# Enhancing Handwritten Signature Identification and Palm Biometric Objectives

**Dr. Balasani Venkata Ramudu[1] Mr. Chiranjeevi Kondabathini[2] Mr. Udaya Kiran Mandhugula[3]**

*1 Assistant Professor, Department of CSE, MRITS (Malla Reddy Institute of Technology & Science), Misammaguda, Hyderabad Telangana, INDIA.*

*2, 3 Assistant Professor, Department of Information Technology, Vidya Jyothi Institute of Technology, Hyderabad, Telangana, INDIA.*

---------------------------------------------------------------------***---------------------------------------------------------------------

Abstract- Soft biometrics are already widely used as a support tool for user identification. However, it is not the only use for biometric information that is conceivable because such information can be sufficient to obtain minimal details from the user that are unrelated to his identity. Examples of what might be referred to as soft biometrics include gender, hand orientation, and emotional state. Utilizing physiologic modalities for soft-biometric work is extremely prevalent, prediction, but behavioral data is frequently disregarded. Keystroke dynamics and handwriting signature are two potential behavioral modalities that could be used to predict a user's gender, but they are rarely discussed in the literature together. This study seeks to fill this gap by examining the influence of combining these two distinct biometric modalities on the accuracy of gender prediction and the best way.

***Key Words***: Item key-strokes, Bio-metric signatures, digital signs, dynamic temporal wrapping (DTW)

## 1. INTRODUCTION

Traditional user authentication techniques are based on a possession (Example: The key is an identification card, an authentication card, punch biometric card...) and /or anything you know (Example: pin, password). The new user authentication in multi paradigm is introduced by biometric authentication: something that you are (iris, face or finger print) or whatever you create (Example: hand-written signature, voice or text). The People still utilise handwriting in the way to transmit, retain, and ease to communication in the internet age because paper and a pen are convenient.

A signature is a unique kind of handwriting that uses distinctive symbols and flourishes. Numerous autographs may be illegible. They are a type of creative writing (Cemil,2005). For the Sort of behavioral biometrics, the process of authenticating a user's identity using a signature based on their handwritten signature.

In contrast to previous methods of personal identification and verification, Biometrics Technology has a huge possibility of personal verification done automatically (Pirlo,1994). Since signatures have for ago recognised, the most widely used in our daily lives, banking statements, banking transactions, automated money transfers of funds, and other uses for commerce, signature-based verification is a popular and advantageous method for personal verification. As opposed to previous methods of personal identification and verification, the potential for automatic personal verification using biometrics is enormous. (Pirlo,1994). The benefit of signature-based verification over other biometrics is that it doesn't require any invasive testing and is generally regarded because signatures have far ago recognised per widely used method of personal identification in daily activities, such as in banking transactions, banking statements, banking transactions, automated money transfers of funds, commerce applications, automatic fund transfers, and other situations

It is common to distinguish between two types of verification systems: systems with no world wide web or static where There are dynamically or exclusively online systems, where the signatures signal is taken throughout the writing process and the dynamic information is thus made available, and static systems, where the signature signal is captured after writing procedure is complete and the static image is readily accessible. This study examines the authentication of online signatures.

As part of the online Verification of signatures system, users can sign with hand gloves, smart pens, or digitizing tablets. The original design of the Web-based validation or Online Verification of Signatures System considered the following 4 aspects:

i. Data- Acquisition Pre-processing,
ii. Extraction Features,
iii. Matching (classification),
iv. Decision Making.

Traditional user authentication techniques are based on a possession (Example: The key is an identification card, an authentication card, punch biometric card...) and /or anything you know (Example: pin, password). The new user authentication in multi paradigm is introduced by biometric authentication: something that you are (iris, face or finger print) or whatever you create (Example: hand-written signature, voice or text). The People still utilise handwriting in the way to transmit, retain, and ease to communication in the internet age because paper and a pen are convenient.

A signature is a unique kind of handwriting that uses distinctive symbols and flourishes. Numerous autographs may be illegible. They are a type of creative writing (Cemil,2005). For the Sort of behavioral biometrics, the process of authenticating a user's identity using a signature based on their handwritten signature.

In contrast to previous methods of personal identification and verification, Biometrics Technology has a huge possibility of personal verification done automatically (Pirlo, 1994). Since signatures have for ago recognised, the most widely used in our daily lives, banking statements, banking transactions, automated money transfers of funds, and other uses for commerce, signature-based verification is a popular and advantageous method for personal verification. As opposed to

previous methods of personal identification and verification, the potential for automatic personal verification using biometrics is enormous. (Pirlo, 1994). The benefit of signature-based verification over other biometrics is that it doesn't require any invasive testing and is generally regarded because signatures have far ago recognised per widely used method of personal identification in daily activities, such as in banking transactions, banking statements, banking transactions, automated money transfers of funds, commerce applications, automatic fund transfers, and other situations It is common to distinguish between two types of verification systems: systems with no world wide web or static where There are dynamically or exclusively online systems, where the signatures signal is taken throughout the writing process and the dynamic information is thus made available, and static systems, where the signature signal is captured after writing procedure is complete and the static image is readily accessible. This study examines the authentication of online signatures. As part of the online Verification of signatures system, users can sign with hand gloves, smart pens, or digitising tablets. The original design of the Web-based validation or Online Verification of Signatures System considered the following 4 aspects:

i. Data- Acquisition Pre-processing,
ii. Extraction Features,
iii. Matching (classification),
iv. Decision Making.

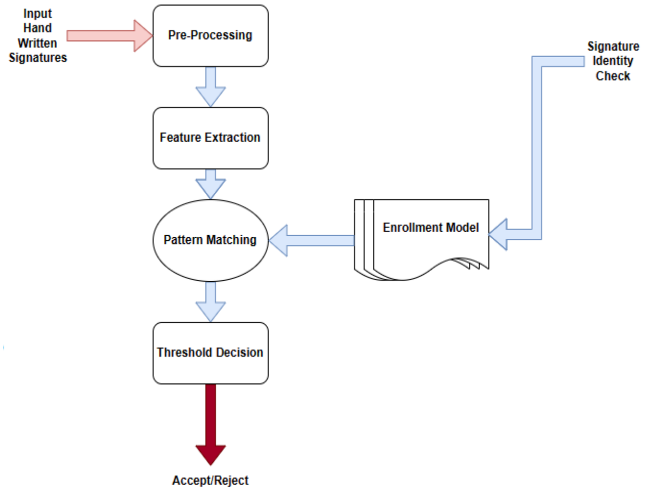

Figure: 1 Authentication Verification of Signatures Systems - Online

**Input device -input signature:** A digitising tablet, laptop, PDA, Touch pad smart pen, or pen tablet is the typical input device for an online Verification of signatures system.

Extraction of characteristics: Some the features will have greater discriminating power than others. Therefore, some the features selection should be closed stage, once features are retrieved, to dynamic systems, two types of characteristics may be extracted:

Static characteristics: These features that the greatest, minimum, and average writing speeds, circumference measures, etc., are taken from the whole signature process. Major complexity in this instance relates to the feature extraction procedure itself. It is difficult to choose a reliable, useful, and efficient feature.

Dynamic characteristics: These features include how a parameter, such as location, velocity, acceleration, pressure, or other quantity, changes over time. In dynamic feature approaches, the feature extraction phase is seldom ever used and the matching step experiences significant challenge.

Calculation of similarity between the input characteristics and an asserted identity model constitutes matching. The four most well-known methods for pattern recognition, according to Jain et al. (2000) are: Template Matching, Classification of Statistical, Structure Matching, neural networks.

**Input device -input signature:** A digitising tablet, laptop, PDA, Touch pad smart pen, or pen tablet is the typical input device for an online Verification of signatures system.

**Extraction of characteristics:** Some the features will have greater discriminating power than others. Therefore, some the features selection should be closed stage, once features are retrieved, to dynamic systems, two types of characteristics may be extracted:

**Static characteristics:** These features that the greatest, minimum, and average writing speeds, circumference measures, etc., are taken from the whole signature process. Major complexity in this instance relates to the feature extraction procedure itself. It is difficult to choose a reliable, useful, and efficient feature.

**Dynamic characteristics:** These features include how a parameter, such as location, velocity, acceleration, pressure, or other quantity, changes over time. In dynamic feature approaches, the feature extraction phase is seldom ever used and the matching step experiences significant challenge.

Calculation of similarity between the input characteristics and an asserted identity model constitutes matching. The four most well-known methods for pattern recognition, according to Jain et al. (2000) are: Template Matching, Classification of Statistical, Structure Matching, neural networks.

## 2. Discussion on the topic:

The decision entails the method for calculating a decision threshold once a commonality measure has been determined. The decision is ACCEPT if the likeness match above a certain level; otherwise, the choice is REJECT. Users are first registered in a technique for online signature validation by supplying sample signatures (reference signatures). The check signature is then compared against signatures used as references for the person when a user presents a signature (Test Signature) claiming to be that person. The user is denied if the dissimilarity exceeds a specific level.

Comparing the test signature to every signature in the bench mark set during verification, yielding a number of distance values. The next step is to select a technique for combining the sum of these distance values that represents the A test signature's difference from the bench mark set, and to arrive at a conclusion, compare it to a threshold. Competent forgeries and random forgeries are the two categories of forgeries. A competent forgery is one that has been practised on authentic signatures and is performed by a person who has access to them.

## 3. Evaluation of Biometric Technologies' Performance:

The problem of Verification of signatures may be seen as a pattern recognition issue with two classes: the real and the fake. The same person's signatures exhibit a significant degree of variation depending on the nation, age, season, customs, mental or psychological state, and physical and practical circumstances. When two signatures are similar, there is only one thing you can be sure of in this field.

The effectiveness example of a biometric verification system assessed using Type -I and Type -II error rates, which are the error representation of a two-class pattern recognition issue. The Type I error rate, also known as the False Rejection Rate (FRR), calculates the proportion of real signatures that are incorrectly identified as forgeries in relation to the categorization threshold. The Type II error rate, also known as the false acceptance rate (FAR), measures how many fake signatures are accepted as legitimate ones in relation to the categorization threshold.

Munich and Perona (1998) said that it is evident that one form of error may be exchanged for another type of fault. There would be a 0% FRR and a 100% FAR if every signature were accepted, and a 100% FRR and a 0% FAR if every signature were denied. Choosing between errors curve is the FRR function of the FAR curve with the parameter known as the categorization threshold. It gives the algorithm's behaviour for every operating system and is the best way to describe the system's performance. This curve, which results based on the practical point analysis, is frequently reduced to the scalar, Equal Error Rate (EER). Figure 2 : shows the curves of the Functions of the FRR, FAR, and classification associated error trade-off curve.

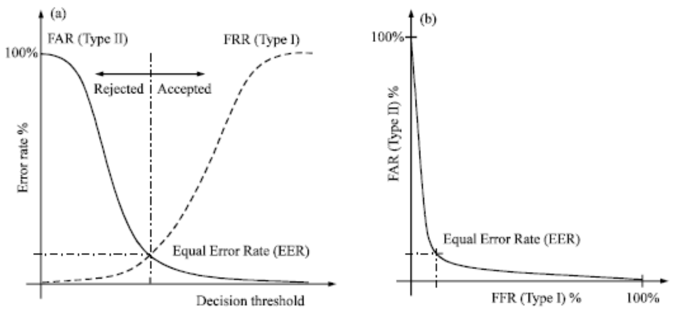

Fig .2(a) Fig. 2(b)

We use Equal Error Rate, where percentage of FAR equal's percentage of FRR, to assess what works well our Verification of signatures method. The statistical performance to the method is estimated by this EER. It may be used as a special statistic to describe the biometric system's level of security.

The error rate at which the percentage of erroneous acceptances and false rejections are equal. The method's statistical performance is estimated by this equal error rate, which also serves as a generalization error estimate for the algorithm. Figures 2(a) and (b) display the trade-off curve and the Equal Error Rate (FRR) and False Acceptance Rate (FAR) with respect to the categorization threshold. A Verification of Signatures System may be validated using various forgeries, will be determined by the testing's outcomes, circumstances of accessible Data.

### 4. Current Status of Online Verification Signatures:

The Researchers employed a test pen that was attached utilising Orthogonal accelerometers on both sides gathered the test signatures at the rate of 400 per second, and provided an example. They saw that most of signatures took among 2 and 10 seconds, with an average of around 5 seconds. The researchers also stated all of the signatures were divided Utilizing segments heuristics, and that the segments had been aligned over time.

There was disagreement between the reference and test signatures and cross correlation between interval matching segments. It was discovered that segments with a duration of 1 to 2 seconds had the best performance. Seventy users reviewed the procedure in which each user provided the first five sample signatures. The distance separating those selected signatures from the remaining signatures was created by selecting one or two reference signatures, at least as much as the predetermined value. These reference signatures were regarded as the greatest ones. 287 fraudulent signatures and 695 extra authentic test signatures were employed for testing. The experimental findings showed that more than 20%, it was discovered that there was a 1.5% False Acceptance Rate (FAR) and a false rejection rate (FRR).

Liu et al. (1979), who were quoted by Gupta (2006), studied the recommended observations of two accelerations made by Herbst, as well as added the burden of writing employed throughout the signature procedure. Going to consider the correlation values predominated the pressure waveform in the most general form, they noticed demonstrates the connection between pressure waveforms displayed a slight inequity. However, they discovered that when the pressure waveform components with low frequency paper contact were removed, it seemed to operate better. The researchers. used pressure and acceleration in several of their studies, Using the signatures of 24 participants, they employed pressure correlations and independently to produce findings that were less than 1.5% of FAR and close to 16% of FRR. It showed that Herbst and Liu's prior results weren't as good (1977).

A lot of research have looked at the field of Electronic Verification of Signatures. Ostrem and Crane (1983) provided a system in which testing included a registration step, which Gupta (2006) noted. In the registration step, a reference feature vector, 20 or 22 sample signatures, and Standard Deviation (SD) of each feature were determined. The Euclidean norm of the distance was then determined by comparing the test signature vector's comparison to the reference signature vector. The signature is regarded as authentic if the distance is short enough, else it is rejected as a fake. Only a fictitious rejection happened if none of the three signatures passed the test for verification, which the system permitted up to three times. According to the experimental findings, erroneous rejection and acceptance rates (FAR and FRR, respectively) ranged from 0.5% to around 3%.

Acknowledged Hastie et al. and reported on a model in which it was believed that a test signature consisted of a reference signature that updated periodically. The five-step procedure for Verification of signatures that the researchers presented is as follows:

**Step 1:** Smoothing to average out the measurement errors, a cubic spline approximation was utilised.

**Step 3:** A time warp function was created to time warp in order to find correlation among the signatures, test signatures and reference signatures.

**Step 2:** After smoothing, speed-speed was calculated.

Step 4: The signature was divided into a series of segments known as letters using low speed areas (low speed, for example, was defined as 15% of mean speed) of segmentation.

Step 5: Calculated the reference signature by averaging it based on the letters.

The authors also noted that Nelson and Kishon's study, which was published, featured the outcomes of applying the aforesaid strategy (1991). The authors said that 10 samples of real signatures and four samples of forgeries from each of the 20 participants were utilised for testing. According to the experimental findings, FRR and FAR were both 0%. Nelson and Kishon (1991) also made the case that, depending on the dynamics of the signature, it can be crucial in hand Verification of signatures,

Additionally, 105 people were randomly chosen to provide forgeries for 22 subjects. Each of the 22 participants received six expert forgeries from eight different people. These offered a total of 792 fakes, whereas 22x8x6 = 1056 were utilised as verification. So it seems like some of the forged documents turned down. A portion of among the database was drawn from a total of 15 real signatures for each of the 50 people, of which 6 were utilised as the reference signature and 10 as test signatures. In contrast, the researchers utilised 704 forgeries for verification, each of which provided 4 forgeries. There were 8 forgers for every one forger. An EER of 3.8% was stated to have been acquired based on their experimental findings.

The method proposed by Chang et al. (1993) Chinese hand signatures can be checked online using this method using Bayesian neural networks was disclosed in the article written by Gupta (2006). A total of 16 parameters, including the total duration, the number of segments, the speed on average, the Ratio of upper/lower component densities, the width-to- the average distance when comparing heights in each of the twenty signature directions, and the ratio of left-to-right component density, were employed in the study, according to the authors. The researchers utilised a database made up of 80 people who collectively supplied 200 simples and 800 real signatures. 200 expert forgeries performed by 10 forgers were used in the experiment for verification, and the results showed 1.8% FRR and 2.2% FAR.

The statistical approach for hand signatures submitted by for verification Nelson et al. (1994) was discovered in the Gupta paper (2006). According to the authors, the proposed method utilised a total 25 features, including two aspects relating to time, six velocity and acceleration-related features, A feature that dealt with the relationship between the two pen velocity components, four shape-related features, and eight attributes that provided information on the density of the route tangent angles., nearly ten features that gave angular velocity densities of angular changes, and one feature that dealt with the distribution density of the angle changes. Additionally, they described the statistical foundation for hand Verification of signatures. The Mahalanob is distance method, and the quadratic discriminant technique the proportions of each feature's Standard Deviation (SD) to its mean are computed and then used to rank-order the features. This is a straightforward approach of feature selection .The rationale behind why a feature with the smallest normalised standard deviation will help to distinguish between forgeries and real signatures with competence was not stated. There were several different evaluation methods employed, including individual best 8, 10, 12 or 14 of the 25 attributes. Even though the individual top 8 and 10 discovered to produce the fantastic outcome with FRR close to 0%, the achievement of all these sets was similar. The authors determined that the top 10 characteristics out of the 25 features may be used in conjunction with a Euclidean distance technique to get results with 0.5% FRR and 14% FAR.

A graphics tablet was used to gather 200 signatures in X (t), Y (t) form are stored in a database. Which Lee et al. (1996) utilised to develop a dynamic online Verification of signatures system. The authors also said initially extracted a 40 parameter feature set before progressing to set of 49 normalised characteristics that can still distinguish between forgeries and authentic signatures while tolerating irregularities in the former. They looked at strategies for choosing and maybe orthogonal zing features depending on the amount of training data available and the complexity of the system. Several different classifier types were investigated for decision making in study. Using 15 parameter features, In particular, an asymptotic performance to then 5% FAR at 0.80% FRR was achieved by an altered iteration of the majority classifier, which also produced 2.5% EER.

Examined and claimed that his proposed approach was based on these principles, according to Gupta (2006), who cited Nalwa's work. The author also clarifies that three signature databases were utilised to evaluate the suggested technique. The first had 325 expert forgeries and 1004 real signatures from 209 different people. The second collection, which was compiled in a lone session, had 1000 autographs from 102 different people. There were 401 expert forged documents. Several real signatures and forgeries were also taken out of the data set. The third piece of data included 43 signers' 424 expertly forged autographs in addition to 790 real ones. The results from the three test databases and one that applied reference signatures 4, 5, and 6 to all three were displayed. According to the experimental findings, the EER fell between the ranges of 2 to 5%.

A technique for the automated checking handwritten signatures submitted online utilising both global and local attributes was disclosed by Kashi et al. in 1998. For many elements of signature form and production dynamics, both the facets of both the global and local were recorded. The researchers showed that the performance of verification was much enhanced by incorporating a local characteristic in light of the identified signature likely through the globalization of Hidden Markov Models characteristics of a signature. The effectiveness of Verification of signatures techniques evaluated on the Murray Hill database was also mentioned by the author's 542 real signatures and 325 fakes were employed in the test database. Every one of the 59 subjects' first six signatures were utilised in each reference set. There were 32 people who contributed 325 forgeries in all. The best outcome from their study methodology has an EER of 2.5 percent.

According to the researchers developed a technique in which they retrieved particular crucial points for each signature, such as the beginning and end points of a stroke and variations in trajectory points. The authors also made clear that the total number of strokes was employed as a characteristic across the board. The x and y coordinates were used to extract spatial and temporal local characteristics. Two datasets were used to test the suggested approach. 52 authors contributed 10 signatures to the initial dataset, which had 520 total signatures in total. A superset of this dataset, the second dataset includes 1,232 signatures from 102 writers, with 17 of those writers contributing more than ten signatures throughout the course of many sessions spread out over a period of up to a year. After examining an actual signature, twenty authors provided three expert forgeries apiece (for a total of just 60). The best error rates were 3.3% FRR and 2.7% FAR when using a common threshold, and 2.6% FRR and 1.5% FAR when employing writer-dependent thresholds. The FAR rates seemed to be the result of arbitrary forgeries. There were no FARs for expert forgeries.

The authors also said that there were 24 total time sequences identified because of the first and second derivatives of each of these sequences were computed. As a result, 24,000 values would be produced by a signature sample with, let's say, 1000 samples. After normalising the functional data, a zero mean and a single standard deviation were obtained. Hidden Markov Models, based on the sequences, were used to model signatures. A database of signatures from 50 individuals, 15 of which were real and 15 of which were forgeries, was used to evaluate the performance. All tests were run with the same threshold, which produced an EER of 4.83%, which was lowered to 0.98% by applying user-specific criteria.

Dynamic Temporal Warping (DTW) was used in a unique way by map with exact match important components of signatures. First, Alignment of the signatures using the DTW, and the mapping between the signatures was used to match the signature's key points. The signatures were then divided into parts at these precisely matched critical places, and comparisons were carried out between these segments. A condensed version of the Mahalanob is distance was used to calculate the distance between the two. Although the testing process was not entirely obvious, it seemed that a reference signature was found using 6 samples from each signer. Each of the six samples was compared to the other five, and the number of matching points was counted. The reference for the person is therefore the signature with the highest overall matching scores.

An Electronics Verification of Signatures system that employs decision-level fusion to combine local and global information was presented by the authors Fierrez-Aguilar et al. (2005b). Using Parzen Windows Classifiers, international information was retrieved using a depiction based on features. Hidden Markov Models were used to extract local information as time functions of several dynamic features and identify it. The extensive MCYT signature database, which included the signatures of 440 signers and a total of 18500 signatures, provided experimental findings for both random and expert forgeries. On the basis of feature ranking, experiments with feature selection were conducted. Additionally, it was demonstrated that the two suggested systems provide complimentary recognition data that can be successfully used with Fusion of decision-level scores. The experimental findings from the method were encouraging, with expert forgeries EER of 5–7% produced 1% with five training signatures, and 4% with twenty. The sporadic fakes EER, on the other hand, was between 0.5% and 1.5% for 20 training signatures and between 1 and 1.5% for 5 training signatures.

Target dependent score normalization was applied by Fierrez-Aguilar et al. (2005a) on the SVC2004 database, which contains 50 sets of signatures. Every set includes 20 real signatures from one author and 40 expertly faked signatures from five additional contributors achieved with an EER of 7.85%.

Described a method for producing synthetic handwritten signatures in the form use in dynamic Verification of signatures test. Collection of time-stamped pen data channels. Using variance that naturally occurs in real source data, the approach added simulated variability to the created data. In a verification scenario, a commercial dynamic signature engine was utilised to rate the effectiveness of the synthesised pictures. The chosen verification engine's style of operation is to offer a binary judgement on whether a supplied signature is real or fake when checked against a reference template made up of three signatures. Additionally, the degree of confidence connected to this binary result is returned. A default confidence rating of above 80 is considered to be a valid signature. The Verification of signatures Competition's publicly accessible database was utilised to acquire signatures, azimuth, altitude, and time-stamped time -bound X, Y, and pen-on-tablet sequences. The data collection includes representations for forty different signers. 20 files for each signer's signature are actual signatures, while the other 20 are expertly forged copies.

The experiment did not make advantage of the expert forgeries. Individual verification rates of the synthesised signatures with different lengths were evaluated in accordance with their positions during the synthesis cycle in order to investigate this reduced verification performance. Further research revealed that the synthesised signatures 1 and 200 were the interpolations that were most similar, while the remaining 98 signatures were interpolations to seed signatures 1 and 2, using the seeds as a starting point. The synthesised signature 100 was composed of a mid-lane interpolation .according to the researchers. Between positions 23 and 78, it was discovered that the typical rate of verification exceeded the mark of 85.66% attained by signatures.

The dataset comprises of 200 signature donors, from whom 50 real signatures and 50 expertly forged signatures were taken. On the other hand, the Persian dataset was recorded using a digitising tablet with a 150 Hz sample rate.

Table: 1 Percentage outcomes of the experiment.

| | MCYT | | PERSON | |
|---|---|---|---|---|
| | RANDOM | SKILLED | RANDOM | SKILLED |
| FALSE REJECTION RATE(FRR) | 1.10 | 5.50 | 1.30 | 3.05 |
| FALSE ACCEPTANCE RATE (FAR) | 4.9 | 9.10 | 3.45 | 5.15 |
| EQUAL ERROR RATE (EER) | 3.45 | 7.25 | 2.38 | 4.09 |

From 80 signature providers, a total of 800 real signatures were obtained. 400 skilled and 400 random forgeries were also utilised to assess the effectiveness of the method. When making random forgeries, forgers sought to imitate merely the form of the signature, but sophisticated forgeries were discovered when forgers were given access to Animations illustrating the various signature procedures, which they might replay multiple times to become familiar with process of signing. Additionally, for the sake of the experimental setting, the databases of signatures were split test sets and training sets. Form competent forgeries, the training set includes 10 real and 10 fake signatures from the From the Persian database and the MCYT database, there are 6 real and 6 fake signatures. The test set, however, comprises of 480 (12x40) Persian databases and 3000 (30x100) MCYT databases. The same quantity of training sets and other users' signatures were utilised to test the forgery detection in the event of random forgeries. Table 1 displays the experimental results from their suggested system.

## 5. Conclusion

Online signature verification for handwritten signatures very promising the total area of study from both a business perspective and a scientific. Online Verification of signatures has recently gained renewed attention due to the fact that it makes use of a standardised a private confirmation technique that is recognised on a legal and social level, along with the ongoing development of the Internet and the growing need for security protection the development of the e-society. Additionally, recent findings from international contests utilising common databases and testing procedures have shown that Verification of signatures systems may attain an accuracy level comparable to other biometric systems (Vielhauer, 2005), an active signature is one that is written approach that needs the user to carry out the clear act of signing, unlike physiological biometrics. In every application where it is important to validate the transaction and the user, online Verification of signatures is, thus, the most advantageous, As a result, there are ever more potential applications for online Verification of signatures, and a variety of devices with advanced features and a simple interface for online handwriting acquisition are being developed at the same time.

The end of result is that a notable annual rise is anticipated the global market for Verification of signatures will soon have a wide range of possible applications. Ureche and Plamondon, 1999). Evidently, new study findings have significantly advanced the state of the art in the sector, further exaggerating this tendency. However, further efforts are required to be able to strengthen the societal and commercial applications connected utilising electronic verification of signatures. The most significant findings are covered in this article, which also demonstrates the most recent developments in online signature verification. Additionally, some of the most promising lines of study in this area have been highlighted. Research doesn't need to focus only on accuracy and perfection in the future because it has already done so for the most part in the past. Instead, it should focus on a wide range of challenges related to various conditions inside the programme itself.

Since the promise of using electronic verification of signatures, a variety of Online Verification of signatures may no longer be believed to be solely relegated to academics and labs conducting research as applications is becoming a reality during the e-society era. Additional research is unquestionably needed to thoroughly investigate and assess the potential of handwritten signatures, which are still highly distinctive signs that indisputably show the positive reinforcement and involvement of people.

### ACKNOWLEDGEMENT

The heading should be treated as a 3rd level heading and should not be assigned a number.

### REFERENCES

1. Cemil, Oz., 2005. Signature Recognition and Verification with Artificial Neural Network Using Moment Invariant Method. In: Advances in Neural Networks ISNN, Wang, J., X. Liao and Z. Yi (Eds.). Springer-Verlag, New York, ISBN: 978-3-540-25913-8, pp: 195-202.
2. Chang, H.D., J.F. Wang and H.M. Suen, 1993. Dynamic handwritten Chinese Verification of signatures. Proceedings of the 2nd International Conference on Document Analysis and Recognition, Oct. 20-22, Tsukuba Science City, Japan, pp: 258-261
3. Chang, W. and J. Shin, 2007. Modified dynamic time warping for stroke-based on-line Verification of signatures. Proceedings of the 9th International Conference on Document Analysis and Recognition, Sept. 23-26, Curitiba, Parana, Brazil, pp: 724-728
4. Crane, H.D. and J.S. Ostrem, 1983. Automatic Verification of signatures using a three-axis force-sensitive pen. IEEE Trans. Syst. Man Cybernetics, 13: 329-337.
5. De Bruyne, P., 1985. Verification of signatures using holistic measures. Comput. Security, 4: 309-315.
6. Feng, H. and C.C. Wah, 2003. Online Verification of signatures using a new extreme points warping technique. Pattern Recognition Lett., 24: 2943-2951.

7. Fierrez-Aguilar, J., J. Ortega-Garcia and J. Gonzalez-Rodriguez, 2005. Target dependent score normalization techniques and their application to Verification of signatures. IEEE Trans. Syst. Man Cybernetics, Part C: Appl. Rev., 35: 418-425.
8. Fierrez-Aguilar, J., L. Nanni, J. Lopez-Penalba, J. Ortega-Garcia and D. Maltoni, 2005. An on-line Verification of signatures system based on fusion of local and global information. Proceeding of the 5th IAPR International Conference on Audio and Video Based Biometric Person Authentication, July 20-22, Hilton Rye Town NY, pp: 523-532
9. Gupta, G.K. and R.C. Joyce, 2007. Using position extrema points to capture shape in on-line handwritten Verification of signatures. Pattern Recognition, 40: 2811-2817.
10. Gupta, G.K., 2006. The State of the Art in the On-Line Handwritten Verification of signatures. Academic Press, Faculty of Information Technology, Victoria, Australia
11. Gupta, G.K. and R.C. Joyce, 1997. A Study of Some Pen Motion Features in Dynamic Handwritten Verification of signatures. Department of Computer Science, James Cook University, Townsville, Australia
12. Herbst, N.M. and C.N. Liu, 1977. Automatic Verification of signatures based on accelerometry. IBM J. Res. Dev., 21: 245-253.
13. Hastie, T., E, Kishon, M. Clark and J. Fan, 1991. A model for Verification of signatures. Proceedings of the IEEE International Conference Systems, Man and Cybernetics, Oct. 13-16, University of Virginia, Charlottesville, Virginia, pp: 191-196
14. Hu, L. and Y.H. Wang, 2007. On-line Verification of signatures based on fusion of global and local information. Proceedings of the International Conference on Wavelet

Analysis and Pattern Recognition, Nov. 2-4, Beijing, China, pp: 1192-1196

15. Jain, A.K., F.D. Griess and S.D. Connell, 2002. Online Verification of signatures. Pattern Recognition, 35: 2963-2972.

16. Jain, A.K., R.P.W. Duin and J. Mao, 2000. Statistical pattern recognition: A review. IEEE Trans. Pattern Anal. Machine Intell., 22: 4-37.

17. Jain, A., R. Bolle and S. Pankanti, 1999. Biometrics: Personal Identification in Networked Society. 1st Edn., Springer, New York, ISBN-10: 0792383451, Pages: 411

18. Kamel, N.S., S. Sayeed and G.A. Ellis, 2008. Glove-based approach to on-line Verification of signatures . IEEE Trans. Pattern Anal. Machine Intell., 30: 1109-1113.

19. Kashi, R.S., J. Hu, W.L. Nelson and W. Turin, 1998. A hidden markov model approach to online handwritten Verification of signatures . Int. J. Document Anal. Recognition, 1: 102-109.