Fuzzy Signature Verification And Interpretation System Using Stroke Comparator

[1]Dr.K.Vivekanandan, [2]Mrs. C. Meena

Abstract

Off line Signature Verification and Interpretation is an important part of many business processes. Signature Verification and Interpretation is the process of verifying and interpreting the identity of a person by checking the signature against samples kept in a database and helping the user to interpret them. To develop a system that can verify signatures with sample signatures (templates) stored in a database, the proposed system is divided into four components. (i) **Data capture** – the process of converting the signature into digital form as offline procedure (ii) **Preprocessing** –This step is used to reduce noise, to apply filters, to zoom-in/zoom-out an image, etc. The system introduces fuzzy logic to improve the quality of images obtained during preprocessing which greatly enhances the accuracy of the image and significantly helps in refining the image for the process of comparing the signatures. (iii) **Feature Extraction and segmentation** – to obtain the boundaries and partitioning of the signature. (iv) **Comparison and interpretation** – matches the input signature with the templates consisting of three sample signatures. The result given as a fit ratio is obtained by thresholding the fit value. Hamming Distance algorithm is used to justify the threshold value used. The comparison process uses edge detection and pixel matching techniques. The result can be further

improvised by using another threshold value that might have occurred due to changes in the background, varying strokes, etc. The output will interpret whether the signature is accepted or rejected with appropriate explanations. Several approaches to obtain the optimal threshold value from the reference set are investigated.

Keywords : Stroke Comparator, Signature Verification, Signature Interpretation, Segmentation, Fuzzy Logic, Hamming Distance, Preprocessing.

1. INTRODUCTION

The tremendous increase in the use of documents is the most important gifts in modern civilization Society is now growing in such a fashion that document characterizes virtually everything one does or encounters in life. It originates right from the built of a man in the form of birth certificate to death in the form of death certificate. Signature Recognition technologies play a very important role in information processing. Each day, billions of business and financial documents have to be processed by computer [3]. In many instances, acquisition / a dispossession of property depend upon the authenticity of a single signature [11]. Despite electronic payments by credit cards having become so widespread, transactions involving checks, payment receipts, etc., are still increasing throughout the world [2]. Handwriting signature is a learned behaviour acquired by an individual

[1]Reader, School of Management, Bharathiar University, Coimbatore E-mail: kavivek@lycos.com

[2]Research Scholar, Department of Computer Science and Engineering, Bharathiar University, Coimbatore. E-mail : cmeena2003@yahoo.co.in

through continuous practice over a long period of time. After persistent practice it becomes an unconscious act to produce a developed writing, which is peculiar to each individual. This peculiarity differentiates his or her writing from the other persons and cannot be duplicated by any other person. However, writings produced by the same person, even at the same time, under the same conditions are not alike [4]. In such situations Offline Signature Verification System is much needed, where signatures to be verified are compared to prove whether they are authentic or not. Offline systems deal with a static image of the signature. Offline signatures verification and Interpretation system deals with the problem of reading a hand written signature, that is, at some point in time (minutes, months, years) after it was written [23]. Offline handwriting recognition is performed after the writing is completed [1]. A signature verification or recognition system has to be designed to meet a set of requirements in terms of performance and robustness conditions [15]. Signature verification tries mainly to exploit the singular, exclusive, and personal character of the writing. In a typical off line signature verification system a signature image, as scanned and extracted from a bill, a check or any official document is compared with a few signature references provided, for example, by a user at the opening of his account [18].

1.1. Aim of the system

Signature Verification and Interpretation system is an important part of many business processes [11]. One of the important objectives of offline Signature Verification And Interpretation System (SVAIS) is to authenticate a signature by comparing it with reference signatures provided by the signer [19].

Signature verification tries mainly to exploit the singular, exclusive and personal character of the writing [8]. It refers to a specific class of automatic handwriting processing where the specimen signature is compared with signatures collected during enrollment into the system [18]. They are unique, self-initiated, motoric act provides an active means to simultaneously authenticate both the transaction and the transactioner [22].

The SVAIS requires the extraction of writer specific information from the signature signal, irrespective of its hand written content. This information has to be almost time-invariant and effectively discriminant [18]. Most writing systems (alphabet) have significant redundancy, and therefore, it is possible to develop automatic recognizes, that use only part of the shape definition for the recognition [19]. Signature verification has been an active research topic for several decades in the image processing and pattern recognition community [2]. In these applications, the writer of a piece of handwriting is often identified by professional handwriting examiners (graphologist). Although human intervention in text-independent writer identification has been effective, it is costly and prone to fatigue [20]. The purpose of the signature verification and interpretation process is to identify the writer of a given sample, to confirm or reject the sample and give the meaning for confirmation or rejection if necessary.

Machine recognition and verification of signature is a very special and difficult problem. The difficulty [5] arises mainly because the complexity of signature patterns and the wide variations in the patterns of a simple person (i.e. there is no ideal signature shape for any one person), The forged signatures produced by professional forgers may be very similar to the original. Even a well-trained and careful eye may not be able to detect the difference, The difficult conditions under which the actual signing may seriously affect the quality of the signature, The existence of a large number of signatures in the database requires a rapid and efficient searching method [11].

Several types of analysis, recognition, Interpretation can be associated with handwriting. Handwriting recognition and interpretation system objectives are to filter out the variations so as to determine the message [19]. Almost all signature verification systems are used mainly for identifying an individual's authenticity. Each signature has various features that can be used to recognize the writing habits or individual characteristics of a person [14].

1.2. Application areas of the system

This System can be used in many applications such as cheques, certificates, contracts, historical documents [11]. Bankers come across signatures in number of situations. For example, signatures of customer drawer or agent – drawer on cheques, Specimen signature of the account holders, Signature of the bankers on drafts or on a 'certified cheques', etc. [24].

2. MATERIAL AND METHODS

2.1. System Overview

The process of signature verification and interpretation is best illustrated in the following figure - 1 [4].

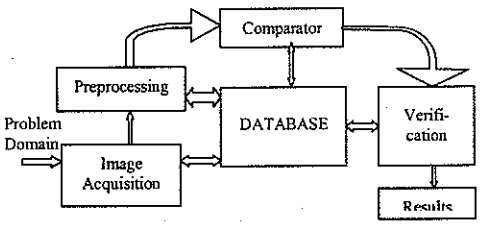


Fig. - 1 : Process of Signature Verification And Interpretation System (SVAIS)

In any signature verification system, the most important step is the conversion of the signature into a digital Image.

2.1.1. Acquisition of the image

A digital image can be considered as a matrix whose row and column indices identify a point in the image and the corresponding matrix element value identifies the gray level at that point. The elements of such a digital array are called, image elements, picture elements, pixels, or pels [9]. Specimen signature image of a person is to be scanned with high resolution, stored and it should be accessible. This process approximately requires the size of the signature image scanned to 200 dpi resolutions with 256 X 256 pixels. The resultant signature image is stored in a Bit Map Picture (BMP) format.

Volunteers were used to collect forged and unforged signatures. Since it was very difficult to find professional forgers, additional volunteers were asked to simulate the true samples of all persons. They were allowed to practice many times and correct their mistakes in the final version of the forged samples. The signatures collected were categorized as

(i) Database signatures - original signatures obtained from signers (3 from 100 signers)

(ii) Specimen signatures - signatures obtained for verification and interpretation purpose

a. Original Specimen – Specimen signatures signed by the original signer (5 from 100 genuine signers)

b. Forgery specimen – Specimen signatures forged by the volunteers (5 from 100 volunteers)

The database was formed with signatures images collected from 100 individuals. Every signer was asked to sign three signature using different types of pens in a limited space on a white sheet of paper. Thus the database was formed with a set of 300 samples signatures. Further to the database collection, specimen signatures were further collected from both the original signer and forged signers to test the validity of the system. Unforged signatures from these 100 individuals were also collected so that genuine signature verification and interpretation could be done. Volunteers were asked to forge these 100 individual's signatures, so that they can be divided into the above-mentioned categories.

2.1.2. Preprocessing methods

Preprocessing a given image is done mainly to obtain an image, which is of better and improved quality than the original image for a specific application. The preprocessing steps are performed once over the whole image before any recognition [12]. Preprocessing methods are used to remove noise, to eliminate much of the variability of signature data. First, a noise filter is applied to the original image in order to improve the robustness against noise introduced in the scanning process [13]. Indeed, a perfect preprocessing system would make the signature of the same person uniform, removing as much noise as possible and preparing the resulting data for feature extraction and classification, thus improving the performance of the recognition and verification system [11]. It is also used to correct any defects in an image, improve the lighting on the image or it makes it bigger or smaller. Preprocessing a given image is done mainly to obtain an image, which is of better and improved quantity then the original image for a specific application. Several preprocessing techniques like Brightness, Contrast and Transparency, Rotation (180°, 90°CW, 90° CCW, quarter turn, Flip horizontal, Flip vertical), Filters (Softening filters, sharpening filters, special filters like Minimum rank filter, Medium rank filter, Maximum rank filter, customer filtering and embossing), Cropping and Resampling [7], Conversion of image modes, Combine and Overlay Text, Edge detection and Line Art, Segmentation [9] [17] and Feature extraction [10] were used in SVAIS.

2.1.3. Fuzzy logic

It is an important algorithm used for all the preprocessing steps automatically to improve the accuracy of the image. Fuzzy image processing is the collection of all approaches that understand, represent and process the images, then segments and features as fuzzy sets. The representation and processing depend on the selected fuzzy technique and on the problem to be solved [25]. There are many reasons to use fuzzy image processing techniques. The most important of them are (i) Fuzzy techniques are powerful tools for knowledge representation and processing and (ii) Fuzzy techniques can manage the vagueness and ambiguity efficiently. In our system, spatial domain methods are used and this process directly involves the pixels of matrix R. In this method, each pixel can be modified independently or can be modified on the basis of pixels in its neighbourhood. In fuzzy image processing methods, matrix $R=\{r_{ij}\}$ of a given image is converted into its fuzzy counter part, $\tilde{R} = [\tilde{r}_{ij}]$, which is then manipulated by appropriate fuzzy operators. The conversion from R to $\tilde{R}$ is usually done by the formula

$$\tilde{r}_{ij} = \left(1 + \frac{\hat{b} - r_{ij}}{\beta}\right)^{-\gamma} \quad (1)$$

For all $i \in N_m$ and $j \in N_n$, where $\hat{b} \in [0, b_{max}]$ is a reference constant defining the degree of brightness for which r_{ij} is l and b, g are positive parameters that affect the conversion formula and one determined from required properties of enhancement operation to be applied in a given image [6].

2.1.4. Method and development of comparison process

The Sign Verification Module (SVM) of the signature verification can be used to compare the specimen signature with the already stored database signature. The working of SVM is shown in the following Figure - 2.

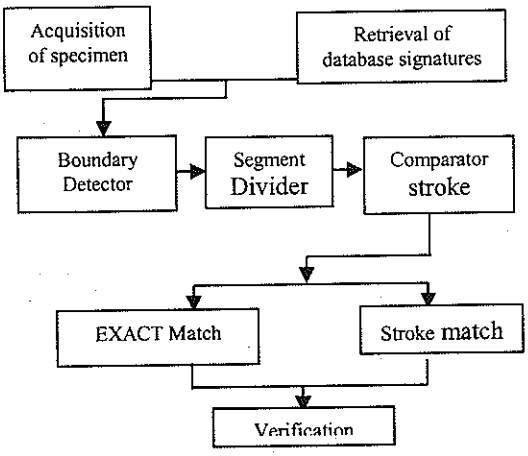


Fig. - 2 : Working of Signature Verification Module (SVM)

2.1.4.1. Boundary detector (BD)

The signature is initially scanned in a left to right fashion and then in a top to bottom fashions to detect the top, left, right most edges of the signatures. This step is repeated for all 4 images, (the specimen and 3 database images). This step crops only that area of the image that actually contains the signature, ignoring all other irrelevant details of the signature. The area that will be cropped approximately reduces the area to be compared by 1/4th of the original image as clear in Fig.-3a and Fig.-3b respectively.

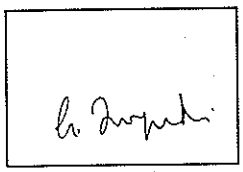


Fig.-3a Original Signature

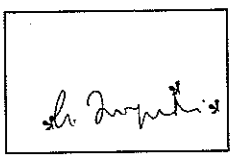


Fig.3b Top, Left, Right most edges detected

The co-ordinates of the 3 points (indicated with * in the above figure) detected as above are fixed as the boundaries of the area to be matched. These images are designated as Edge Detected Specimen image (EDSI), Edge Detected Database Image 1 to 3 (EDDI1-EDDI3). Fig.-4a, 4b, 4c and 4d shows the cropped images.

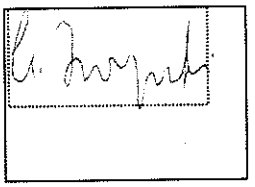


Fig.-4a EDSI

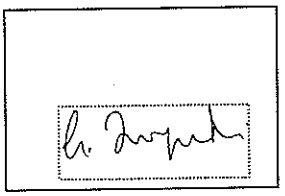


Fig.-4b EDDI1

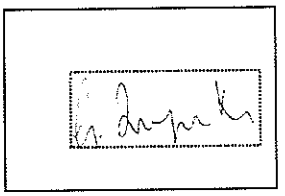


Fig.-4c EDDI 2

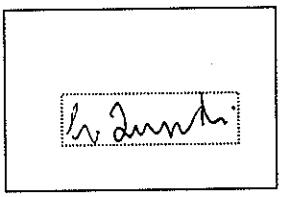


Fig.-4d EDDI 3

The resultant images are shown in Fig.-5a, 5b, 5c, 5d.

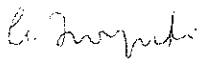


Fig.-5a EDSI

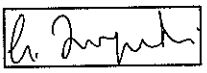


Fig.-5b EDDI1

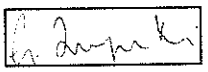


Fig.-5c EDDI2

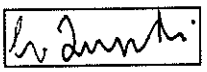


Fig.-5d EDDI3

2.1.4.2 Segment Divider

An image contains various regions corresponding to different objects or their parts in the scene. The pixels comprising a region receive information from points of corresponding object or its part. Since different objects or different parts of the same object have different characteristics, feature values recorded at pixels belonging to various regions should be different. If we map the feature values at every pixels to a feature space, we expect to find distinct clusters formed corresponding to types of regions in the image. Now an appropriate set of boundary functions can isolate each cluster from the others. Consequently, pixels in the image are classified into various regions. Thus the image is segmented. If we consider a single feature then the distribution of pixel values in the feature space is degenerated to a feature

histogram and the boundary function to a threshold. One of the simplest kind of features in gray level image is gray value at a pixel. Thus, image can be segmented by simple gray level thresholding method.

The EDSI and EDDI1 - EDDI3 are divided into equal sized segments/ blocks of size 8 x 8. Diagrammatically it is shown in Fig.-6a, 6b, 6c and 6d respectively.

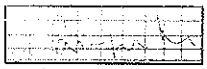


Fig.-6a EDSI

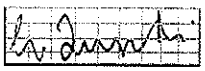


Fig.-6b EDDI1

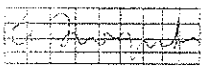


Fig.-6c EDDI 2

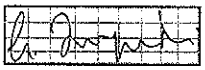


Fig.-6d EDDI3

2.1.4.3. Development of the stroke comparator

(i) Hamming distance

Hamming Distance is a method which is mainly used in areas of encoding and decoding, where the algorithm is used to detect whether retransmission of message has to take place or not. This method mainly identifies or counts the number of error areas in the message being transmitted. In SVM, this algorithm is used to compare stokes in the specimen and database signatures, to count the number of stroke areas differing. This count is then compared with a predefined threshold value (which is taken as ½ the size of the segment size), thus deciding whether to accept the segment as matched one or not. Using Hamming Distance simplifies the comparison process and makes the system simple. If the following is considered as a pixel substring of a segment,

Specimen Signature = 1 1 2 0 2 1 1 2 2

And Database Image 1 = 1 0 2 1 1 2 1 0 2

then, we define hamming distance between these two images as S^n which is the number of places where they differ.

Thus

D(1 1 2 0 2 1 1 2 2, 1 0 2 1 1 2 1 0 2) = 5

The substring is obtained again in a row by row fashion [26].

(ii) Stroke Comparison

The stroke comparator compares the segments in a row-wise fashion, one segment at a time using the following method.

Any signature signed at 2 different times may vary. Keeping this in mind, the stroke comparator performs two types of matching, that is, the exact match and the allowance match. The stroke comparator has been made flexible to include slight variations in the strokes, variations in the thickness of pen tip. This is done using "Allowance Match". These two matches can be calculated in the following manner.

Exact Match Count (EMC) =

$$\begin{cases} EMC & \text{if } (P_1, P_2) \neq 0 \\ EMC + 1 & \text{if } (P_1, P_2) = 0 \end{cases}$$

When $P_1 \neq P_2$,

Allowance Match Count (AMC) =

$$\begin{cases} AMC + 1 & \text{if } (P_1+2, P_2)=0 \text{ or } (P_1-2, P_2)=0 \\ AMC & \text{otherwise} \end{cases}$$

P_1 and P_2 are the pixel values of the signatures and 0 indicates a match in the above mathematical formulae. The comparator initially tries to perform an "exact" match between the strokes with the segment. If an exact match is not made, then it tries performing an "allowance" match. The allowance match flexibility is introduced by giving allowance for a 2-pixel shift (either left or right) that may be caused by the use of a thicker pen (pen's tip is thicker) or by individual variation in the curves of the signature. The allowance was fixed to a maximum threshold of 2 pixels only, so that authentic signatures alone show a match. This 2 pixels threshold also makes sure that

overlapping and curves are avoided. Fig.-7a and 7b are examples of signatures containing slight stroke variation, which are authentic.

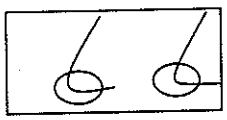


Fig.-7a

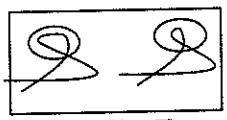


Fig.-7b

Authentic Stroke Variations with slight variations

(iii) Authentic Stroke Variations

The segment matching process results in a match (1) or mismatch (0)

$$\begin{cases} 1 & \text{if EMC + AMC >= y} \\ 0 & \text{otherwise where y = ½ the size of the} \end{cases}$$

segment size

Based upon the result obtained from each segment, a signature is considered to be authentic if the count is greater than or equal to a user defined threshold value and is calculated as below.

The success rate of segment comparator is calculated by using 2 threshold values. The first threshold value is used by the segment comparator and is fixed to be 50% of the block size. A block / segment is considered to be a true match, if both exact match and allowance match count exceeds this threshold value. Taking into consideration both exact and allowance matches, segment counter is calculated as the summation of both exact and allowance match count.

$$SMC = \sum_{i=A}^{n} EMC + AMC,$$ where n is the number of segments.

The second threshold is an user defined threshold and if the segment match counter value exceeds this user defined threshold, then the signature is accepted else it is rejected, that is,

$$\begin{cases} 0 & \text{if SMC > user defined threshold} \\ 1 & \text{otherwise.} \end{cases}$$

2.1.5. Verification and Interpretation

At the end of the verification process, the Signature Verification System helps the user by interpreting the reason for variation in the specimen and database signatures. The various types of interpretation that can be obtained by the proposed system are Stroke variation or pen thickness difference, Difference in the picture format, Pictures may have different dimensions, Pictures may have different color depth, Different surface area and Opinion not given. This interpreted result is much needed, since if the user opts for an exact match to be performed, then the whole of comparison process can be repeated to find an exact match between the specimen and database signatures.

3. RESULTS AND DISCUSSION

3.1. Fuzzy preprocessing

To improve the accuracy of the acquired images, the signature may undergo a series of preprocessing steps. In the proposed system, the fuzzy logic is introduced automatically in all the preprocessing steps. The effectiveness of applying fuzzy logic to preprocessing techniques is evident in Table I which depicts the comparison results of specimen signatures with database signatures I, II and III.

TABLE I

Comparison of signatures before preprocessing, after preprocessing and after fuzzy preprocessing

DATABASE SIGNATURE	BEFORE PREPROCESSING (%)	AFTER PREPROCESSING (%)	AFTER FUZZY PREPROCESSING (%)
I	56	78	99
II	68	89	92
III	70	76	93

The above results clearly indicate that automatically applying fuzzy logic with preprocessing steps in any signature verification and interpretation system improves comparison process, thus producing accurate verification and interpretation results. This fact is supported by the findings reported by [18] and [19] where they have insisted that it is necessary to **perform preprocessing prior to verification in scanned images.**

3.2. Signature verification

3.2.1 Threshold Values

A threshold value is used as a reliability factor to separate the genuine and forgery signatures. It was found that the accuracy of the system was inversely proportional to the threshold value provided by the user during runtime. The comparator module of SVIAS uses this threshold value to compare the three database signatures with the specimen signature to produce the final interpreted result.

TABLE II

Performance comparison of comparator with three user defined threshold values (n=100)

SIGNER	USER DEFINED THRESHOLD VALUE	ACCURACY PERCENTAGE
I	70	95
	75	94
	80	91
II	70	94
	75	93
	80	92

Table II reveals the results of comparing the accuracy of the specimen signatures in percentage against the set of three database signatures. The three threshold values taken into consideration were 80, 75 and 70. The accuracy levels increased from 91 percent to 95 percent as the threshold value decreased.

The system produced 95, 94 and 91 percent accuracy for person I with threshold values 70, 75 and 80 respectively. Similarly for person II, the output accuracy was 94, 93 and 92 percent respectively.

Adding a threshold value as the deciding factor in signature verification is supported by **[57] and [100].**

3.2.2. Testing process

The signature verification and Interpretation system was implemented and tested in the following phases.

FIRST PHASE

FIRST PHASE	
Collection of Samples	- 300
Each person	- 3
Total No. of samples	**- 100**
TEST PHASE	
Collection of Samples	- 1000
Each person	- 10
(4 Genuine & 6 Forgery)	
Total No. of samples	**- 100**
SECOND PHASE	
Collection of Samples	- 1000
Each person	- 100
(40 Genuine and 60 Forgery – 20 Skilled, 20 Unskilled and 20 random)	
Total No. of samples	**- 10**

Upon testing, in most of the cases, signatures of the same person have shown less variation and counterfeit signatures showed a tremendous percentage variation (equivalent to signatures being rejected). The following results are discussed using the results obtained from one person selected randomly from the second phase and the specimen signature and the database signature are given in Fig. 8a, 8b, 8c, 8d and 8e.

Sample signatures of Bhaskaran

Original Signer's Signature Fig. 8a **Forgery Signature Fig. 8b**

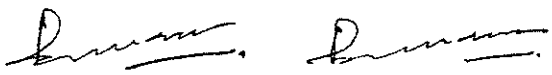


Fig. 8c Fig. 8d

Fig. 8e

Table III shows the results obtained by comparing the specimen signatures consisting of both genuine and forged signatures for person I with database signatures I, II and III respectively.

TABLE III

Comparison of specimen signatures (genuine and forged) with database signature i, ii and iii for person I

Comparison Result (%)	Database Signature I		Database Signature II		Database Signature III	
	Genuine N = 40	Forgted N = 60	Genuine N = 40	Forgted N = 60	Genuine N = 40	Forgted N = 60
Below 40	2	49	2	50	2	52
45 - 75	7	11	8	10	6	8
Above 75	31	0	30	0	32	0

Two genuine signatures were in the category below 40% when compared with database signature I, II and III. While seven, eight and six respectively belonged to the 40-75 percent category and 31, 30 and 32 fit in the category above 75%.

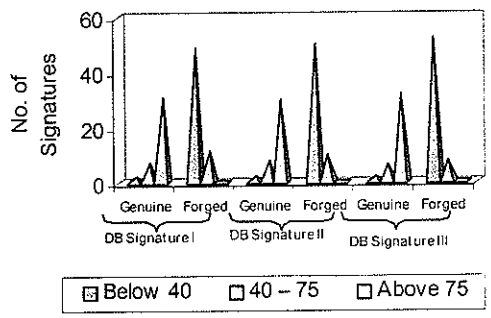
With forged signers, 49, 50 and 52 produced below 40 percent match result, 11, 10, 8 signatures were in the group 40 to 75 percent and no signatures match in the category above 75 percent.

The above results are given graphically in Chart I.

The system produced 95% accuracy for all the three database signatures when compared with the genuine specimen signatures. The accuracy of the system varied for forged signatures when compared with database signatures I, II and III, that is, 90.8%, 91.6%, 93.3% respectively, averaging to an approximate accuracy above 90%.

CHART I

Comparison results of specimen signatures with three database signatures



3.2.3. FAR (False Acceptance Rate) and FRR (False Rejection Rate) of the system

The FAR and FRR were calculated for 100 signatures collected from person I (40 genuine, 60 forged). The comparisons of results were based on three threshold values, 70, 75 and 80. Table IV tabulates the results obtained from SVAIS for threshold values 70, 75 and 80.

TABLE IV

Correct, far and frr results of svais

Type of Signature	Threshold Value 70			Threshold Value 75			Threshold Value 80		
	Correct(%)	FAR %	FRR (%)	Correct(%)	FAR %	FRR (%)	Correct(%)	FAR %	FRR (%)
Genuine	95	-	5	95	-	5	92.5	-	7.5
Jnskilled	95	5	-	95	5	-	90	10	-
Random	100	-	-	100	-	-	100	-	-
Skilled	90	10	-	85	15	-	80	20	-

95%, 95%and 92.5% of person I's genuine signature were correctly identified with threshold values were 70, 75 and 80 respectively. 95%, 95%and 90% of unskilled signatures were correctly identified as forgery signature when the threshold values were 70, 75 and 80 respectively and 90%, 85% and 80% of the skilled signatures were rightly categorized as forgery when the threshold values were 70, 75 and 80 respectively. 100% random signatures were correctly identified as forged signatures in all the threshold values.

The FAR were 5%, 5%, 10% for threshold values 70, 75 and 80 respectively for unskilled forgery whereas they were 10%, 15% and 20% for skilled forgery. The FRR were 5%, 5% and 7.5% with three threshold values 70, 75 and 80 respectively in the case of genuine signatures. Charts IIa, IIb and IIc shows the graphical representation of the above results.

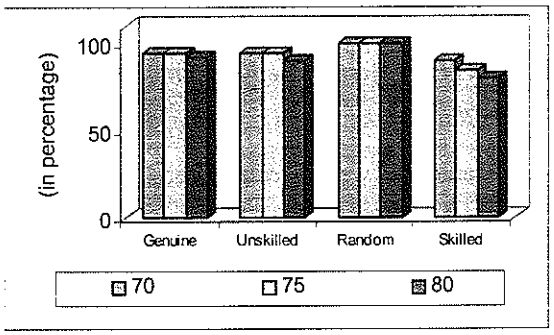


CHART IIa
Correct Signature Vivification Results

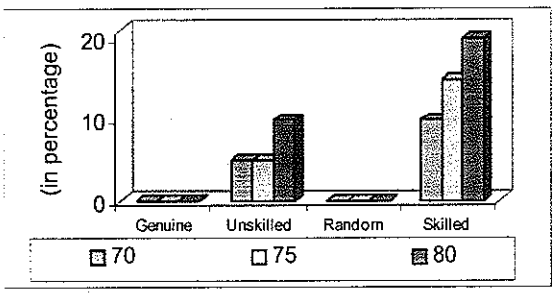


CHART IIb
False Acceptance Rate (Far)

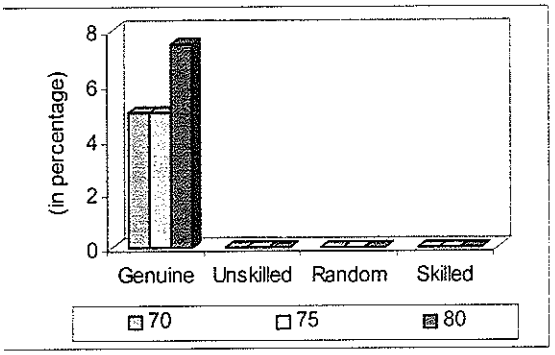


CHART IIc
False Rejection Rate (Frr)

Table V shows the total accuracy percent obtained from SVAIS.

TABLE V
Total accuracy percent, far and frr obtained for the specimen signatures using three user defined threshold values

Category	Threshold 70	Threshold 75	Threshold 80
Correct	95%	94%	91%
FAR	3.75%	4.8%	7.2%
FRR	1.25%	1.2%	1.8%

With threshold value as 70, SVAIS produced 95% accuracy, while the FAR rate was 3.75 and FRR rate was 1.25%. With threshold value was raised to 75, the accuracy decreased to 94% and FAR increased to 4.8 and FRR value was 1.2%. When threshold value was raised to 80, the system efficiency further reduced to 91%, while the FAR and FRR was 7.2% and 1.8% respectively.

Chart III shows the total accuracy percent, FAR and FRR obtained for the specimen signatures using three user defined threshold values for person I.

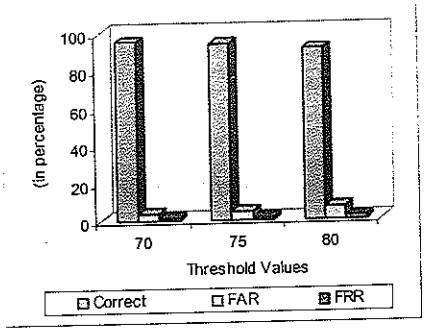


CHART III
Total signature for three Threshold values

3.3. Interpretation

3.3.1 Interpretation results for Threshold Value - 70

Table VI shows the interpretation results in percentage for Threshold value 70.

TABLE VI

Interpretation results in percent for user defined threshold value 70

	Original	Skilled	Unskilled	Random
Full Match	95	6	3	0
Match with two database signatures	1	2	1	0
Match with two of the database signatures	3	0	1	0
Does not match with any of the atabase signatures	0	90	95	100
Opinion not given	1	2	0	0

From Table VI it is clear that the system correctly produced a full match for 95% of the genuine signatures, while 6 and 3 skilled and unskilled forged signs were wrongly accepted. Only one signer's genuine signature fit into the second category (match with one of the database signatures), while 2 of the skilled signatures and one of the unskilled signatures matched with one of the database signatures. Similarly three of the genuine signatures and one of the skilled signatures matched with two of the database signatures. 90 and 95 signatures of the skilled and unskilled forged signatures were rejected because they did not match with any of the database signatures. One genuine signatures and two unskilled signatures went into the category of opinion not given.

3.3.2 Interpretation results for Threshold Value - 75

Table VII shows the interpretation results for Threshold value 75.

TABLE VII

Interpretation results in percent for user defined threshold value 75

Type of Signature	Original	Skilled	Unskilled	Random
Full Match	95	6	2	0
Match with one of the database signatures	0	4	1	0
Match with two of the database signatures	1	2	2	0
Does not match with any of the database signatures	3	86	95	100
Opinion not given	1	2	0	0

From Table VII it can be seen that 95 genuine signers were correctly identified while 6 of the skilled forgers and 2 of the unskilled forgers were erroneously recognized. Four of the skilled and one of the unskilled forgers signatures matched match with one of the database signatures. One of the genuine signatures, two of the skilled and unskilled forgery signatures matched with two of the database signatures. Similarly, three of the genuine signatures and 86 and 90 signatures of the skilled and unskilled forged signatures were rejected because they

did not match with any of the database signatures. Opinion was not given by SVAIS for one genuine signature and two skilled signatures.

3.3.3 Interpretation results for Threshold Value - 80

Table VIII shows the interpretation results for Threshold value 80.

TABLE VIII

Interpretation results in percent for user defined threshold value 80

Type of Signature	Original	Skilled	Unskilled	Random
Full Match	93	13	8	0
Match with one of the database signatures	4	1	1	0
Match with two of the database signatures	2	4	1	0
Does not match with any of the database signatures	0	80	90	100
Opinion not given	1	2	0	0

The results in Table VIII show that 93 of the genuine signers were correctly identified while 21 of the forged signatures (13 skilled and 8 unskilled) mistakenly identified. Four of the skilled and one of the skilled and unskilled signatures forgery matched with only one of the database signatures. Two of the genuine signatures matched with two of the database signatures, along with five (4 skilled and one unskilled) forged signatures. 85 and 90 signatures of the skilled and unskilled forged signatures were rejected because they did not match any of the database signatures. Three signatures (one genuine and two unskilled) did not receive any opinion from the system proposed. The performance of the SVAIS can thus be evaluated as follows : (1) The accuracy of the comparator increases as the threshold value increases and (2) The system is able to produce 95% accuracy while comparing the specimen signature with genuine signatures.

The system is able to produce 90% accuracy while comparing the specimen signature with forged signatures. Similar results were seen in almost all the other cases also. The SVAIS was able to produce a 90% accuracy for finding the forged signatures and nearly 95% accuracy for un-forged signatures. After applying various preprocessing steps on the signature, the comparison process takes only a minimum time to compare the signatures (15 – 25 nanoseconds). The time taken for preprocessing depends on the scanned signature quality and also on the method which the user employs. As accurate result with minimum time is the major requirement of the commercial environment, the SVAIS satisfies both these criteria. Apart from percentage variation, the SVAIS also interprets the comparison result shown in the form of stroke variation or pen thickness difference, difference in the picture format, pictures may have different dimensions, pictures may have different color depth, different surface area.

The SVAIS is a novel approach that was designed and developed for accurate and quick verification and interpretation of the signatures.

4. CONCLUSION

In this paper, a novel based approach is presented to study the performance of signature verification and interpretation system using fuzzy preprocessing techniques, hamming distance algorithm, feature extraction and segmentation. Comparison of signatures gave the result in the form of interpretation with almost 95% accuracy for same person's signature and 90% accuracy for the forgery signatures with minimum speed. The signatures obtained can be improvised by using many

of the filters, sharpening tools given in the preprocessing module. Fuzzy logic is used for all the preprocessing methods to improve the accuracy of the signature image. Also the system interpret the result in the form stroke variation or pen thickness difference, difference in the picture format, pictures may have different dimensions, pictures may have different color depth, different surface area. In general, a stroke is defined as a continuous draw between the pen fall and the pen rise. In this sense, a stroke is treated as a list of line segments with different gradients [10]. The signature verification and recognition algorithm could be made more robust by adding more global descriptors of the signatures that could allow the system to discard coarse forgeries [15]. However, signature verification has the additional disadvantage that a forger with enough information about the true signature and having adequate training could deceive the algorithm. It would also be possible to have a system to improve the accuracy of the images and the stroke variation for identifying the forgery signature in an improved version. Most of the offline successes have come in constrained domains, such as postal addresses, bank checks, and census forms [19]. The system upon testing produced satisfactory results while comparing with the specimen signatures. Therefore, automatic signature verification has the unique possibility of becoming the method of choice for identification in many types of electronic transactions [16].

References

1. Abuhaiba I.S.I and Ahmed P., "*Restoration of Temporal information in offline Arabic Handwriting*", Pattern Recognition, Vol 26, No.7, PP. 1009-1017, 1993.
2. Blodgett, J., "*Beyond check image statements : A new strategy for the 1990s.*", Adv. Imag., Vol. 9, PP. 73-75, Oct. 1994.
3. Ching Y. Suen, Qizhi Xu, Louisa Lam, "*Automatic recognition of hand written data on cheques Fact or Fiction*", Pattern Recognition Letters 20(1999) 1287-1295.
4. Deepti Jindal, Harmeet Kaur and P.K. Chattopadhyay, "*A metric analysis of handwriting: A study of signatures*", International Journal of Forensic Document Examiners, Vol.5, Jan / Dec 1999.
5. Fairhust, M.C., "*Signature Verification Revisited : Promoting Practical Exploitation of Biometric Technology*", Electronics and Communication Engineering, PP 273-280, 1997.
6. George, J. K. and Yuan, B., "*Fuzzy Sets and Fuzzy Logic – Theory and Applications*", Prentice Hall of India Private Limited, New Delhi, 1997, PP. 374-377.
7. Giovanni seni, Rohini K. Srihari and Nasser Nasrabadi, "*Large vocabulary Recognition of online Handwritten cursive words*", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.18, No.7, July 1996.
8. Goddard, A., "*Disappointing verdict on signature software*", New Scientist, Vol. 142, 1994, P.20.
9. Gonzalez, C.R. and Woods, E.R., "*Digital Image Processing*", Addison-Wesley, Fifth Edition, 2000, PP. 7-9.
10. Hung-Pin Chiu, Din-Chang Tseng, "*A novel stroke-based feature extraction for Hand written Chinese character recognition*", Pattern Recognition 32(1999) 1947-1959.
11. Ismail M.A., Samia Gad, "*Offline Arabic signature recognition and verification*", Pattern Recognition 33 (2000) 1727-1740.
12. John T. Favata, "*Offline General Hand written Word Recognition Using an Approximate BEAM Matching Algorithm*", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 23, No.9, September 2001.

13. Junliang Xue, Xiaoqing Ding, Changsong Liu, Rui Zhang and WeiWei Qian, "*Location and Interpretation of destination addresses on hand written Chinese envelopes*", Pattern Recognition Letters 22(2001) 639-656.

14. Kumar, K., "*Russell A. Gregory's Identification of Disputed Documents, Fingerprints and Ballistics*", Eastern Book Company, Law Publishers and Booksellers, Reliance Printers, Lucknow, 4th Ed., 1989, P.7.

15. Leclerc, F. and Plamondon, R., "*Automatic Signature Verification*", Pattern Recognition and Artificial Intelligence, Vol.8, No.3, PP.643-660, 1994.

16. Munich, M.E. and Perona, P., "*Visual Identification by Signature Tracking*", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.25, No.2, Feb. 2003.

17. Nafiz Arica and Fatos T. Yarman-Vural, "*Optical Character Recognition for Cursive Handwriting*", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No.6, June 2002.

18. Nei Kato, Masato Suzuki, Shin'ichiro Omachi, Hirotomo Aso and Yoshiaki Nemoto., (1999). A Handwritten Character Recognition System Using Directional Element Feature and A Symmetric Mahalanobis Distance, IEEE Transactions on Pattern Analysis and Machine Intelligence, March, Vol.21, No.3, Pp.258-270. (Paper No. 87)

19. Plamondon, R. and Lorette, G., "*Automatic Signature Verification and Writer Identification - The State of the Art*", Pattern Recognition, Vol.22, No.2, PP.107-131, 1089.

20. Plamondon, R.and Sargur N. Srihari, "*Online and Offline Handwriting Recognition: A Comprehensive Survey*", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 22, No.1, January, 2000.

21. Said H.E.S, Tan T.N, Baker K.D, "*Personal Identification Based on Handwriting*", Pattern Recognition 33(2000) 149-160.

22. Salim Djeziri, Fathallah Nouboud and Rejean Plamondon, "*Extraction of Signatures from check background based on Filiformity Criterion*", IEEE Transactions on Image Processing, Vol.7, No.10, Oct. 1998.

23. Sansone C. and Vento M., (2000). Signature Verification: Increasing Performance by a Multi- Stage System, Pattern Analysis and Applications 3: Pp.169-181. (No in paper – 100)

24. Sharma B.R, "*Bank Frauds Prevention and Detection*", Sumeroo Publishers Chandigarh First Edition, 1984.

25. Sriganesh Madhvanath and Venu Govindaraju, "*The Role of Holistic Paradigms in Handwritten Word Recognition*", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.23, No.2, February 2001.

26. Truss,J., "*Discrete Mathematics for Computer Scientists*", Addison Wesley Publications, 2000, P.466.

27. Tizhoosh, '*Fuzzy Image Processing*', Springer, 1997.

Dr. K. Vivekanandan received Ph.D. in Computer Science from Bharathiar University in 1996. He is a Reader in Management Sciences, Bharathiar University, Coimbatore. He is also guiding more than 8 Ph.D. Research scholars. He has published more than 25 Research papers in National and International Conferences and Journals.

Mrs. C. Meena Research Scholar, Department of Computer Science and Engineering, Bharathiar University, Coimbatore.