the paper, capacitated by the muscles of the arm, signature is affixed.

Two methods are involved in a handwritten signature verification. They are Static or offline signature verification and Dynamic or on-line signature verification. In a static mode, handwritten signature data is converted to digital form by scanning the signature from the signature collection paper. In this case, the handwritten signatures are represented as a gray level image. In adynamic signature verification, signature data acquisition is done by using a special pen on an electronic surface. The most conventional online data acquisition devices are digitizing tablets [22].As the writing of the signature is being produced, information such as the speed, order of strokes, number of strokes, acceleration and local pressure are captured.

4.1 Verification (1-to-1 matching)

Verification or 1-to-1 matching is a recognition method of matching an individual's captured biometric features with his biometric template stored in secure memory or database. This is otherwise called a 1-to-1 matching, as shown in Fig. 2.

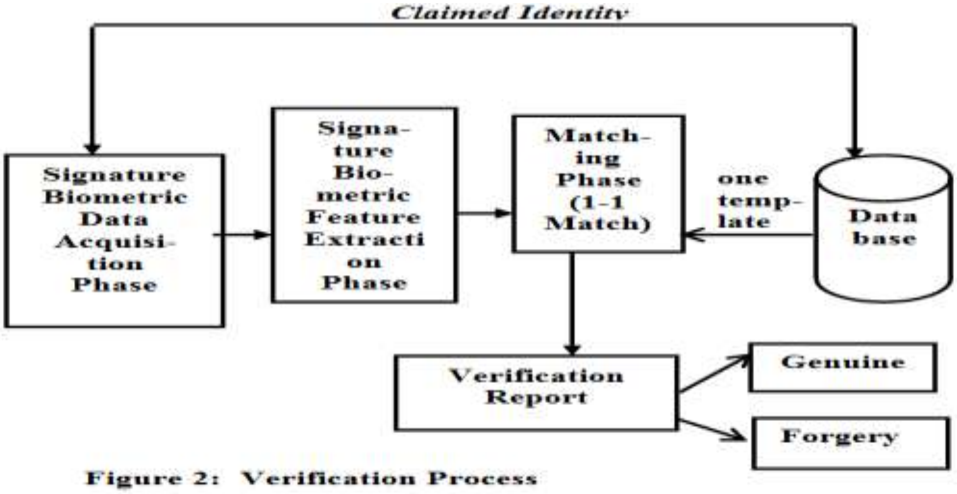

Claimed Identity
Signature Biometric Data Acquisition Phase
Signature Biometric Feature Extraction Phase
Matching Phase (1-1 Match)
one template
Data base
Verification Report
Genuine
Forgery

Figure 2: Verification Process

This method is mostly used for access monitoring because it has low processing time. False Reject and False match errors are errors mostly encountered with verification.

In the case of verification (1:1), a removable storage like a contact or contactless smart card can be used; and the storage unit will be part of the server station in case of the client-server system. The biometric database used for identification must be a big central data base holding all the records of people known to the biometric system. It must be flexibly large enough to accommodate the 'n' number of biometric identities. Therefore, it requires large amount of processing time and power. The cost of a biometric verification database is much lower than that of a biometric identification. Results are generated more quickly and accurately with verification databases than identification databases, even when the size of the verification database increases [1].

4.2 Signature Biometric System

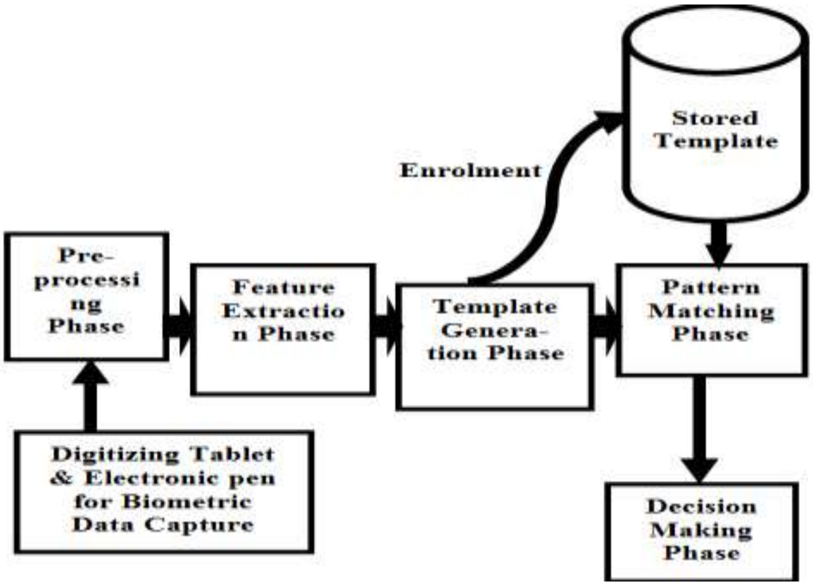
The following modules or processes are involved in a signature biometric system: Biometric Sensor for Data Capture, Pre-processing Phase, Feature Extraction Phase, Template Generation Phase, Template storage, Pattern Matching Phase, and Decision Making Phase, as shown in fig. 3.

Dynamic signature verification methods can be grouped into two main processes: (a) Important signals such as the pressure, velocity, position, acceleration vs time are regarded as mathematical time functions where the values directly constitute the feature set. (b) In the second group, the techniques refer to several parameters as features. These parameters are computed from the measured signals. The global and local information can be taken into account either implicitly or explicitly. These information may be handled either jointly or separately.

In a dynamic signature verification, the following should be considered:

i)**Signature Aspect Ratio:-** This calculates the height and the width of the signature which is represented by the size of the signature on Y-axis and X-axis respectively. The signer must ensure that he signs the same number of strokes and ensure uniformity in size.

ii)**Number of strokes:-** This constitutes the sum total of all the lines used in the entire signature. It starts counting the moment the signer puts down his pen until he lifts it up i.e. finishes signing (pen-up).



Fig,3: A Signature Biometric System

iii)**Number of Pen-ups:** This is the number of times a signer picks up a pen during signing a signature. This excludes the last lifting of pen which marks the end of signing.
iv)**Signing Time:-** This captures the time it takes a signer to sign his signature in milliseconds.
v)**Time-down ratio:-** This is total number of time, the pen comes in contact with the signing surface.
vi)**Time-up ratio:-** This is the opposite of Time-down ratio which shows the time duration in which the pen was isolated from the signing area. This is one of the important features used in verification algorithm which is used to distinguish between two opposing features and actuates the obtaining of a more stable characteristic of a person.
vii)**Signature speed:-** This is the sum of the total length of the signature and the time in which the pen was in direct contact with the signing area. It gives the signing speed expressed in pixels per millisecond. This feature, however, may not be static due to the differences in the physical and mental condition of a person.
viii)Velocity along the x-axis: This feature represents speed expressed in number of pixels per millisecond, which indicates how quickly people sign if only the x coordinate is considered in the system. It calculates the total length which pen passed along the x-axis and is divided by the total time in which the pen was lowered to the signing area. This feature depends on the physical and mental condition of the person and is often used less than other characteristics.
ix)Velocity along the y-axis: Here the feature represents speed expressed in number of pixels per millisecond, which indicates how quickly people sign if only the ycoordinate is considered in the system. It calculates the total length which pen passed along the y-axis and is divided by the total time in which the means for writing was lowered to the signing area. This feature depends on the physical and mental condition of the person and is often used less than other characteristics.
x)Average pressure: This feature is obtained by monitoring the level of pressure which pen leaves on the signing area. In order to obtain the average pressure it is necessary to add up all levels of the received pressure to one variable and divideby the total number of packages. The biggest influence on this characteristic has signers body.
xi)Strongest pressure moment: This feature can be characterized as the only local characteristics of signatures which can be global as it is unique in the entiresignature. In order to extract this feature, monitoring the level of pressure whichpen leaves on the signing area is needed. The highest level is observed and thetime of its creation is recorded. It is assumed that the signature always has nearly the same moment of the strongest pressure.

xii)Speed: When a signature is captured with a digitizer, the pen motions (dynamics) are recorded. According to Zimmerman et al., when signing, the hand can operate in a rule known as ballistic movement, where the muscles are not controlled by sensual feedback. Ballistic motions are usually fast, practicedmotions whose accurateness rises with speed [22]. In the on-line signature there isa significant feature that can be extracted, which is the speed of the signature.During the signing process, the speed of the pen ball is changing at every point of the signature. These changes are repeated in a fixed way every time a person signsagain. To find out the speed of the signature it is needed to record the time at

which a specific point is sampled. Here,
Speed = Distance/Time (1)
xiii)Acceleration: Acceleration produced by pen movements while one is writing orsigning provide useful information for handwriting research, particularly forapplications like automatic signature verification. Measurement of penacceleration is usually done with accelerometers integrated into a pen or withdevices that either derive pen acceleration from other physical measures or sensephysical quantities equivalent to pen acceleration. Acceleration signals arecharacterized in terms of phase, amplitude and frequency. This characterization makes possible the extraction from the accelerometer output those signal components relevant to the handwriting process.

4.3 Types of Forgeries

Coetzer et al., identified three different types of forgeries in a signature: Random, Simple and Skilled forgeries[23].
Random forgery: In a random forgery, the forger randomly replicates a person's signature without knowing the person (not even his name) or having any access to his genuine signature.
Simple forgery: In a simple forgery, the forger is already aware of the author's name, but has no access toa sample of the signature.
Skilled forgery: The forger has access to one or more samples of the genuine signature and is able to reproduce it. But based on the various skilled levels of forgeries, it can also be divided into six different subsets.

Nguyen V. et al, shows various levels of skilled forgeries [24] such as:

a) A forged signature can be another person's genuine signature. Justino et al.,categorized this type of forgery as a Random Forgery [25].
b) A forged signature is produced with the knowledge about the genuine writer's name only. Hanmandlu et al., categorized this type as a Random Forgery[26]whereas Justino et al. categorized this type as a Simple Forgery[25]. Weiping et al., categorized this type as a Casual Forgery[27].
c) A forged signature imitating a genuine signature's model reasonably well is
categorized as a Simulated Forgery by Justino et al.,[25].
d) Signatures produced by inexperienced forgers without the knowledge of theirspelling after having observed the genuine specimens closely for some time arecategorized as Unskilled Forgeries by Hanmandlu et al., [26].
e) Signatures produced by forgers after unrestricted practice by non-professionalforgers are categorized as Simple Forgery/Simulated Simple Forgery by Ferrer etal. [28], and a Targeted Forgery by Huang and Yan, [29].
f) Forgeries which are produced by a professional imposter or person who hasexperience in copying Signatures are categorized as Skilled Forgeries byHanmandlu et al., [26].

4.4 Signature Data Acquisition

We obtain a digital signature data signature by using a special pen on an electronic surface.This is an uninterrupted or direct acquisition of a signature image without the intermediate use of paper. Themost conventional online data acquisition devices are digitizing tablets Zimmerman et al., [22]. Electronic pens are also able to detect position, velocity, acceleration, pressure, pen inclination, and writing forces etc.

4.5 Pre-processing

Immediately after signature data acquisition, some pre-processing techniques are applied. Noises are inevitably present during biometric data capture. Pre-processing refers to the process of preparing the input signature image to be ready for the next step of the system by removing noises and enhancing the signature rigid patterns. This produces a good enough quality of output signature image[Benson-Emenike&Nwachukwu, [1]. Pre-processing ensures that the desired data is fed to the feature extraction module. Normally,acquired signature images are of different formats and resolutions and need to beprocessed to enable accurate feature extraction. The acquired images may containunexpected marks, stains, or noise which would cause negative effects on the recognition accuracy. We adopt a Pre-processing method known as Plainarised Region Of Interest **[**PROI], as shown in fig. 4. This method involves some processes that eliminatenoise and convert signature images to a suitable format for feature extraction. The PROI pre-processing algorithms for dynamic signature verification involves the following processes: Signature Size Normalization, Thinning, Denoising and Filtering, Binarization, and Width Normalisation.

Signature Size Normalization: Signature image normalisation is performed once they are captured, this gives a basis for further denoising and processing activities. This is necessitated by the fact that acquired data may have some sensorial and situational incapability. In this work, Normalisation is done using Fourier Transform. Here, the image is divided into small processing blocks of 32 by 32 pixels and then we perform the Fourier Transform on each block according to:

$$\mathrm{Ft}(a,b) = \sum_{i=0}^{K-1}\sum_{j=0}^{L-1} f(i,j) \times \exp\left\{-\,p2\Pi \times \left(\frac{ai}{K} + \frac{bj}{L}\right)\right\} \qquad (2)$$

For a = 0,1,2, … 31, and b = 0,1,2, … 31.

In order to enhance each block by its dominant frequencies, after Fourier Transform, each block is multiplied with its magnitude a set of times, where magnitude can be given as:

$$\mathrm{ABS}\big(\mathrm{Ft}(a,b)\big) = |\mathrm{Ft}(a,b)| \qquad (3)$$

and the enhanced block will be based on:

$$u(i,j) = \mathrm{Ft}^{-1}\{\mathrm{Ft}(a,b) \times |\mathrm{Ft}(a,b)^{r}|\} \qquad (4)$$

Where Ft^{-1} $\{\mathrm{Ft}(u,v)\}$ is given by:

$$\mathrm{Ft}(i,j) = \frac{1}{KL}\sum_{i=0}^{K-1}\sum_{j=0}^{L-1} \mathrm{Ft}(a,b) \times \exp\left\{p2\pi \times \left(\frac{ai}{K} + \frac{bj}{L}\right)\right\} \qquad (5)$$

for i = 0,1,2,…… 31, and for j= 0,1,2,…… 31.

Thinning: This is the transformation of a digital image into a simplified form, but the image should be topologically equivalent. It is a kind of topological skeleton,but computed by means of mathematical morphology operators that are used toremove selected foreground pixels from binary images.

Denoisingand Filtering process: Denoising is a noise removal operation which has no effect on the signature pattern. Image Noise is usually an unwanted random variation observed in the brightness or the color information of an image. Noise could be introduced into an image through unwanted speckles, smears, scratches or other forms of unwanted noise that might thwart feature extraction.Noise causes a wrong conclusion in the verification of images and hence should be removed prior to performing image analysis processes.Thus, median filtering is used to eliminate the existing noises.

Binarization: The process by which the image is converted into black and white iscalled binarization. Here, we adopt a locally adaptive binarization method known as adaptive thresholding. This involves the conversion of the gray level to 0 if it is below threshold value and to 1 if it is above threshold value. The threshold value is the mean taken from the gray level of the current block (32*32) to which the pixel belongs. This is given by the equation:

$$\mu ab = \frac{1}{MN}\sum_{y=bN}^{(b+1)N-1}\sum_{x=aM}^{(a+1)M-1} R_n\,(x,y) (6)$$

where µab = mean of region (axb)th sub-image of size (M x N) and Rn (x,y) = original image. The pixel wise binarized image is given by

$$I_{new}\,(b_1\,,b_2)\begin{cases}1 \text{ if} I_{old}\,(b_1\,,b_2) \geq \mu_{ab} \\ 0 \qquad \text{otherwise}\end{cases} \qquad (7)$$

Width normalization: All signature images have to be reduced to a standard size soas to ease the process of feature extraction.

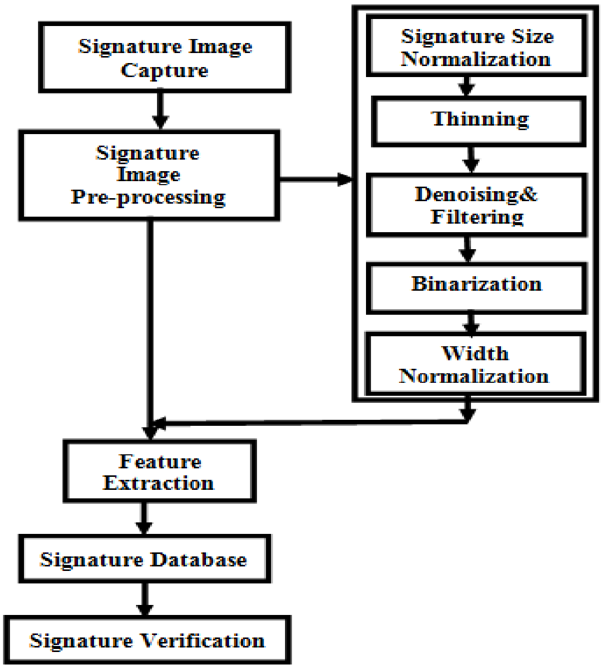


Fig. 4: Signature Image Capture, Pre-Processing Using PROI method and Verification.

4.6 Feature Extraction Techniques

Feature Extraction is an important part of any pattern recognition system. The process in which digital information is modified, simplified, combined so that the salient information can be classified, is called feature extraction Plamondon and Lovette[35]. To be successful, a feature extraction technique should be justifiable using rules that govern the formation of the class of pattern being considered. As features are refined as inputs for the learning process and the decision process, feature extraction techniques are crucial to the success of the whole process of automated pattern recognition [71]. Good features are those that enable the system to identify a pattern's class with the least amount of errors. Baltzakis and Papamarkos commented that the selection of features must be appropriate for the application and the approach [31]. Klement et al.summarized the three requirements that concerned the feature selection process [32] such as: (i) Speciality (minimizing intra-class variability and maximizing inter-class variability); (ii) Universality (can be applied to any writer); (iii) Environmental independence (with respect to writing instruments and materials).

In other words, it is essential that a feature extraction technique could minimize or even eliminate the negative effects from variations such as rotation, shift, or dilation of the pattern being considered. In general, two types of features can be considered for signature verification: i. parameter-based features ii. function-based features. In the case of function-based features, Congedo et al, signatures are usually characterized in terms of a time function and the values of the time function constitute the feature set [33]. Conversely, when parameter features Lee et al., [34]are considered, the signatures are characterized as a vector of elements; each one represents the value of a feature. It has been shown by Plamondon and Lorette[35]that function features generally provide better performance as compared to parameter features, but they usually need time-consuming procedures for matching. In addition, parameters are generally grouped into two main categories: i. global parameters and ii. local parameters. The whole signature is considered for global parameters. Usual global parameters are total time duration of a signature, number of pen ups and downs, number of components, global orientation of the signature, etc. Local parameters concern features extracted from a few exact parts of the signature.

When features are extracted, they are used to generate a feature vector. In computer vision and image processing the concept of feature is used to denote a piece of information which is relevant for solving the computational task related to a certain application. A feature vector is an n-dimensional vector of numerical featuresthat represent some object [36]. It consists of mainly two steps, pre-processing and feature extraction. As previously mentioned, pre-processing is performed on the signature images from a database so as to prepare it for the process of feature extraction and to ensure that all the signature images are of the same dimensions so that it is easier and convenient to extract the features.

V. CONCLUSION

There are numerous problems associated with traditional methods of verification such as one could forget, misplace, lose or steal tokens, since they are not based on natural traits. They cannot be adequately used to distinguish between an authorized person and an impostor hence guarantees insufficient security demands. The use of biometrics in identification or authentication has been proved to be stronger, more secure and dependable. Therefore, our handwritten dynamic signature biometric verification using Plainarised Region Of Interest [PROI] method is the answer to all these limiting factors in the area of signature verification.

REFERENCES

[1]. M. E. Benson-Emenike and E. O.Nwachukwu,An Efficient Image Preprocessing In An Improved Intelligent Multi Biometric Authentication System. International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 9 – No.6, September 2015 – www.ijais.org

[2]. B. Miller, Vital signs of identity. IEEE spectrum. 2004, 31(2): 22-30.

[3]. A. K. Jain, , R.Bolle, S. Pankanti, A. A. Ross, and K. Nandakumar,Introduction to Biometric.Springer.IEEE Spectrum, 2011, 22-27.

[4]. R. Chellappa, C. L. Wilson, and S. Sirohey, Human and machine recognition of faces: a survey, Proc. IEEE 83(5): 1995, 704-740.

[5]. R. A.Virginia, Iris-based automatic recognition system based of SIFT features, MSc Thesis, Universidad Autónoma de Madrid Escuelapolitécnica superior, 2010.

[6]. A.K. Jain, L. Hong, and R. Bolle, Online fingerprint verification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1997, 302-313.

[7]. N.K. Ratha, Privacy protection in high security biometrics applications. In: Ethics and Policy of Biometrics: Lecture Notes in Computer Science #6005, 62–69. Springer-Verlag Berlin Heidelberg, 2010.

[8]. Y. Bulator, S. Jambawalikar, P. Kumar, and S. Sethia,Hand recognition using geometric classifiers.In proceedings of the ICBA, Hong Kong, China, 2004, 753-759.

[9]. Q. Zhang, andH. Yan, Fingerprint classification based on extraction and analysis of singularities and pseudo ridges. Pattern Recognition, 2004, 37 (11): 2233-2243.

[10]. A. Iannarelli,Ear identification.Paramount publishing Company, 1989.

[11]. A. Bromme, "A Classification of Biometric Signatures" International Conferenceon Multimedia and Expo, ICME, pp. 17-20, 2003.

[12]. C. Rabasse, R.M.Guest and M.C. Fairhurst, "A Method for the Synthesis of DynamicBiometric Signature Data", Ninth International Conference on Document Analysis andRecognition, pp.168-172, 2007.

[13]. D. Y.Yeung, H. Chang, Y.Xiong, S. George, R.Kashi, T.Matsumoto and G.Rigoll, "SVC2004: First International Signature VerificationCompetition", Proceedings of the International Conference on Biometric Authentication, Hong Kong, 15-17 July 2004.

[14]. C. V.Pascual, A. S.Hurtado, E. M. Martinez and J. M. P. Gaspar, " A New Proposal for Score Normalization in BiometricSignature Recognition Based on Client Threshold Prediction", International Conference on Data Mining, 2012, pp.1128-1133.

[15]. D. R. S. Kumar, R. R. Kumar, K. B. Raja, R. K. Chhotaray, S.Pattanaik, " Biometric Security System Based on Signature Verification Using NeuralNetworks", 2010, pp. 580-583.

[16]. E.Maiorana, P.Campisi, A. Neri, "Biometric Signature Authentication using Radon Transform-based Watermarking Techniques" , Biometrics Symposium, pp 1-6, 2007.

[17]. E.Maiorana, P.Campisi and A.Neri, "Bioconvolving:Cancelable Templates for a Multi-Biometrics Signature Recognition System",International Systems Conference on Digital Object Identifier, pp. 495500, 2011.

[18]. E.Maiorana, P.Campisi, J. Ortega-Garcia and A. Neri, "Cancelable Biometrics for HMM-based Signature Recognition", InternationalConference on Biometrics, Theory, Applications and Systems, pp. 1-6, 2008.

[19]. K. B. Nagasundara, S. Manjunath and D. S. Guru, "Multimodal Biometric System basedon Hand Geometry, Palmprint and Signature" , 5th ACM Computer Conference:Intelligent & scalable system technologies, Article No. 4. 2012.

[20]. Mhatre and Maniroja, "Offline Signature Verification Based on Statistical Features",International Conference and WorkshoponEmergingTrendsinTechnology,pp.59-62,Mumbai,India.

[21]. E.Maiorana, P.Campisi, J.Fierrez, J. Ortega Garcia, andAlessandro Neri, “Cancelable Templates for Sequence-based Biometrics withApplication to On-line Signature Recognition”, IEEE Transactions on Systems, Man,and Cybernetics, part a: Systems and Humans, vol. 40, no. 3, pp. 525-537, 2010

[22]. T. G. Zimmerman, G. F. Russell, A. Heilper, B. A. Smith, J. Hu, D. Markman, J. E.Graham and C. Drews, “Retail Applications of Signature Verification”, Proceedings ofSPIE, Vol. 5404, pp. 206-214, 2004.

[23]. J. Coetzer, B. Herbst, J. D. Preez, “Off-line Signature Verification using the DiscreteRadon Transform and a Hidden Markov Model. EURASIP Journal on Applied SignalProcessing”, 4, pp. 559–571, 2004.

[24]. E. J. R. Justino, F. Bortolozzi and R. Sabourin, “A Comparison of SVM and HMMClassifiers in the Off-line Signature Verification”, Pattern Recognition Letters2005;26(9):pp.1377–1385, 2005.

[25]. M. Hanmandlu, M. H. M. Yusof, V.K. Madasu, “ Off-line Signature Verification andForgery Detection using Fuzzy Modelling”, Pattern Recognition Letters;38(3):341–356, 2005.

[26]. H. Weiping, Y. Xiufen and W. Kejun, “A Survey of Off-line Signature Verification”, Inproc. International Conference on Intelligent Mechatronics and Automation, pp. 536–541. 2004.

[27]. M. Ferrer, J. Alonso, C. Travieso, “Off-line Geometric Parameters for AutomaticSignature Verification using Fixed-point Arithmetic”, Pattern Analysis and MachineIntelligence, 27(6), pp. 993–997, 2005.

[28]. J. Ortega-Garcia, J. Gonzalez-Rodriguez, A. Simon-Zorita and S. Cruz-Llanas, “ FromBiometrics Technology to Applications Regarding Face, Voice, Signature andFingerprint Recognition Systems”, In: Biometric Solutions for Authentication. 2002.

[29]. N. Papamarkos and H. Baltzakis, “Off-line Signature Verification using MultipleNeural Network Classification Structures. In: 13th International Conference on DigitalSignal Processing Proceedings. 1997, pp. 727–730.

[30]. V. Klement, K. Steinke and R. Naske, “The Application of Image Processing and Pattern Recognition Techniques to the Forensic Analysis of Handwriting”, International Conference on Security through Science Engineering, 1980.

[31]. G. Congedo, G. Dimauro, A. M. Forte, S. Impedovo and G. Pirlo, “Selecting ReferenceSignatures for On-line Signature Verification”, International Conference on ImageAnalysis and Processing, pp. 521–526, 1995.

[32]. J. Lee, H. S. Yoon, J. Soh, B. T. Chun, Y. K. Chung, “Using Geometric Extrema forSegment-to-segment Characteristics Comparison in Online Signature Verification”,Pattern Recognition, 37(1), pp. 93–103, 2004.

[33]. R. Plamondon, G. Lorette, “Automatic Signature Verification and Writer Identificationthe State of the Art”, Pattern Recognition, 22(2), pp.107– 131, 1989.

[34]. V. S.Inamdar , P. P. Rege and M. S.Arya, “Offline HandwrittenSignature based Blind Biometric Watermarking and Authentication Technique usingBiorthogonal Wavelet Transform” , International Journal of Computer Applicationsvolume 11– No.1, pp. 0975 – 8887, 2010.

Benson-Emenike "Handwritten Dynamic Signature Biometric Verification Using Plainarised Region of Interest [Proi] Method "The International Journal of Engineering and Science (IJES) 7.7 (2018): 56-66