Signature-based Biometric Authentication

Srikanta Pal[1], Umapada Pal[2] and Michael Blumenstein[1]
[1]School of Information and Communication Technology,
Griffith University, Gold Coast, Australia.
[2]CVPRU, Indian Statistical Institute, Kolkata, India.
Email: srikanta.pal@griffithuni.edu.au

Abstract

In a modern, civilized and advanced society, reliable authentication and authorization of individuals are becoming more essential tasks in several aspects of daily activities and as well as many different important applications such as in financial transactions, access control, travel and immigration, healthcare etc. In some situations, when individual equipment is required for confirmation of one's identity to other groups of people in order to make use of services or to achieve access to physical places, it is always necessary to declare self-identity and to prove the claim. Traditional authentication methods, which are based on knowledge (password-based authentication) or the utility of a token (photo ID cards, magnetic strip cards and key-based authentication), are less reliable because of loss, forgetfulness and theft.

These issues direct substantial attention towards biometrics as an alternative method for person authentication and identification. The word 'biometric' has been derived from the Greek words "Bio-metriks", "Bio" which means life and "metriks" which means measures. Therefore a biometric is the measurement and statistical analysis of unchanging biological characteristics. Biometrics evaluate a person's unique physical or behavioural traits to authenticate their identity. As biometric identifiers are unique to persons, they are more reliable in verifying identity than token-based and knowledge-based methods. In the last few years, substantial efforts have been devoted to the development of biometric-based authentication systems. Biometrics provide an expected and successful solution to the authentication problem, as it offers the construction of systems that can identify individuals by the analysis of their physiological or behavioural characteristics [1]. In fact, the field of biometrics is the science of using digital technologies and the intention of biometric systems is to perform the recognition or authentication of people based on some biological characteristics that are intrinsically unique for each individual. The effectiveness of a biometric system is measured mainly by the distinguishing attributes that are used to verify the identity. A large number of biometric traits have been investigated and some of them are nowadays used in several applications. Common physical traits include fingerprints, ear, hand or palm geometry, vein, retina, iris and facial characteristics [2]. Behavioural traits include voice, signature, keystroke pattern and gait.

A biometric scheme can either verify or identify the authentication of an individual. In verification mode, it authenticates the person's identity on the basis of his/her claimed identity. In identification mode, it establishes the person's identity (among those enrolled in a database) without the subjects having to claim their identity [3]. Among all other biometric traits, signature verification occupies an important and a very special place in the field of biometrics.

1. Overview of Biometric Traits and Technologies

Biometric systems are a constantly growing technology, which have been widely used in many official and commercial identification applications. A biometric method is essentially a pattern recognition system which makes a personal identification decision by determining the authority of specific physiological or behavioural traits [4]. Nowadays a large number of biometric traits have been investigated and some of them are used in several applications. The diagram of a generic biometric system as specified in [39] is shown in Figure 1.

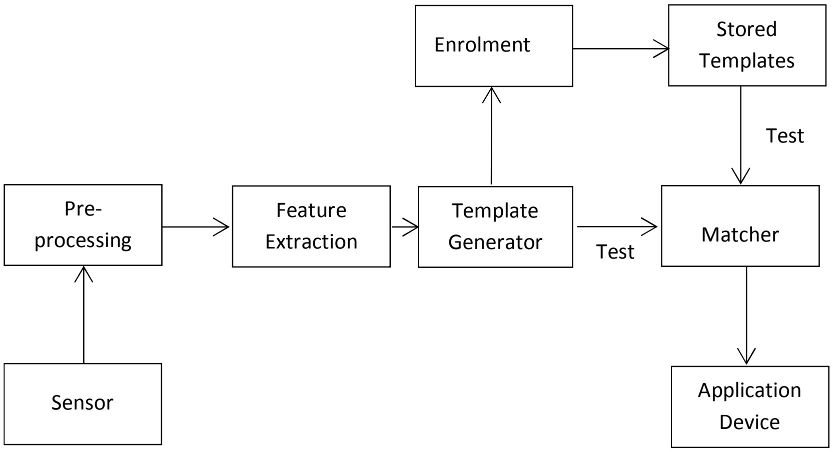

Figure1. A Generic Biometric System

Each biometric technology has its strengths and limitations. It is not expected that one biometric trait will efficiently fulfil the needs of all the applications. The match between a specific biometric and an application is determined depending upon the requirements of the application and the properties of the biometric characteristic. A number of biometric characteristics have been in use for different applications [5]. Each biometric characteristic has its effectiveness and disadvantages, and the choice depends on the specific application. No single biometric is expected to successfully meet all of the requirements (e.g., accuracy, practicality, and cost) of all applications (e.g., digital right management, access control, and welfare distribution) [6]. In other words, no biometric is “optimal” although a number of them are “admissible.” The suitability of a specific biometric for a particular application is determined depending upon the requirements of the application and the properties of the biometric characteristic. A large number of biometric traits have been explored and a brief description of some important and commonly used biometric traits is discussed as follows. Examples of different biometric characteristics are shown in Figure 2.

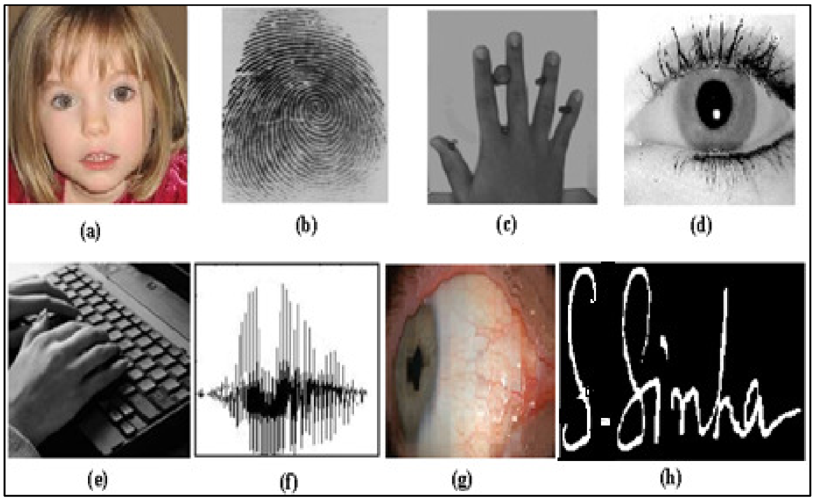

Figure2. Examples of Some Biometric Characteristics: (a) Face, (b) Fingerprint, (c) Hand geometry, (d) Iris, (e) Keystroke, (f) Voice, (g) Sclera, (h) Signature.

- Face recognition investigates facial characteristics, and facial images are one of the common biometric characteristics to undertake personal recognition. A facial recognition method is an application of computer for automatically identifying or verifying a person from a digital image. A face recognition scheme generally consists of four modules: face detection and tracking, facial feature finding, face representation, and matching [7]. In a research by Jain et al. [10], authors have indicated that the applications of facial recognition range from a static, controlled authentication to a dynamic, uncontrolled face identification process. The face recognition approaches [8] are usually based on either: (a) the position and shape of facial characteristics (eyes, eyelid, eyebrows, nose, lips, and chin and their spatial relationships) or (b) the investigation of the face image samples. The main objective of face recognition system is security related, but there are some kind of applications related to personal use, convenience and productivity enhancement.
- The pattern of ridges and valleys on the surface of a fingertip are considered as fingerprint. Fingerprints are one of the forms of biometric applied to recognize

individuals and verify their identity. Fingerprints recognition system is one the most common biometric authentication systems. Fingerprints remain constant throughout life of a person and it has been used by human for personal identification for many decades [9]. Over the last few decades in the field of biometric authentication, no two fingerprints have ever been detected to be similar, not even those of identical twins. According to Jain et al. [10] fingerprint recognition or fingerprint authentication refers to the automated technique of verifying a match between two individual fingerprints [10]. Comparison of several features of the print pattern is generally required for the analysis of fingerprints matching. Three basic patterns of fingerprint ridges are the arch, loop, and whirl. Arch: The ridges enter from a side of the finger, move towards the centre making an arc, and then exit the other part of the finger. Loop: The ridges come from one side of a finger, create a curve, and then exit on that same side. Whirl: Ridges create circularly around a central point on the finger.

- Hand geometry is a biometric that uses the geometric shape of the hand with its shape, size of palm, and lengths, widths of the fingers [11] for authenticating a user's identity. This biometric offers a good balance of performance characteristics and is comparatively easy to use. It might be appropriate where there are more users or where users access the system infrequently and are perhaps less disciplined in their approach to the system. Environmental factors, such as dry weather or personal anomalies such as dry skin, do not provide to have any negative effects on the authentication accuracy of hand geometry-based methods. The geometry of the hand is not known to be very unique and hand geometry-based recognition systems cannot be scaled up for techniques requiring identification of an individual from a huge population. Hand geometry information may not be constant during the period of growth of children. In addition, a person’s adornments (e.g., rings) may pose further challenges in extracting the correct hand geometry information.
- An iris scan presents an investigation of the rings, furrows and freckles in the coloured ring of the eye. The iris is the annular area of the eye surrounded by the pupil and the sclera (white of the eye) on either side. Iris-based biometrics, involve analysing features found in the coloured ring of tissue that surrounds the pupil. The iris patterns are formed six months after birth and become stable after about one year. After that, the patterns remain unchanged for life. The complex iris texture carries very unique information which is useful for personal recognition [12]. Each iris is supposed to be unique and, like fingerprints, even the irises of identical twins are expected to be different. It is very hard to surgically tamper the texture of the iris. Although the early iris-based recognition systems required considerable user participation and were expensive, the new methods have become more accessible and cost-effective. Iris biometrics work with glasses

and contact lenses in place and are one of the few devices that can work well in identification mode.

- Retina-based biometrics involve analysing the coating of blood vessels located at the back part of the eye. A recognized technology, this technique involves using a low-intensity light source through an optical coupler to scan the unique patterns of the retina [13]. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point. This is not convenient if glasses are used or concerned about having close contact with the reading device. For these argues, retinal scanning is not well accepted by all users.
- Voice is a combination of physical and behavioural biometrics. Voice authentication is not based on voice recognition but on voice-to-print authentication, where advanced technology converts voice into text. Voice biometrics has a good potential for growth; because it needs no new hardware as most PCs already contain a microphone. According to J. P. Campbell [14], features of a person's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are employed in the synthesis of the sound. These physical features of human speech are invariant for an individual, but the behavioural part of the speech of a person changes over time due to age, health conditions (such as cold), emotional state, etc. [14]. Voice is also not very distinctive and may not be appropriate for large-scale identification.
- It is hypothesized that each person types on a keyboard in a characteristic way. This behavioural biometric is not expected to be unique to each individual but it is expected to offer sufficient discriminatory information that permits identity verification [15]. Keystroke dynamics is a behavioural biometric; for some persons, one may expect to detect huge variations in typical typing patterns. Moreover, the keystrokes of an individual using a system could be monitored unobtrusively as that person is keying in information. However, this biometric allows 'continuous verification' of an individual over a period of time.
- Among the various biometric techniques, sclera recognition is considered as one of the important traits. As the sclera area is a highly-protected portion of the eye, it is very difficult to spoof. Identification of a person by the vessel patterns of the sclera is possible because firstly, these patterns possess a high degree of randomness, which is never the same for any two individuals, even for identical twins and this makes it ideal for personal identification. Secondly, the patterns remain stable throughout a person's lifetime [16], these patterns even differ for the right and the left eye of the same individual. Additionally this trait can be easily combined with iris biometrics. It is interesting to note that humans are the only mammals with extensive exposed sclera, which is amenable to imaging of the encompassing conjunctival vasculature. The various challenges in sclera recognition include accurate segmentation of the sclera area, sclera vessel enhancement and the extraction of discriminative features of the sclera vessel

pattern for authentication and identification purposes. The task becomes more difficult, as frequently a complete sclera image is not obtained but it is occluded by portions of the eyelid and eyelashes. Moreover different lighting conditions can change the appearance of the texture patterns by accentuating and attenuating various grey tones. Also, the authentication system should work in real-time so that extraction, representation and comparison of texture images should not consume large computational resources. After that, a classification system uses the mathematical model of the sclera texture to compare with other sclera images to identify specific individuals or identify an individual.

2. Signature Biometrics

For security and control in recognition of human identity, most biometric identifiers require a special type of device/equipment or sensor system. However, biometric authentication using signatures can be realized with no additional sensor except a pen and a piece of paper. Nakanishi et al. [17] have shown that every human being has limited biometrics and if the biometric data are leaked out or accessed inadvertently, and the identity of the person whose biometrics they belong to is disclosed, they can never be used for authentication again. So, to deal with this problem, cancellable biometric techniques have been introduced. Among various biometric modalities, only the signature is considered cancellable from a viewpoint of spoofing [17]. Even if a signature shape is known by others, it is possible to cope with the problem by changing the shape. Among all of the biometric authentication systems that have been proposed and implemented, automatic handwritten signatures are considered as the most legally and socially accepted attributes for personal identification. The most challenging aspect in the automation of signature-based authentication is the need for obtaining high accuracy results in order to avoid false authorization or rejections.

Handwritten signature authentication is based on systems for signature verification and signature identification. Whether the given signature belongs to a particular person or not is decided through a signature identification system, whereas the signature verification system decides if a given signature belongs to a claimed person or not. Signature-based authentication can be either static or dynamic. In the static mode (referred to as off-line), only the digital image of the signature is available. In the dynamic mode, also called “on-line”, signatures are acquired by means of a graphic tablet or a pen-sensitive computer display.

A signature is a biometric attribute created by a complex process originating in the signer’s brain as a motor control “program”, implemented through the neuromuscular system and left on the writing surface by a handwriting device [18]. Consequently, signature-based identification and verification is also considered as an important authentication technique among all of the most popular biometric-based authentication methods in the area of personal identification.

A signature also has a high legal value, since it has always played a role in document authentication and it is accepted both by governmental institutions and for commercial transactions as a mean of identification. Moreover, contrary to the majority of other biometrics, a signature can be reissued, in the sense that, if compromised, with a certain degree of effort the user can change his signature. On the other hand, it can be influenced by physical and emotional conditions and it exhibits a significant variability that must be taken into account in the authentication process.

Signature verification analyses the way a user signs his/her name [19]. Signing features such as speed, acceleration, velocity, and pressure are as important as the completed signature's static shape. Signature based authentication enjoys a synergy with existing processes that other biometric based authentication methods do not. People are generally used to signatures as a means of transaction-related identity authentication. Signature verification devices are reasonably accurate in operation and obviously lend themselves to applications where a signature is an accepted personal identifier. Remarkably, comparatively limited significant signature applications have emerged compared with other biometric methodologies.

Of the many possible biometrics available, the handwritten signature perhaps has the longest history, and is the best established biometric mechanism both for identity, cheque and transaction authorisation, and is the most widely accepted by the general public [20]. In many practical situations there are advantages in using the simple handwritten signature as a means of confirming identity and authorising system access, yet signatures are notoriously variable and difficult to characterise uniquely, are also prone to forgery and misuse, and the technological challenges presented by automatic signature verification are significant [21].

Signature based biometrics authentication is widely used in forensic applications. The goal of forensic study is that of determining whether observed evidence can be attributed to an individual. The main aim of signature based biometric authentication with forensic application is the prevention of crime.

Jain and Ross [22] have shown that an inherent advantage of a signature-based biometric system is that the signature has been established as an acceptable form of personal identification method and can be incorporated transparently into the existing business processes requiring signatures such as credit card transactions. A block diagram of a generic signature authentication system is shown in Figure 3. This figure follows the classical signature verification model steps, that is, data acquisition, pre-processing, feature extraction, comparison (which is usually called 'verification' in the signature identification and verification field) and performance evaluation.

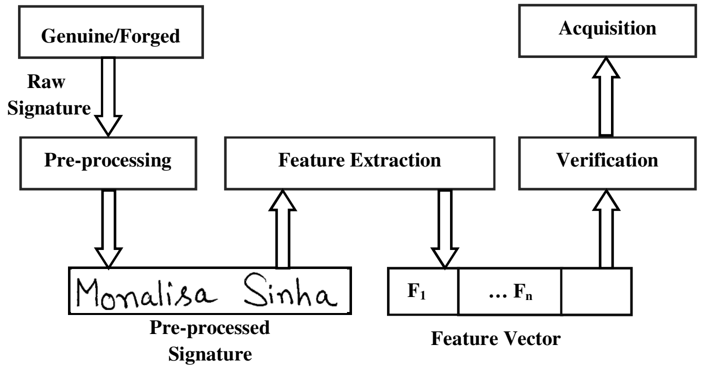

Figure3. Block Diagram of an Automatic Signature Verification System

3. Signature Verification Concept

Pattern recognition is one of the most important and active fields of research. During the past few decades, there has been a considerable growth of interest in problems of pattern recognition. In the last few years many methods have been developed in the area of pattern recognition.

Signature verification is a significant area of study in the field of pattern recognition. Many techniques of verification have been built up specifically to address the off-line signature verification problem. In general, to deal with the problem of off-line signature verification, researchers have investigated a commonly used approach which is based on analysing two different patterns of classes, class 1 and class 2, where class 1 represents the genuine signature set, and class 2 represents the forged signature set. When the performance of the off-line signature verification system is calculated, usually two types of errors [23] are considered: the False Rejection, which is called a Type-1 error and the False Acceptance, which is called a Type-2 error. Hence, there are two types of error rates: False Rejection Rate (FRR) which is the percentage of genuine signatures treated as forgeries, and False Acceptance Rate (FAR) which is the percentage of forged signatures treated as genuine. The Average Error rate (AER) is the average of FAR and FRR. When we deal with the experiments of a system, we must make a trade-off between FRR and FAR based on the application and other aspects of where and how the system is used. Conversely, if the decision threshold of a system is set to have the percentage of false rejections approximately equal to the percentage of false acceptances, the Equal Error Rate (EER) is calculated. During the enrolment phase, the input signatures are processed and their personal features are extracted and stored into the knowledge base. During the classification phase, personal/salient features extracted from an accepted signature are compared against the information in the knowledge base, in order to judge the authenticity of the applied signature.

According to Ismail et al. [24], an automatic signature verification system should meet the following requirements:

- Reliability: The forgeries should be rejected and the genuine signatures should be accepted if there is adequate distinction between the input samples and the original patterns.
- Adaptability: Genuine signatures should be accepted even with slight variations
- Practicality: It is possible to implement such systems in real-time.

4. Multi-script Signature Verification Concept

Although significant research has already been undertaken in the field of signature-based authentication, particularly when single-script signatures are considered, however conversely, less attention has been devoted to the task of multi-script signature-based authentication. In the signature-based personal identification and verification area, introduction of multi-script challenges is a very recent concept and a novel scheme.

As a multi-script and multi-lingual country, India doesn't have the concept of a single language. The country has a set of official regional scripts and languages recognized for some of its individual states for official communications. There are ten major scripts in India for the documentation of its official languages. They are Devanagari, Bangla, Gurumukhi, Guajarati, Oriya, Kannada, Telugu, Tamil, Malayalam and Urdu (Nastaliq). Most of the Indian scripts have originated from an ancient script called Brahmi through various transformations [25]. Devanagari script is being used for writing many languages namely Hindi, Marathi, Nepali, Sanskrit, Konkani, Maithili, Santali, Sindhi, and Kashmiri. Hindi, written in Devanagari script, is the national language of India.

When a country deals with two or more scripts and languages for reading and writing purposes, it is known as a multi-script and multi-lingual country. Multilingualism is a widespread phenomenon as there exist more than 6500 languages around the world. Most countries have only a single language but very few countries have more than one script for reading and writing purposes. In India, there are officially 23 (Indian constitution accepted) languages and 11 different scripts. In such a multi-script and multi-lingual country like India, languages are not only used for writing/reading purposes but also applied for reasons pertaining to signing and signatures. In such an environment in India, the signatures of an individual with more than one language (regional language and international language) are essentially needed in official transactions (e.g. in a passport application form, an examination question paper, a money order form, bank account application form etc.). To deal with these situations, signature verification techniques employing single-script signatures are not sufficient for consideration. Consequently in a multi-lingual and multi-script scenario, signature verification methods considering more than one script are in great demand.

Development of a general multi-script signature-based authentication system, which can verify the identity of people using signatures of all scripts, is very complicated and it is not possible to develop such a method in the Indian scenario. The verification accuracy in such multi-script signature environments will not be desirable compared to single script signature verification. To achieve the necessary accuracy for multi-script signature authentication, it is first important to identify signatures based on the type of script and then use individual single script signature verification for the identified signature script.

India is a union of 29 states and most of the regions use three different languages (international language, national language and regional language). West Bengal is a state where Bangla (local language), Hindi as a national language and English as an international language are generally used for official transactions. A generic multi-script signature verification system considering these three different scripts of signatures (Bangla, Hindi and English) is shown in Figure 4.

5. Classification of Biometric Signatures

For increasing the reliability of biometric-based authentication methods and systems, different groups of biometric signatures have been undertaken in research and scientific discussion to make the authentication systems more protected.

Arslan Bromme [26] has presented that the usage of biometric signatures within the biometric enrollment, authentication and de-enrollment processes shows mainly two classes of biometric signatures in use for mono-modal biometric processes: i. mono-modal biometric signatures for single biometric signatures and ii. mono-modal biometric templates representing sets/classes of single biometric signatures.

Taking multimodality into account, two more classes of biometric signatures are considered: multi-modal biometric signatures as lists of mono-modal biometric signatures for more than one biometric method used, and multi-modal biometric templates for lists of mono-modal biometric templates.

On the superset level with regard to mono-modal or multi-modal biometric processes for changing environmental conditions or changing biological characteristics (e.g. aging), other high level classes will arise: mono-modal biometric multi-templates for sets of mono-modal biometric templates and multi-modal biometric multi-templates for lists of mono-modal biometric multi-templates.

On the other hand, different combinations of biometric traits have also been taken into account in research to make the authentication systems more secure. Biometric systems using a single biometric trait either for identification or for verification is called a unimodal biometric system [27]. According to Teddy Ko [28] an unimodal biometric authentication system sometimes fails to be accurate enough for the identification of a large user population due to some problems such as noisy dataset,

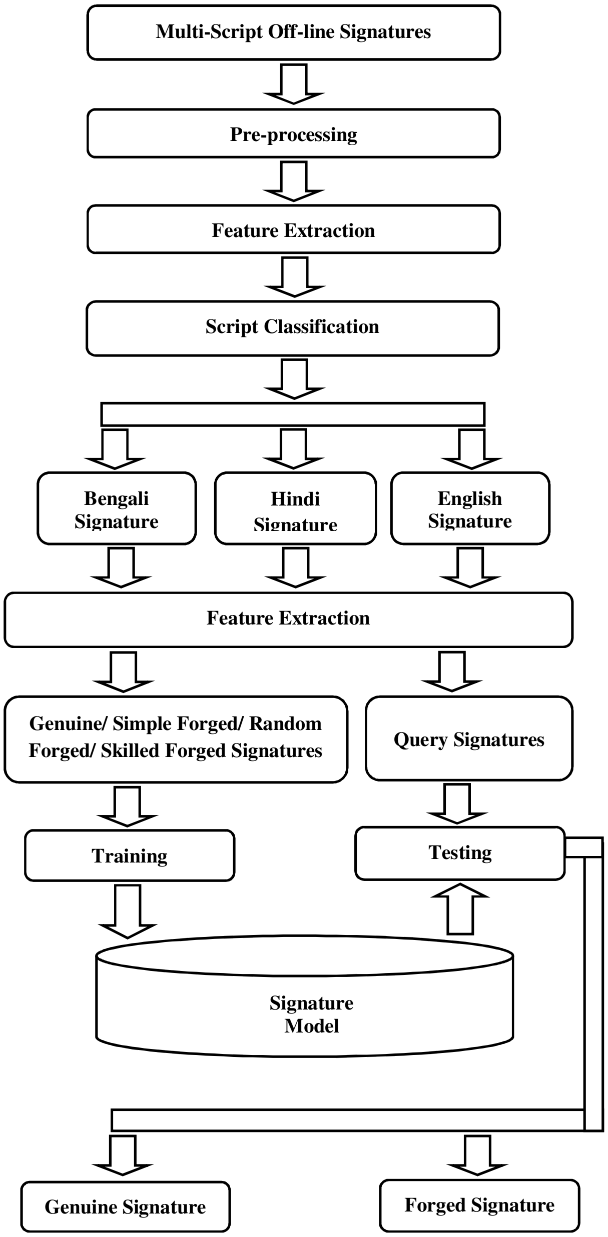

Figure4. Multi-script Signature Verification System

non-universality, limited degrees of freedom, spoof attacks, intra-class variations, and undesirable error rates.

However, no biometric trait is truly universal [29]. Biometric systems based solely on a single biometric may not always meet security requirements. Thus multi-biometric systems are emerging as a trend which helps in overcoming limitations of single biometric solutions. So the problems associated with unimodal biometric systems can be overcome by multimodal biometric systems. A multimodal biometric system unifies the information presented by multiple biometric sources. Multiple biometric sources include multiple sensors, multiple instances, multiple samples, multiple algorithms, or multiple biometric traits [30].

6. Signature Stability

Stability analysis of handwritten signatures is very relevant for automatic signature verification and this is also a very important characteristic for investigating the intrinsic human properties related to the handwriting generation processes concerning human psychology and biophysics. Each handwritten signature strongly depends on a large number of factors such as the psychophysical state of the signer and its social and cultural environment as well as the conditions under which the signature apposition process occurs [31]. In addition, its study can provide new insights for a more accurate treatment of signatures for verification purposes, hence contributing to the design of more effective signature verification systems. For these reasons, it is not surprising that the scientific community has been devoting much effort to the analysis of signature stability.

A lot of approaches estimate signature stability by the analysis of a specific set of characteristics, when dynamic signatures are considered. In general, these approaches have shown that there is a set of features which remain stable over long time periods, while others can change significantly in time [32]. More precisely, a comparative study of the consistency of certain features of dynamic signatures has demonstrated that position, velocity and pen inclination can be considered to be among the most consistent, when a distance-based consistency model is applied [33]. Other results, based on personal entropy, demonstrated that position is a stronger characteristic than pressure and pen inclination in both short and long-term variability. Moreover, although pressure may give better performance results in a short-term context, it is not recommended for signature verification in the long-term.

When static signatures are considered, the degree of stability of each region of a signature can be estimated by a multiple pattern-matching technique [34]. The basic idea is to match corresponding regions of genuine signatures in order to estimate the extent to which they are locally different. A preliminary step is used there to determine the best alignment of the corresponding regions of signatures, in order to diminish any differences among them.

Although stability has been observed in signatures, the signing process does not lend itself to the production of repeatable, perfectly accurate and identical characteristic data issued from successive trials. The only certainty in this domain is that when two signatures are identical and one of them is a forgery, i.e. probably a copy. In fact, a great deal of variability can be observed in signatures, depending on country, age, time, habits, psychological or mental state, physical and practical conditions. Two types of signature variability have to be clearly distinguished: intraclass or intrapersonal variability, i.e. the variation observed within a class of genuine signature specimens of one individual, interclass or interpersonal variability, i.e. differences which exist between genuine signature classes produced by two different writers. In theory, intraclass scatter must be as low as possible and interclass scatter extensive enough to be used for class separation.

The stability comes from the intrinsic properties of rapid human movements that somehow constitute the basic element of each signature [32]. In fact, a number of major psychophysical phenomena have been observed on a regular and consistent basis during the study of these movements. The most remarkable is without doubt what is known as the invariance of velocity profiles. A technique for the analysis of stability in static signature images has been presented by Impedovo et al. [35]. The technique uses an equimass segmentation approach to non-uniformly split signatures into a standard number of areas. Consecutively, a multiple matching technique is adopted to estimate stability of each area, based on cosine similarity.

7. Signature Verification vs. Identification

In the field of automatic signature recognition, two different types of signature recognition systems are considered such as signature verification and signature identification systems. Signature-based biometric technologies are used for either one of those two purposes, verification or identification, and the implementation and selection of the technology and related procedures are closely tied to this aim. Technologies differ in their capabilities and effectiveness in addressing these purposes. Verification (Am I whom I claim I am?) includes confirming or rejecting a person’s demanded identity. In identification, someone has to establish a person's identity (Who am I?). Each one of these approaches has its own complexities and could probably be solved by a signature authentication system. These two examples illustrate the difference between the two primary uses of biometrics: identification and verification.

Signature identification (1:N, one-to-many, recognition): A signature identification system must recognise a signature from a list of N signatures in the template database. The process of determining a person’s identity by performing matches against multiple templates. Identification systems are designed to determine identity based solely on signature information.

Signature Verification (1:1, matching, authentication): A signature verification system simply decides whether a given signature belongs to a claimed signature or not. It is the process of establishing the validity of a claimed identity by comparing a verification template to an enrollment template. Verification needs that an individuality be claimed, after which the individual's enrollment template is located and compared with the verification template. Verification responses the query, 'Am I who I claim to be?'

8. Dynamic and Static Signature Verification

The biomechanical processes involved in the production of the human signature are very complex. In vastly simplified terms, the main excitation is thought to take place in the central nervous system, more specifically in the human brain, with predefined intensity and duration describing the intent of the movement. The signal of the intent (or the movement plan) is passed through the spinal cord to the particular muscles which are activated in the intended order and intensity. As a result of such activation and relaxation of the muscles and whilst holding a pen, the resultant arm movement is recorded in the form of a trail on paper as a handwritten signature.

Based on the handwritten signature data acquisition method, two types of systems for handwritten signature verification can be identified: static (off-line) systems and dynamic (on-line) systems.

8.1 Dynamic Signature Verification

Whenever handwriting is captured as a user writes for the purpose of recognition or analysis, it is called on-line handwriting recognition. This process requires special devices, such as stylus or digitizer pen and tablet, to capture the writing information on-the-fly. The temporal stream of information which is extracted as the writing is produced is called on-line features, which include local pressure, acceleration, speed, number of strokes, and order of strokes. The signature image can be simulated with high accuracy using this temporal-spatial feature information.

Dynamic signature verification system uses a digitizer or an instrumented pen to give a representation of the written signature generating one or several signals which vary with time. The raw data are then pre-processed to remove spurious information, to filter the significant signals and to validate the acquisition process. The next step involves what is referred to as the feature extraction process. Specific and discriminant functions or parameters are computed from the filtered input data and are used to represent a signature.

Dynamic signature verification methods can be classified in two principal groups. In the first group of dynamic signature verification, the techniques deal with functions as features. In this case, the complete signals (i.e. position, pressure, velocity, acceleration vs. time, etc.) are regarded as, mathematical time functions where the values directly constitute the feature set [36]. In the second group of dynamic signature verification, the techniques refer to several parameters as features. These parameters are computed from the measured signals. Both global and local information are either explicitly or implicitly taken into explanation, separately or together.

- Number of strokes: This feature is the total number of lines contained in the entire signature. One line is from the time since the signer put down the pen to the contact surface until it is filed or until pen-up occur.
- Number of pen-ups: This feature shows how many times writer picked up a pen during signing a signature. It should be noted that the last lifting of pen is not counted because it marks the end of the signing.
- Signature aspect ratio: This feature considers the width of the signature (signature size on the x-axis) expressed in pixels of a tablet and normalized on pixels of the screen and the height of a signature (the size of signatures on the y-axis) expressed in the same way that puts them in proportion. The assumption is that the user will sign each time the same in terms of creating a signature in one, two or more lines and that the size of signatures each time will be approximately the same.
- Signing time: Feature expresses the total time needed to get a person to sign, usually in milliseconds, since the beginning of the signing. It is assumed that the time for a trained signature will always be nearly equal.
- Time-down ratio: It describes how much of total signing time the pen was in contact with the singing surface. To a person who has trained signature, this characteristic will be fairly constant because it is directly related to the signing time.
- Time-up ratio: This feature opposite to Time-down ratio, and indicates how long of total signing time a pen was separate from the signature area. This feature is used for authentication algorithm, which may favour one of two opposing feature in relation to represent a more stable signature characteristic of the person.
- Signature speed: This feature is derived from the total length of the signature and the time in which the pen was in direct contact with the signing area. It tells the speed of signing expressed in pixels per millisecond. Trained signature should not have significant differences over the time. However, this feature strongly depends on the physical and mental condition of the person.
- 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.

- 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 y coordinate 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.
- 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 divide by the total number of packages. The biggest influence on this characteristic has signers body.
- 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 entire signature. In order to extract this feature, monitoring the level of pressure which pen leaves on the signing area is needed. The highest level is observed and the time of its creation is recorded. It is assumed that the signature always has nearly the same moment of the strongest pressure.
- Speed: When a signature is captured with a digitizer, the pen motions (dynamics) are recorded. According to Zimmerman et al. [36], 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, practiced motions whose accurateness rises with speed [36]. In the on-line signature there is an 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 signs again. 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.
- Acceleration: Acceleration produced by pen movements while one is writing or signing provide useful information for handwriting research, particularly for applications like automatic signature verification. Measurement of pen acceleration is usually done with accelerometers integrated into a pen or with devices that either derive pen acceleration from other physical measures or sense physical quantities equivalent to pen acceleration [37]. Acceleration signals are characterized 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.

8.2 Static Signature Verification

When the recognition is undertaken using only the static images of handwriting, the process is called off-line recognition. Despite the unique advantage over its on-line counterpart, as no specialized capture device is required, the amount of information obtained from off-line recognition is two orders greater, but much less meaningful and more difficult to interpret. Moreover, the traces of dynamic information are very difficult to compute. Traditionally, the recovery of such information requires professional skills and techniques whose implementation on computers is not easy [38]. Several evaluations performed by expert document analysts concluded that the detection of forgeries of high skill require not just static information but also dynamic information, a survey by Plamondon and Lorette [37] reported. Some rare attempts to extract direct pressure information were made by Ammar et al. [40]. With the distinct characteristics mentioned above, on-line recognition systems are able to achieve better results than their off-line counterparts [41].

Off-line systems utilize the classic method of on-paper signatures for person verification. The signature obtained is digitized by an optical scanner or camera. An alternative is to input the image through a tablet or any other suitable device. Subsequently, respective applications determine the match of the person's signature with a reference sample by comparing the overall trace (image) of the signature. Based on this particular principle, the current very unreliable methods, commonly practiced in banking and retail for example, are utilized to verify handwritten signatures, relying on the human factor in the form of a calligraphy expert.

9. Types of Forgeries

There are usually three different types of forgeries to take into account. According to Coetzer et al. [42], the three basic types of forged signatures are indicated below:

- Random forgery: The forger is not familiar and has no access to the genuine signature (not even the author's name) and reproduces a random one.
- Simple forgery: The forger is familiar with the author's name, but has no access to a 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.

The paper [43] shows various skill levels of forgeries and these are shown below.

- A forged signature can be another person's genuine signature. Justino et al. [44] categorized this type of forgery as a Random Forgery.
- A forged signature is produced with the knowledge about the genuine writer's name only. Hanmandlu et al. [45] categorized this type as a Random Forgery whereas Justino et al. [44] categorized this type as a Simple Forgery. Weiping et al. categorized this type as a Casual Forgery [46].
- A forged signature imitating a genuine signature's model reasonably well is categorized as a Simulated Forgery by Justino et al. [44]

- Signatures produced by inexperienced forgers without the knowledge of their spelling after having observed the genuine specimens closely for some time are categorized as Unskilled Forgeries by Hanmandlu et al. [45]
- Signatures produced by forgers after unrestricted practice by non-professional forgers are categorized as Simple Forgery/Simulated Simple Forgery by Ferrer et al. [47], and a Targeted Forgery by Huang and Yan [48].
- Forgeries which are produced by a professional imposter or person who has experience in copying Signatures are categorized as Skilled Forgeries by Hanmandlu et al.[45]

10. Related Work on Signature-based Biometric Authentication

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:

10.1 Single-script Signature-based Biometric Authentication

Arslan Bromme [26] has shown that every human being has static, dynamic, physiological and behavioural biological characteristics, which can be used for biometric person recognition. Handwritten signatures are one of the behavioural biological characteristics. Biometric signatures can be used for classes of biometric systems which are similar to those used within the core processes of biometric authentication systems. The main objective of that paper was the classification of biometric signatures.

Rabasse et al. [49] described a method for the generation of synthetic handwritten signatures, in the form of sequences of time-stamped pen data channels, for use in on-line signature verification experiment. The method presents modelled variability within the generated data based on variation that is naturally found within genuine source data. Experimentation using the SVC2004 [50] dataset and a commercial signature verification engine shows 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. Rather than a simple interpolation between the two seed signature, our method deploys an intelligent mapping and introduces naturally occurring variability within each signature. Derivative Dynamic Time Warping (DTW) to find minimum Euclidean edit distance between points within two seed signatures.

A new proposal for score normalization in biometric signature recognition based on client threshold prediction was proposed by Pascual et al. [51]. 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 approach is use for signature verification techniques. This work focuses on target dependent techniques.

Biometric security system based on signature verification using neural networks is presented by Kumar et al. [52]. The global and grid features are combined to generate new set of features for the verification of signature. The Neural Network is also used as a classifier for the authentication of a 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 i. Aspect Ratio, ii. Signature Height, iii. Image Area, iv. Pure Width and v. Pure Height have been used for the experiments. A number of 600 signature samples collected from 20 signers were considered for their experiments.

Maiorana et al. [53] 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 Radon transform which well fits to the signature images. In order to test the authentication performances of this approach, 50 signatures have been acquired from each of 30 users, taking for each of them 10 signatures in five different sessions during a week time span. Some approaches for the protection and authentication of biometric data using watermarking have been proposed in another report [54] where robust watermarking techniques are used to embed codes or timestamps.

Another approach [55] discusses a protected on-line signature-based biometric authentication system, where the biometrics considered are secured by means of non-invertible 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 of the considered system. The experiments were evaluated on the public MCYT signature database.

Another on-line signature-based biometric authentication system is presented by Maiorana et al. [56]. In this proposed technique, the 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 cancelable templates from the same original dataset, thus offering a proper solution to privacy concerns and security issues, is intensely explored.

Nagasundara et al. [27] 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.

In an approach by Mhatre and Maniroja [57] a signature based authentication by using two different algorithms was introduced. 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 [58] 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. 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.

10.2 Multi-script Signature-based Biometric Authentication

A different signature verification technique considering multi-script signatures has been proposed by Pal et al. [59]. This multi-script signature verification method involving English and Hindi signatures is very significant in multi-script signature environment. This multi-script signature identification and verification technique has never been used for the task of signature verification and this task was the first report in signature verification area. In that paper, the multi-script signatures were identified first on the basis of signature script type and afterward verification experiments were investigated based on the identified script result. Two different results for identification and verification were calculated and analysed.

In another approach by Pal et al. [60] the performance of signature script identification was reported. An experiential contribution towards the understanding of multi-script signature identification was presented. In that proposed signature identification technique, the signatures of Bengali (Bangla), Hindi (Devanagari) and English are considered for the identification process. The aim of that paper was to identify whether a claimed signature belongs to the group of Bengali, Hindi or English signatures. In a multi-script signature verification environment, signature script identification plays an important role. If the signatures are identified based the script used for writing signatures, subsequently the individual signature verification can be done based on the identified script result. Zernike Moment and histogram of gradient were employed as two different feature extraction methods. In the proposed scheme, Support Vector Machines (SVMs) were considered as classifiers for signature identification.

In another report by Pal et al. [61] a script identification scheme of signatures was investigated. In their paper, a technique for a bi-script off-line signature identification method is proposed. In this signature identification system, the signatures of English and Bengali (Bangla) are considered for the identification procedure. Different features like, modified chain-code direction features, under-sampled bitmaps and gradient features computed from both background and foreground components are employed for this purpose. SVMs and Nearest Neighbour (NN) techniques are considered as classifiers for signature identification in the proposed scheme. A dataset of 1554 English signature samples and 1092 Bengali signature samples are used to generate the experimental results. Different results based on different features are calculated and analysed.

An investigation of the performance of a signature identification system involving English and Chinese off-line signatures was presented by Pal et al. [62]. In that paper, a foreground and background based technique was proposed for identification of scripts from bi-lingual (English/Roman and Chinese) off-line signatures. The aim of the system was to identify whether a claimed signature belongs to the group of English signatures or Chinese signatures. The identification of signatures samples based on its script is a major contribution in a multi-script signature verification environment. Two background information extraction techniques were used to produce the background components of the signature images. Gradient-based technique was used to extract the features of the foreground as well as background components. Zernike Moment feature was also used on signature samples. (SVMs are used as the classifier for signature identification in the proposed system.

A two-stage approach for English and Hindi off-line signature identification and verification was proposed by Pal et al. [63]. The main aim of their approach was to demonstrate the significant advantage of signature script identification in a multi-script signature verification environment. In their proposed signature verification technique the performance of a multi-script off-line signature identification system, considering a joint dataset of Hindi and English signatures, was initially investigated and subsequently a verification task was explored separately for English signatures and Hindi signatures based on the identified script result. The gradient feature, water reservoir feature, loop feature and aspect ratio were employed and SVMs were considered for verification.

An experimental contribution in the direction of multi-script off-line signature identification and verification using a novel technique involving off-line English, Hindi (Devnagari) and Bangla (Bengali) signatures is introduced by Pal et al.[64]. In the first stage of the proposed signature verification technique, the performance of a multi-script off-line signature verification scheme, considering a joint dataset of English, Hindi and Bangla signatures, was investigated. In the second stage of experimentation, multi-script signatures were identified based on the script type, and subsequently the verification task was explored separately for English, Hindi and Bangla signatures based on the identified script result. The chain code and gradient features were employed, and Support Vector Machines (SVMs) along with the Modified Quadratic Discriminate Function (MQDF) were considered in this scheme. From the experimental result achieved, it is noted that the verification accuracy obtained in the second stage of experiments (where a signature script identification method was introduced) is better than the verification accuracy produced following the first stage of experiments. Experimental results indicated that an average error rate of 20.80% and 16.40% were obtained for two different phases of verification.

11. Signature Database Availability

Although research into signature verification has been pursued for several decades, there has been only a limited number of standard public off-line signature databases created. The scarcity of standard databases has partly resulted from the privacy aspect of the collection of handwritten signatures and a number of constraints that a standard database should meet. Due to the lack of availability of significant and public signature databases, developments of signature verification systems have been negatively affected. It has been difficult to make a significant comparison among different approaches presented in the literature due to the use of custom databases by researchers, and that these databases are not publicly available. The design and construction of an off-line signature corpus involves a long and complex procedure in which aspects such variability of drawing surface, changes of the writing instrument, differences between sessions, number of signers, number of genuine signs per person, forgery procedure and number of forgeries per person, etc. should be taken into account [65]. It is not easy to build a corpus which has considered all the above-mentioned variables mainly due to the difficulties in recruiting appropriate signers.

One of the major problems that can be found in the performance evaluation of signature verification systems, in both identification and verification modes, is the lack of publicly available large signature databases. The quality of available datasets also differs, as there has been no standard collection procedure. Besides, it is very costly to create a large corpus with different types of forgeries, especially skilled forgeries. So, the research in automatic signature verification has long been constrained by the limited availability of a standard database. Presently there are only a few publicly-available databases. Some of them are summarized in Table 1.

Table 1. Handwritten Signature Corpuses Available

Corpus Name	Signers	Genuine	Forgeries
GPDS signature [66]	**160**	**24**	**30**
SVC2004 [50]	**40**	**20**	**20**
MCYT-100 [67]	**100**	**25**	**25**
MCYT-75 [68]	**75**	**15**	**15**
GPDS signature [65]	**960**	**24**	**30**

12. Signature Data Acquisition and Pre-processing

On the basis of the handwritten signature data acquisition method, two types of systems for handwritten signature verification have been identified (as mentioned previously): static (off-line) systems and dynamic (on-line) systems. In static mode, handwritten signature data is converted to digital form by scanning the signature from the signature collection paper. In this mode, the handwritten signatures are represented as a gray level image. On the other hand, one can deal with the signature data acquisition in online method by using a special pen on an electronic surface. The most conventional online data acquisition devices are digitizing tablets [36]. Electronic pens are also able to detect position, velocity, acceleration, pressure, pen inclination, and writing forces etc.

Once the signature has been acquired, either off-line or on-line, some pre-processing techniques are usually needed. The pre-processing step is vital in order to ensure that only the desired data is fed to the feature extraction module. Normally, acquired signature images are of different formats and resolutions and need to be processed to enable accurate feature extraction. The acquired images may contain unexpected marks, stains, or noise which would cause negative effects on the recognition accuracy. Pre-processing includes steps eliminating such noise and converting the image to a suitable format for feature extraction. Other important pre-processing techniques (signature size normalization, binarization, thinning, smearing, skew correction, skeleton extraction) are also considered in static signatures for accurate feature extraction. Typical pre-processing algorithms for dynamic signature verification involve filtering, noise reduction and smoothing. Another vital pre-processing step that strongly influences all the successive phases of signature verification in both static and dynamic modes is segmentation [69]. Some of the pre-processing steps are carried out in the following sub-steps.

- 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 to remove selected foreground pixels from binary images.
- Filtering process: Generally, digital image might contain speckles, smears, scratches or other forms of unwanted noise that might thwart feature extraction. Thus, median filtering is used to eliminate the existing noises.
- Binarization: The process by which the image is converted into black and white is called binarization.
- Width normalization: All signature images have been reduced to a standard size so as to ease the process of feature extraction.

13. 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 [70]. 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 [72] commented that the selection of features must be appropriate for the application and the approach. Klement et al. [73] summarized the three requirements that concerned the feature selection process: (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, [74] signatures are usually characterized in terms of a time function and the values of the time function constitute the feature set. Conversely, when parameter features [75] 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 [76] 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.

13.1Feature Vector Generation

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 features that represent some object. The flowchart in Figure 3 shows the process of feature vector generation [77]. 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. A flowchart of feature vector generation is shown in Figure 5.

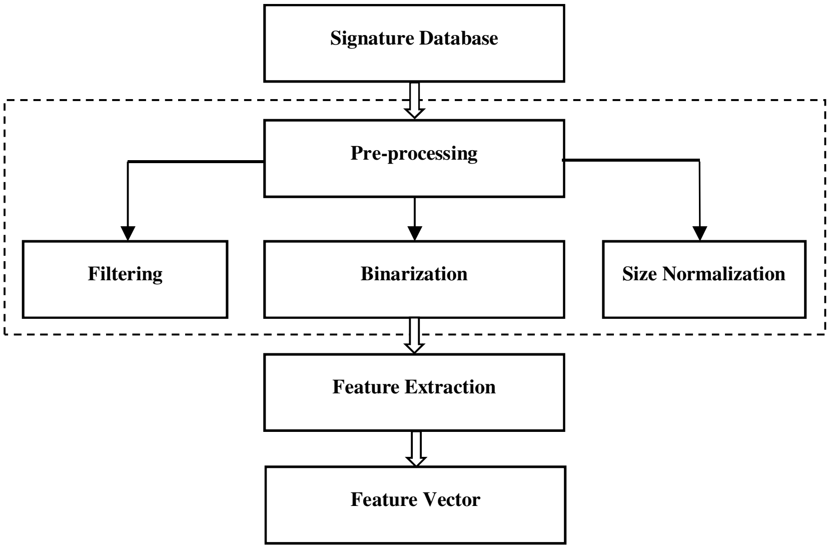

Figure5. Feature Vector Generation Flowchart

14. Classification

In the signature verification method, the authenticity of the test signature is evaluated by matching its features against those stored in the knowledge base developed during the enrolment stage. This process generates a single response that states the authenticity of the test signature samples. Some of the most relevant approaches to signature verification as mentioned in [69] are shown in Figure 6.

When template matching methods are considered in verification, a questioned signature sample is matched against templates of authentic/forged signatures. Dynamic Time Warping (DTW) is used for the most common approaches in this situation for signature matching. DTW is a Template Matching technique used for measuring similarity between two sequences of observations. DTW allows the compression or expansion of the time axis of two time sequences representative of the signatures to obtain the minimum of a given distance value [78].

An Artificial Neural Network (ANN) is a massively parallel distributed system composed of processing units capable of storing knowledge learned from experience (examples) and using it to solve complex problems. The ANN-based approaches have been widely used for a long time in signature verification area, due to their learning and generalizing capability [79].

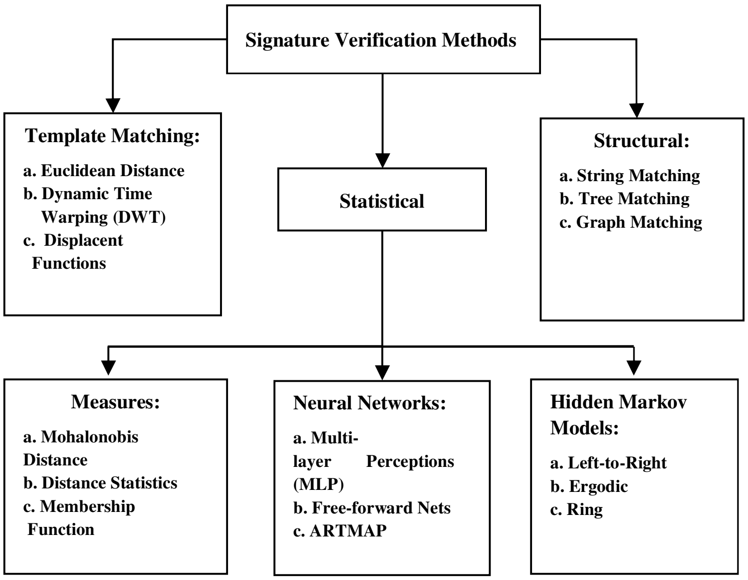

Figure6. Signature Verification Techniques (Classification approaches)

In recent times, more attention has been dedicated to the use of Hidden Markov Models for both offline and online signature verification. These models have found to be well suited for signature modelling since they are highly adaptable to personal variability [80].

SVMs are another promising statistical approach to signature verification. SVMs are a relatively new classification technique in the field of statistical learning theory and they have been successfully applied in many pattern recognition approaches. An SVM can map input vectors to a higher dimensional space in which clusters may be determined by a maximal separating hyper plane. SVMs have been used successfully in both offline [66] and online signature verification [81].

15. Conclusions

This chapter presented a detailed study on signature-based biometric authentication. Automatic signature verification is a very interesting area of research from the scientific point of view. In recent years, along with the continuous enhancement of security requirements, the field of automatic signature-based authentication is being explored with renewed interest. Up to date outcomes achieved in worldwide competitions using benchmark databases have confirmed that signature authentication systems can have an accuracy level similar to those achieved by other biometric systems [82]. Although, a significant amount of work has been undertaken in order to solve the authentication problem, there are still many challenges to be faced. Hence in this Chapter a detailed description of signature-based biometric authentication has been presented and hopefully it will be helpful to the researcher as reference materials.

References

[1] K. W. Boyer, V. Govindaraju, and N. K. Ratha, "Introduction to the Special Issue on Recent Advances in Biometric Systems", IEEE Trans. Systems, Man, and Cybernetics, part B, vol. 37, no.5, pp. 1091–1095, 2007.

[2] A. Samal and P.A. Iyengar, "Automatic Recognition and Analysis of Human Faces and Facial Rxpressions: A Survey", Pattern Recognition, 25(1):65–77, 1992.

[3] A. K. Jain, L. Hong, and S. Pankanti, "Biometric Identification," Communications of the ACM, vol. 43, no. 2, pp. 91–98, 2000.

[4] D. Zhang, J. P. Campbell, D. Maltoni, and R. M. Bolle, "Special Issue on Biometric Systems", IEEE Trans. Systems, Man, and Cybernetics, part C, vol. 35, no. 3, pp. 273–275, 2005.

[5] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, "Biometric Systems: Technology, Design and Performance Evaluation", Springer Verlag, 2005.

[6] A. K. Jain, R. Bolle, and S. Pankanti (Eds), "Biometrics: Personal Identification in Networked Society," Kluwer Academic Publishers, 1999.

[7] D. V. Klein, “Foiling the Cracker: a Survey of Improvements to Password Security,” in Proc. 2nd USENIX Workshop Security, pp. 5–14, 1990.

[8] S. Z. Li and A. K. Jain, “Handbook of Face Recognition”, Springer Verlag, 2004.

[9] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, “Handbook of Fingerprint Recognition”, Springer Verlag, Jun. 2003.

[10] Anil k. Jain, Arun Ross and Sharath Pankanti, “Biometrics: a tool for information security”, IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125-143, 2006.

[11] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzales-Marcos, “Biometric Identification through Hand Geometry Measurements”, IEEE Trans. Pattern Anal. Mach. Intell., vol. 22, no. 10, pp. 1168–1171, 2000.

[12] J. Daugman, “The Importance of being Random: Statistical Principles of Iris Recognition”, Pattern Recognition, vol. 36, no. 2, pp. 279–291, 2003.

[13] R. Hill, “Retina Identification”, Chapter 4 in A., Jain, Bolle, and S., Pankanti, “BIOMETRICS: Personal Identification in Networked Society,” 2nd Printing, Kluwer Academic Publishers, 1999.

[14] J. P. Campbell, “Speaker Recognition: A Tutorial,” Proc. IEEE, vol. 85, no. 9, pp. 1437–1462, 1997.

[15] F. Monrose and A. Rubin, “Authentication via Keystroke Dynamics,” in Proc. 4th ACM Conference on Computer and Communications Security, pp. 48–56, 1997.

[16] A. M. Joussen, “Vascular plasticity - the role of the Angiopoietins in Modulating Ocular Angiogenesis,” Graefe's Archive for Clinical and Experimental Ophthalmology, vol. 239, Issue 12, pp. 972 - 975, 2001.

[17] Isao Nakanishi, Shouta Koike, Yoshio Itoh and Shigang Li, “ DWT Domain On-Line Signature Verification”, Tottori University, Japan, pp. 183-196.

[18] R. Plamondon, “A kinematic Theory of Rapid Human Movements: Part III: Kinetic Outcomes,” Biol. Cybern., Jan. 1997.

[19] V. S. Nalwa, “Automatic on-line Signature Verification,” Proc. IEEE, vol. 85, no. 2, pp. 213–239, 1997.

[20] Jean Jules Brault and Rejean Plamondon, “A Complexity Measure of Handwritten Curves: Modelling of Dynamic Signature Forgery”, IEEE Transactions on Systems, Man, and Cybernetics, 23(2):400–413, 1993.

[21] R. Plamondon , “The Design of an On-line Signature Verification System: from Theory to Practice”, International Journal on Pattern Recognition and Artificial Intelligence, 8(3):795–811, 1994.

[22] Anil K. Jain and Arun Ross, “Multi-biometric Systems”, Communications of the ACM, vol. 47, no. 1 pp.35-40, 2004.

[23] M. C. Fairhurst, “Signature Verification Revisited: Promoting Practical Exploitation of Biometric Technology”, Electronics and Communication Engineering Journal, Vol. 9(6), pp.273–280, 1997.

[24] M. A. Ismail and S. Gad, “Off-line Arabic Signature Recognition and Verification”, Pattern Recognition, Vol. 33(10): pp. 1727-1740, 2000.

[25] B. B. Chaudhuri and U. Pal, “An OCR System to Read two Indian Language Scripts: Bangla and Devnagari (Hindi)”, Proceedings of 4th ICDAR, pp. 1011–1015, 1997.

[26] Arslan Bromme, “A Classification of Biometric Signatures” International Conference on Multimedia and Expo, ICME, pp. 17-20, 2003.

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

[28] Teddy Ko, " Multimodal Biometric Identification for Large User population Using Fingerprint, Face and Iris Recognition". Proceedings of the 34th Applied Imagery and pattern recognition Workshop, pp. 218 – 223, 2005.

[29] A. Ross, A. K. Jain, "Multimodal Biometrics: An Overview", Proceedings of the 12th European Signal Processing Conference (EUSIPCO), pp. 1221-1224, 2004.

[30] A. Ross, K. Nandakumar, A. K. Jain, Handbook of Multibiometrics. Springer.vol.6, 2006.

[31] R. Plamondon, "The Handwritten Signature as a Biometric Identifier: Psychophysical Model and System Design", European Convention on Security and Detection: 16-18 May, 1995.

[32] R. Plamondon, "A Kinematic Theory of Rapid Human Movements: Part I: Movement Representation and generation", Biological Cybernetics, Vol. 72, No. 4, pp. 295-307, 1995.

[33] R. Plamondon and M. Djioua, "A Multi-Level Representation Paradigm for Handwriting Stroke Generation", Human Movement Science, Vol 25, No. 4-5, pp. 586-607, 2006.

[34] G. Congedo, G. Dimauro, S. Impedovo and G. Pirlo, "A New Methodology for the Measurement of Local Stability in Dynamical Signatures", 4th International Workshop on Frontiers in Handwriting Recognition, pp. 135-144, 1994.

[35] D. Impedovo, G. Pirlo, L. Sarcinella, E. Stasolla and C. A. Trullo, "Analysis of Stability in Static Signatures using Cosine Similarity", International Conference on Frontiers in Handwriting Recognition, pp. 231-235, 2012.

[36] 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 of SPIE, Vol. 5404, pp. 206-214, 2004.

[37] R. Plamondon and G. Lorette, "Automatic Signature Verification and Writer Identification Verification the State of Art", Pattern Recognition, vol. 22, no. 2, pp. 107-131, 1989.

[38] S. N. Srihari and G. Leedham, "A Survey of Computer Method in Forensic Document Examination", in 11th Conf. of the Intl. Graphonomics Society, 2003.

[39] http://en.wikipedia.org/wiki/Biometrics.

[40] M. Ammar, Y. Yoshida, and T. Fukumura. A New Effective Approach for Off-line Verification of Signatures by using Pressure Features. in 8th Int. Conf. on Pattern Recognition. 1986.

[41] F. Leclerc and P. R., "Automatic Signature Verification: The State of the Art, 1989-1993", International Journal of Pattern Recognition and Artificial Intelligence, 8(3), pp. 643- 660, 1994.

[42] J. Coetzer, B. Herbst, J. D. Preez, "Off-line Signature Verification using the Discrete Radon Transform and a Hidden Markov Model. EURASIP Journal on Applied Signal Processing", 4, pp. 559–5712004.

[43] V. Nguyen, M. Blumenstein, V. Muthukkumarasamy, G. Leedham, "Off- line Signature Verification using Enhanced Modified Direction Features in Conjunction with Neural Classifiers and Support Vector Machines", International Conference on Document Analysis and Recognition, pp. 734–738, 2007

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

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

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

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

[48] Huang K, Yan H, “Off-line Signature Verification using Structural Feature Correspondence”, Pattern Recognition, 35(11):2467–2477, 2002.

[49] C. Rabasse, R.M.Guest and M.C. Fairhurst, “A Method for the Synthesis of Dynamic Biometric Signature Data”, Ninth International Conference on Document Analysis and Recognition, pp.168-172, 2007.

[50] Dit Yan Yeung, Hong Chang, Yimin Xiong, Susan George, Ramanujan Kashi, Takashi Matsumoto and Gerhard Rigoll, “SVC2004: First International Signature Verification Competition”, Proceedings of the International Conference on Biometric Authentication, Hong Kong, 15-17 July 2004.

[51] Carlos Vivaracho Pascual, Arancha Simon Hurtado, Esperanza Manso Martinez and Juan M. Pascual Gaspar, “ A New Proposal for Score Normalization in Biometric Signature Recognition Based on Client Threshold Prediction”, International Conference on Data Mining, 2012, pp.1128-1133.

[52] D. R. Shashi Kumar, R. Ravi Kumar, K. B. Raja, R. K. Chhotaray, Sabyasachi Pattanaik, “ Biometric Security System Based on Signature Verification Using Neural Networks”, 2010, pp. 580-583.

[53] Emanuele Maiorana, Patrizio Campisi, Alessandro Neri, “Biometric Signature Authentication using Radon Transform-based Watermarking Techniques” , Biometrics Symposium, pp 1-6, 2007.

[54] N. K. Ratha, J. H. Connell, R. Bolle, “Secure Data Hiding in Wavelet Compressed Fingerprint Images”, ACM Multimedia 2000 Workshops, pp. 127- 130, 2000.

[55] Emanuele Maiorana, Patrizio Campisi and Alessandro Neri, “Bioconvolving: Cancelable Templates for a Multi-Biometrics Signature Recognition System”, International Systems Conference on Digital Object Identifier, pp. 495500, 2011.

[56] Emanuele Maiorana, Patrizio Campisi, Javier Ortega-Garcia and Alessandro Neri, “Cancelable Biometrics for HMM-based Signature Recognition”, International Conference on Biometrics, Theory, Applications and Systems, pp. 1-6, 2008.

[57] Mhatre and Maniroja, “Offline Signature Verification Based on Statistical Features”, International Conference and Workshop on Emerging Trends in Technology, pp. 59-62, Mumbai, India.

[58] Emanuele Maiorana, Patrizio Campisi, Julian Fierrez, Javier Ortega Garcia, and Alessandro Neri, “Cancelable Templates for Sequence-based Biometrics with Application 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

[59] Srikanta Pal, Umapada Pal and Michael Blumenstein, “Hindi and English Off-line Signature Identification and Verification”, International Conference on Advances in Computing, PP. 905-910, 2012.

[60] Srikanta Pal, Alireza Alaei, Umapada Pal and Michael Blumenstein, “ Multi-Script Off-line Signature Identification”, International Conference on Hybrid Intelligent Systems, pp. 236-240, 2012.

[61] Srikanta Pal, Alireza Alaei, Umapada Pal and Michael Blumenstein, “Off-line Signature Verification based on Foreground and Background information”. International Conference on Digital Image Computing: Techniques and Applications, PP. 672-677, 2011.

[62] Srikanta Pal, Umapada Pal and Michael Blumenstein, “Off-line English and Chinese Signature Identification Using Foreground and Background Features”. IJCNN Special Session on Machine Learning for Computer Vision at IEEE World Congress on Computational Intelligence, pp. 1-7, 2012.

[63] Srikanta Pal, Umapada Pal and Michael Blumenstein, “A Two-Stage Approach for English and Hindi Off-line Signature Verification”, International workshop on Emerging Aspects in Handwritten Signature Processing, EAHSP 2013, Naples, Italy (not yet published).

[64] Srikanta Pal, Umapada Pal and Michael Blumenstein, “Multi-script Off-line Signature Verification: A Two Stage Approach”, Accepted on International Workshop on Automated Forensic Handwriting Analysis, AFHA 2013, Washington DC, USA, (not yet published).

[65] F. Vargas, M. Ferrer, C. M. Travieso, and J. Alonso. Offline handwritten signature GPDS-960 Corpus. In 9th ICDAR, pages 764–768. IEEE Computer Society, 2007.

[66] M. A. Ferrer, J. B. Alonso, and C. M. Travieso. Offline Geometric Parameters for Automatic Signature Verification using Fixed-point Arithmetic. IEEE PAMI, Trans. on, 27, pp. 993–997, 2005.

[67] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V.Espinosa, A.Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero and Q.-I. Moro, “MCYT Daseline Corpus: a Bimodal Biometric Database”, IEE Proceedings of Visual Image Signal Processing, Vol. 150, No. 6, 2003.

[68] J. Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno- Marquez and J. Ortega-Garcia, “An Off-line Signature Verification System based on Fusion of Local and Global Information”, Workshop on Biometric Authentication, Springer LNCS-3087, pp. 295-306, 2004.

[69] D. Impedovo and G. Pirlo, “Automatic signature verification: The state of the art,” IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 38, no. 5, pp. 609–635, 2008.

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

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

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

[73] 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.

[74] G. Congedo, G. Dimauro, A. M. Forte, S. Impedovo and G. Pirlo, "Selecting Reference Signatures for On-line Signature Verification", International Conference on Image Analysis and Processing, pp. 521–526, 1995.

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

[76] R. Plamondon and G. Lorette, "Automatic Signature Verification and Writer Identification-the State of the Art", Pattern Recognition, 22(2), pp. 07-13, 1989.

[77] Vandana S.Inamdar , Priti. P. Rege and Meenakshi S Arya, "Offline Handwritten Signature based Blind Biometric Watermarking and Authentication Technique using Biorthogonal Wavelet Transform" , International Journal of Computer Applications volume 11– No.1, pp. 0975 – 8887, 2010.

[78] J. P. Leszczyska, "On-line Signature Verification using Dynamic Time Warping with Positional Coordinates," Proc. SPIE, vol. 6347, pp. 634724- 1–634724-08, 2006.

[79] K. Huang and H. Yan, "Off-line Signature Verification based on Geometric Feature Extraction and Neural Network Classification" Pattern Recognition, 30(1), pp. 9–171, 1997.

[80] S. Garcia-Salicetti and B. Dorizzi, "On using the Viterbi Path Along with HMM Likelihood Information for Online Signature Verification", IEEE Trans. Syst., Man, Cybern. B, vol. 37, no. 5, pp. 1237–1247, 2007.

[81] A. Kholmatov and B.Yanikoglu, "Identity Authentication using Improved Online Signature Verification Method," Pattern Recognit. Letters, vol. 26, pp. 2400–2408, 2005.

[82] D. Impedovo, G. Pirlo and M. Refice, "Handwritten Signature and Speech: Preliminary Experiments on Multiple Source and Classifiers for Personal Identity Verification", IWCF, pp. 181-191, 2008.