Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 6, June 2021, pg.38 – 59

Adoption of Off-Line Signature Verification and Forgery Detection System Using Additive Fuzzy and TS Modelling Technique in Financial Auditing and Forensics Investigation

[1]Dr. Adeyemi B.M; [1]Olaoye O.J; [2]Dr. Uchehara C.C; [1]Akinola O.M; [3]Sunmola F.O
[1]Department of Computer Science and Cyber Security, Caleb University, Lagos, Nigeria
[2]Department of Accounting and Finance, Crawford University, Igbesa, Ogun State, Nigeria
[3]Department of Information Technology, Federal University of Technology, Akure, Nigeria
Corresponding Authors: adejid2000@yahoo.com, ona_ola@yahoo.com, Chrischigo71@yahoo.com, fosunmola@futa.edu.ng, Ojolaoye@yahoo.com
DOI: 10.47760/ijcsmc.2021.v10i06.004

Abstract: This paper presents a robust signature verification and forgery detection system using Additive fuzzy and TS modeling technique. The features of various handwritten signatures are sampled with proper analysis and encapsulated to devise an effective verification system. Grid method was used to extract features angles for detection of forgeries and verification of genuine signatures.
In financial Accounting, Auditing and Forensic Investigation, signature forgery could occur in various ways. This could be carried out on papers, sales documents such as invoices or inventory procurement requisition paper, title documents on landed property or other tangible assets. It is also perpetrated on payment authorization such as cheques, payment vouchers both in cash and on bills.
During this exercise, the fraud perpetrators perfect their concentration on the surface paper, and trace the original signature from the mandate given earlier. It has been difficult to use accounting and auditing professions to track down financial fraud in Nigeria mostly with the problem of unearthing ingenious fraud.
Exponential membership function was used to fuzzified the derived functions, and modified into structural parameters suitable to adapt to any possible variations that may result from handwriting styles and also to reflect any other factors due to scripting of a signature. The proposed system is tested on a large database of signatures obtained from 40 subjects.
Keywords: Signature verification, Forgery detection, Additive Fuzzy Model, TS-model and Financial Auditing.

1.0 Introduction

A handwritten signature can be defined as the scripted name or legal mark of an individual, executed by hand for the purpose of authenticating writing in a permanent form. The acts of signing with a writing or marking instrument such as a pen or stylus is sealed on the paper. The scripted name or legal mark, while conventionally applied on paper, may also be accomplished using other devices that capture the signature process in digital format.

Ammar, (2015) discusses what a signature is and how it is produced. He notes that the signature has at least three attributes: form, movement and variation. Since signatures are produced by moving a pen on a paper, movement perhaps is the most important aspect of a signature. Movement is produced by muscles of the fingers, hand, wrist, and, for some writers, arm; these muscles are controlled by nerve impulses. Once a person is used to signing his or her signature, these nerve impulses are controlled by the brain without any particular attention to detail.

Centre for Forensic Studies (2010) ,its reports on Nigeria was of the view that forensic accounting practice could be used to reduce the leakages that has been responsible for corporate failures. Signature forgery could be offline or online depending on the one chosen by the fraud perpetrator at the time of Investigation of the signature fraud under review.

Felipe & Busses (2020), forging signature on documents that does not have to be signed in front of someone else may be carried out in different ways. It may be traced by using transmitted light or tracing by making an intended writing of the signature in a piece of paper and thereafter trace it carefully so that there could be no doubt about the name. This could be said to be a formal signature or informal signature on the document under review.

Max & Jay (2015) in another view state that if the questioned document is a forged cheque, the perpetrator during investigation may be asked to fill out 10-20 blank cheques for varying accounts and sign them. This may be as a result of a stolen cheque, depending on the circumstances and magnitude of the amount involved in the fraud incident. In this circumstance, it is suspected that they may have practiced this signature severally before accepting the one to use on the said cheque or document to ensure that it looks closely with the signature needed to be forged.

The variations in handwritten signatures are quite immense, both within samples from the same individual and to an even larger degree across the population of individuals. The susceptibility of a signature to false imitation is clearly a function of the nature of the signature itself. In a broad sense, signatures can be classified as simple, cursive or graphical based on their form and content, as shown in Figure 1.

A simple signature is one where a person scripts his or her name in a stylish manner. In this type of signature, it is very easy to interpret all the characters in the name. Cursive signatures, on the other hand, are more complex. Though the signatures still contain all the individual characters within the name, they are, however, drafted in a cursive manner, usually in a single stroke. Lastly, the signatures are classified

as graphical when they portray complex geometric patterns. It is very difficult to deduce the name of the person from a graphical signature, as it is more of a sketch of the name of the signer (Ammar et al, 2016).

2.0 Problem Statement

It is a well-known fact that no two signatures, even if signed by the same person, are ever the same. However, if two signatures are *exactly* alike, then one of them is not a genuine signature but rather a copy of either a machine copy such as one produced by a computer or photocopier, or a manually produced copy such as tracing. In addition, simulation must be taken into account, where an individual copies the signature of another using a genuine signature as a model. In these cases, the simulated writing usually exhibits an incorrect interpretation of inconspicuous characteristics of a genuine signature, which are quite hard to recognize by a non expert.

Bajaj, (2017), one of the earliest experts in the field of document examination, observed that variations in handwriting are themselves habitual. This is clearly seen in any collection of genuine signatures produced at different times and under a great variety of conditions. When carefully examined, these signatures show that running through them is a marked, unmistakable individuality even in the manner in which the signatures vary as compared with one another.

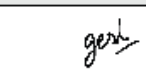
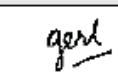
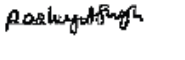
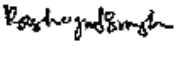
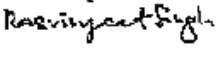
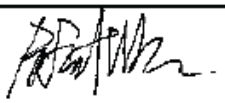
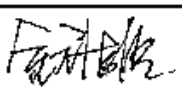
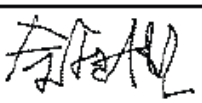
Type	Genuine	Skilled forgery	Unskilled forgery
Simple			
Cursive			
Graphical			

Fig. 1: Types of signatures (Blatzakis, 2011)

He further notes that unusual conditions under which signatures are written may affect the signature. For example, hastily written, careless signatures, cannot always be used unless one has sample signatures that have been written under similar conditions. Furthermore, signatures written with a strange pen and in an unaccustomed place are likely to be different than the normal signatures of a person.

El-Yacoubi, et al (2015), another expert document analyst, surveyed graphometric techniques used for the authentication of questioned documents.

Fadhel, (2016) categorizes the characteristics of genuine handwritten signatures into two broad classes. The characteristic of the second class is the one that is very easily perceived by a casual forger and are

therefore easier to imitate. These are usually the general shape of the signature such as the signatures over all orientation and its position on the document.

Fang, et al (2013) states that the successful forging of a signature or simulating another person's writing by a forger involves, not only copying the features of the genuine signature but also hiding his or her own personal handwriting characteristics. Forgeries in handwritten signatures have been categorized based on their characteristic features (Harrison, 2015). Following are the three major types of forgeries as depicted in Figure 2.

(i) Random forgery: The signer uses the name of the victim in his or her own style to create a forgery known as simple forgery or random forgery. These forgeries represent almost 95% of all the fraudulent cases generally encountered, although they are very easy to detect even by the naked eye

(ii) Unskilled forgery: The signer imitates the signature in his or her own style without any knowledge of the spelling and does not have any prior experience. The imitation is preceded by observing the signature closely for a while.

(iii) Skilled forgery: Undoubtedly the most difficult of all forgeries is created by professional impostors or persons who have experience copying the signature. In order to achieve this, one could either trace or imitate the signature by hard way.

Figure 2. Types of forgeries(Murshed, et al, 2017)

2.1 Handwritten Signature Features

The handwritten signature is a behavioral biometric, which means that the biometric measurement is not based on any physiological characteristic of the individual, but on behavior that can change over time. The process of determining the legitimacy of a handwritten signature is termed *signature verification*. Since an individual's signature alters over time, the use of signature verification for authenticating

sensitive financial transactions over a long period may lead to high error rates. Enrollment to a signature verification system requires the collection of an exclusive set of signature samples that are similar in nature so as to locate an adequate number of common characteristics. Inconsistent signatures lead to high false rejection rates and high enrollment failure rates for individuals who do not sign in a consistent way. However, the positive aspect of signature verification technology is that unlike other physiological biometrics such as face, fingerprint, or iris, if the signature biometrics of an individual are compromised, individuals can simply change their signatures.

In the recent past, many questions have been raised about the scientific basis of the expert opinion offered by forensic document examiners. In order for forensic document examination to retain its credibility and legal acceptability as a science, there must be some statistically sound basis for the decision. In addition, such scientific information is also useful for the efficient development of automatic signature verification systems.

This research is concerned with the automatic analysis of perceptible features in handwritten signatures to determine the features that distinguish a forgery from a genuine signature. In static or off-line signature verification systems, the signature image is characterized as a vector of elements, each one representative of the value of a feature. The careful selection of this feature vector is crucial for the success of any signature verification system.

Types of Features

Features extracted for off-line signature verification can be broadly divided into three main types

i. **Global features** depict or categorize the signature as a whole. These features are usually extracted from all the pixels that lie within the region circumscribing the signature image, such as the length, width or baseline of the signature, although global features are easily extractable and less sensitive to noise, as small distortions in isolated regions of the signature do not cause a major impact on the global feature vector. They are, however, dependent upon the overall position alignment and therefore highly susceptible to distortion and style variations.

ii. **Local features** represent a segment or limited region of the signature image, such as critical junctions and gradients. These features are generally derived from the distribution of pixels of a signature, such as local pixel density or slant. Local features are more sensitive to noise within the region under consideration but unaffected by other regions of the signature. Although they are computationally expensive, they are much more accurate than global features.

iii. **Geometric features** describe the characteristic geometry and topology of a signature, thereby preserving their global as well as their local properties. These features have a high tolerance to alterations and style variations, and they can also tolerate a certain degree of translation and rotation variations.

2.2 General Overview of signature

Features

Many types of features have been proposed for offline signature verification systems with varying degrees of success. Since dynamic information is not available in static signatures, features can only be extracted from the geometric analysis of signatures. Some of the most widely used parameters are the signature image area, the signature height and width, the ratio between the signature height and its width, the ratio between middle zone width and signature width, global and local slant, the number of characteristics points (endpoints, cross-points, cusps, etc.), number of loops, the presence of the lower zone parts, and the number of elements in the signature From this discussion, it is understood that an appropriate combination of global and local features will produce more distinctive and more efficient features, because by localizing global features, the system will be able to avoid major shortcomings of both the approaches and at the same time benefit from their combined advantages.

2.2.1 Data Acquisition

The first step in the design of a static signature verification system is data acquisition. Handwritten signatures are collected from various individuals account owners and some unique features are extracted from them to create a knowledge base for each individual. The features stored in the knowledgebase are then learned by the system and used as a reference for comparing with those of the test signature in the recognition phase. The proposed signature verification system is trained and tested on a database consisting of a total of 1,200 handwritten signature images.

Out of these, 600 are the real account owners authentic signatures, and the other 600 are forgeries. These signatures are obtained from 40 account owners volunteers with each person contributing 15 signature samples, among which 10 are used for learning purposes and the rest for testing as presented in Table 1.

The signatures are handwritten on a white sheet of paper using any type of pen or pencil, and are scanned at a resolution of 300 dpi. A scanned image of the special sheet designed for collecting signatures is shown in Figure

The signatures are collected over a period of four weeks to account for the variations in signature style with time. The forgeries are also collected over the same time frame. The random forgeries are obtained

by supplying only the names of the individuals to the casual forgers who never had any access to the actual genuine signatures.

The unskilled forgeries, in turn, are obtained by providing sample genuine signatures to the forgers, who are then allowed to practice for a while before imitating them to create the forgeries. Each volunteer had to provide five imitations of anyone of the genuine signatures, apart from his or her own signature.

These samples constitute the set of unskilled forged signatures for the set of genuine signatures. We have then requisitioned the services of two expert forgers to provide five forgeries of each genuine signature in the test set so as to create the skilled forged samples of all the persons.

2.2.2 Preprocessing

The signature images scanned during the data acquisition phase are extracted and preprocessed in this module. The steps of preprocessing are briefly discussed in the following sections.

2.2.3 Binarization

Binarization is the first step in preprocessing of signature images. In this process, the input grayscale image is converted into a two-tone image format (i.e., black and white pixels, commonly represented by 1 and 0, respectively).

Table 1. Signature database

Types of Signatures	Training Set	Test Set	TOTAL
Genuine signatures	40 x 10	40 x 5	600
Skilled forgeries	-	40 x 5	200
Unskilled forgeries	-	40 x 5	200
Random forgeries	-	40 x 5	200

2.2.4 Slant Normalization

A practical signature verification system must be able to maintain high performance regardless of the size and slant of a given signature. For handwritten signatures, one of the major variations in writing styles is caused by slant, which is defined as the slope of the general writing trend with respect to the vertical line. It is important that the system be insensitive to slant; hence, the need for slant correction in the signature image. The image matrix is divided into upper and lower halves. The centers of gravity of the lower and upper halves are computed and connected.

The slope of the connecting line defines the slope β of the window (image matrix). The slant-corrected image is obtained by applying the following transformation to all black pixels with coordinate points *x*, *y* in the original image:

$$x' = (x - y) \times \tan(\beta - \beta_0), y' = y \qquad (1)$$

where x' and y' are slant corrected coordinates and β_0 is a parameter specifying the default (normal) slant.

Slant correction needs to precede other preprocessing tasks (i.e., it is applied before smoothing), because smoothing tends to change the image topology, and the correction operation usually creates rough contours to the character.

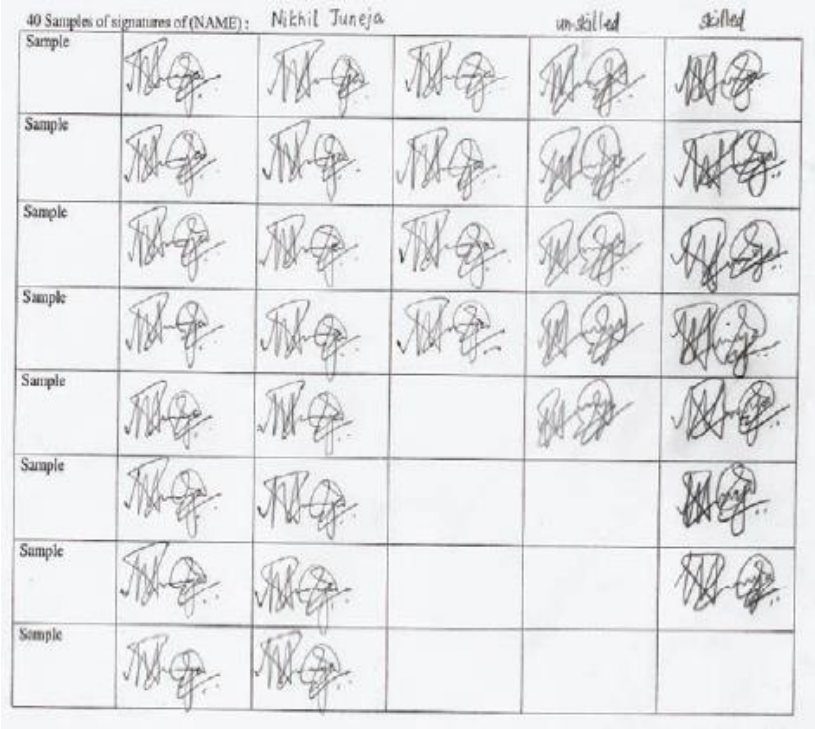


Fig.3: Signature Data Acquisition

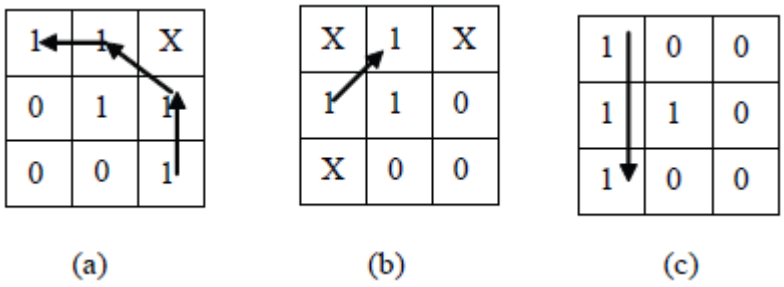


Figure 4. Smoothing using maintenance of connectivity

Determined path length. If correctly chosen, it gives some spectacular results. However, incorrectly chosen lengths would either leave the image unaffected or may delete branches that should not be deleted otherwise.

2.2.5 Size Normalization

After the binarization process, there would be extra zeros on all four sides of the signature image, as zero padding is applied during binarization.

To standardize the size of the signatures, extra rows and columns containing only zeros are removed from all four sides of the image.

Normalization is thus the process of equating the size of all signature samples so as to extract features on the same footing. To achieve this, we use standard bilinear transformation, by which every input bitmap P of size $m \times n$ is transformed into a normalized bitmap Q of size $p \times q$. Both p and q are quadrilateral regions. All the signature images are standardized to a fixed window of size120 x 60 pixels.

2.2.6 Feature Extraction

The success of a pattern recognition system depends largely on the type of features extracted from the dataset. The chief objective of this process is to extract those features that will enable

the system to correctly discriminate one class from the other. In this section, we will present our signature grid method, which has been devised for extracting innovative angle and distance features. The motivation behind the design of the grid is illustrated to prove its efficacy. Edge-based direction features adopted from handwriting recognition are also discussed.

Grid-based Approaches

The structural information contained in a handwritten signature is obtained using a grid that is superimposed on the size-normalized signature image. The feature vector of each grid element includes the boundary code and the total number of pixels inside the grid. The boundary grid is a binary vector that is defined as:

$b_i = \{^{1}_{0}$ 1 pixel at ith position> 0 otherwise (2)

where *bi* is the distance from the upper-left corner of each grid when moving counterclockwise on the boundary. The length of the boundary code is equal to four times the side of each square grid. This boundary code is an incomplete, linear approximation to the structure within each grid when the size of the grid is relatively small, because there are multiple ways to linearly connect a given set of boundary locations within a grid. To alleviate this ambiguity, the intersection between the line stroke and the grid is

thinned so each intersection is represented by only one code element *bi*. The total grid feature is thus represented as:

$$v_{g=(n,b_1,b_2,....b_{41})}\ b_1 \in (0,1)\forall_i \qquad (3)$$

where *n* is the total number of pixels within each grid, and *l* is the side length (in pixels) of the squared grid. Murshed, et al. (1997) performed a local analysis of the shape of a signature within a predefined search region called the identity grid, which is designed for each writer in the system. The signature image is centralized on the identity grid, which is divided into nine regions that are further divided into squares of size 16 x 16 pixels. The *xy*-coordinates of each 16 x 16-pixel square indicate a location of a graphical segment in the identity grid of a particular writer. Feature extraction is performed on each of the 16 x 16- pixel squares that contain a graphical segment by first calculating the center of the square and then extracting the graphical segment enclosed within the 32 x 32-pixel square. A signature image of 512 x 128 pixels is centered on a grid of rectangular retinas, which are excited by local portions of the image (see Figure 5). Each retina has only a local perception of the entire scene, and granulometric size distributions are used for the definition of local shape descriptors in an attempt to characterize the amount of signal activity exciting each retina on the focus of the attention grid.

In Quek and Zhou (2002), the skeletonized image is divided into 96 rectangular segments and for each segment; area (the sum of foreground pixels) is calculated. The results are normalized so the lowest value (for the rectangle with the smallest number of black pixels) would be zero, and the highest value (for the rectangle with the highest number of black pixels) would be one. The resulting 96 values form the grid feature vector. A representation of a signature image and the corresponding grid feature vector is shown in Figure 6. A black rectangle indicates that for the corresponding area of the skeletonized image, there would be the maximum number of black pixels. On the contrary, a white rectangle indicates the smallest number of black pixels.

3.0 Methodology

Signature Grid Method

The signature grid is defined as the region of interest within which the signature image is enclosed. The size of the grid, therefore, depends on the signature being enclosed within it. The grid is divided into eight partitions, which in turn are subdivided into 12 equal boxes. The chief motivation behind the use of a signature grid is to divide the signature into local regions or boxes, which, over a set of all samples of a writer, form a fuzzy set. In this way, we areable to capture the global behavior through the local features, which forms an intelligent knowledgebase of unique features for a particular individual. The other motivation for designing the grid is to reduce the area of focus to just the signature image.

Figure 5. A signature image centered on a grid of rectangular retinas

Figure 6. The grid feature vector for a signature

The preprocessed image is partitioned into eight portions using the equal horizontal density method. In this method, the binarized image is scanned horizontally from left to right and then from right to left, and the total number of dark pixels is obtained over the entire image. Thepixels are clustered into eight regions such that an approximately equal number of dark pixels falls in each region. This process, known as the horizontal density approximation method, is illustrated in Figure 7.

From Figure 7, we note that the total number of points (dark pixels) is 48. If we divide the total pixels by four, we obtain 12 pixels per partition. Since the partition is done column wise, obtaining exactly 12 points in each partition is difficult. Therefore, we take approximately 12 points in each partition using a two-way scanning approach. In this method, we scan the image from left to right until we reach the column where the number of points in a particular partition is 12 or more. We repeat the same procedure while scanning the image in a right-to-left direction. Then we partition the image in both directions: from left to right and right to left. Next, we take the average of two column numbers in each partition. Each partition is now resized to a fixed window of size38 x 60 pixels and is thinned again. This partition is again subdivided into four rows and three columns, constituting 12 boxes. In total we have 96 boxes for a

single signature. This approach is termed the signature grid method. The idea behind this method is to collect the local information contained in the box.

3.1 Signature Grid Features

Signature grid features are extracted using the signature grid method, which is based on the spatial division of the signature image. The signature is initially preprocessed and partitioned using the signature grid, as explained in the previous sections. The signature grid is divided into 96 (12 x 8) equal boxes superimposed on the signature image. The bottom left corner of each box is taken as the absolute origin (0,0), and distance and angle features are computed with reference to the origin of the box. The vector distance for *k*th pixel in *b*th box at location (*i*, *j*) is calculated as: this method is to collect the local information contained in the box.

3.2 Signature Grid Features

Signature grid features are extracted using the signature grid method, which is based on the spatial division of the signature image. The signature is initially preprocessed and partitioned using the signature grid, as explained in the previous sections. The signature grid is divided into 96 (12 x 8) equal boxes superimposed on the signature image. The bottom left corner of each box is taken as the absolute origin (0,0), and distance and angle features are computed with reference to the origin of the box. The vector distance for *k*th pixel in *b*th box at location (*i*, *j*) is calculated as:

$$d_k^b = \sqrt{\left(i^2 + j^2\right)} \tag{4}$$

These vector distances constitute a set of features based on distance. Similarly, for each *k*thblack pixel in a box at location (*i*, *j*), the corresponding angle is computed in a similar manner. By dividing the sum of distances of all black pixels (having value '1') present in a box with their total number, a normalized vector distance, γ_b, for each box is obtained as:

$$\gamma_b = \frac{1}{n_b} \sum_{k-1}^{n_b} d_k^b \tag{5}$$

where, n_b is number of pixels in *b*th box.

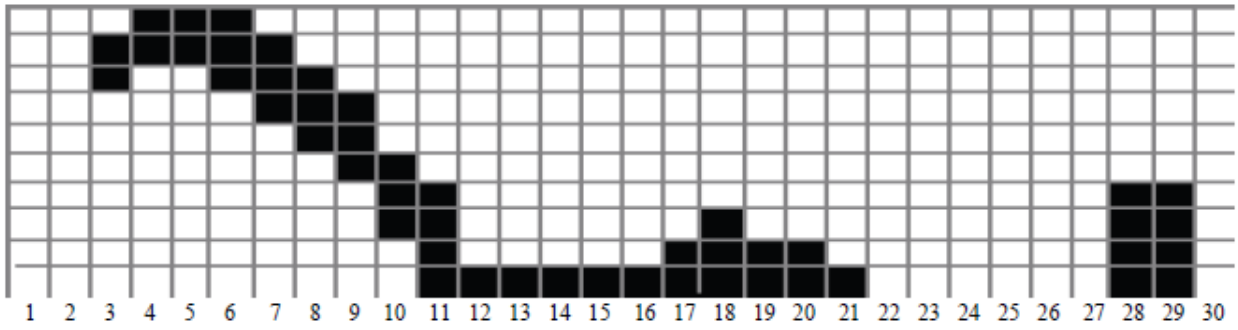


Figure 7. Partition using horizontal density approximation method

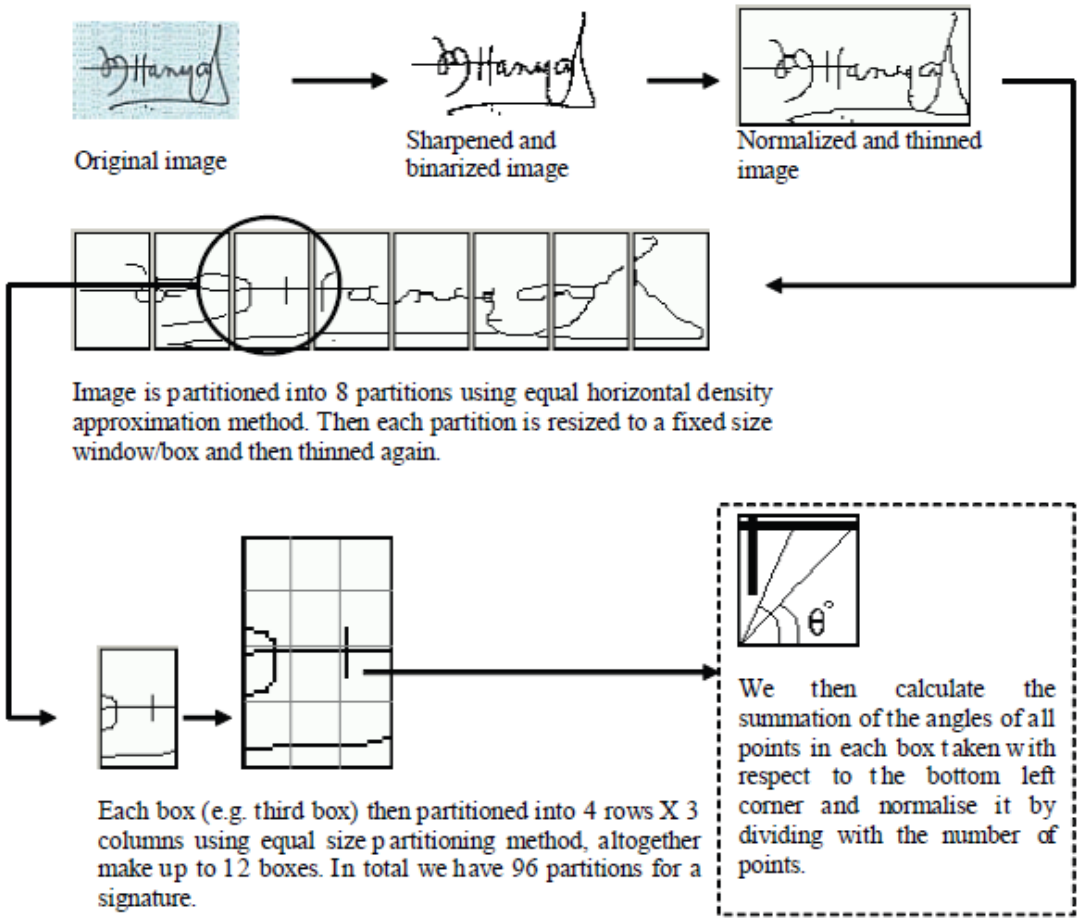


Figure 8. Preprocessing and feature extraction

Then the sum of all angles in a box *b* is divided by the number of 'l' pixels present in that box to yield a normalized angle *b* : Then the sum of all angles in a box *b* is divided by the number of 'l' pixels present in that box to yield a normalized angle *b* : Then the sum of all angles in a box *b* is divided by the number of 'l' pixels present in that box to yield a normalized angle *b* :1

$$\gamma_b = \frac{1}{n_b}\sum_{k=1}^{n_b}\theta_k^b \qquad (6)$$

where, *nb* is number of pixels in *b*th box. The angle and distance features obtained from all 96 boxes constitute the complete feature set of a particular signature sample. For the present problem of signature verification and forgery detection, we have experimented with both distance and angle distributions. However, it is found that the angle distribution is better than distance distribution due to its nonlinearity as depicted in figure 9.

Hence, the choice fell on extracting angle information from the boxes. We now discuss the Then the sum of all angles in a box *b* is divided by the number of 'l' pixels present in that box to yield a normalized angle *b* :

4.0 Test and Result: Verification System

Automatic verification of handwritten signatures on bank checks is integral to the success of a bank check processing and authentication system. The focus of this paper is hence on the development of an automatic system for verification and forgery detection of handwritten signatures extracted from paper documents using The features considered in the recognition system are angle and distance features. Sharpened and Original image binarized image Normalized and thinned image is partitioned into 8 partitions using equal horizontal density approximation method. Then each partition is resized to a fixed size window/box and then thinned again. Each box (e.g. third box) then partitioned into 4 rows X 3 columns using equal size partitioning method, altogether make up to 12 boxes. I n total we have 96 partitions for a signature.

We then calculate the summation of the angles of all points in each box taken with respect to the bottom left corner and normalize it by dividing with the number of points.

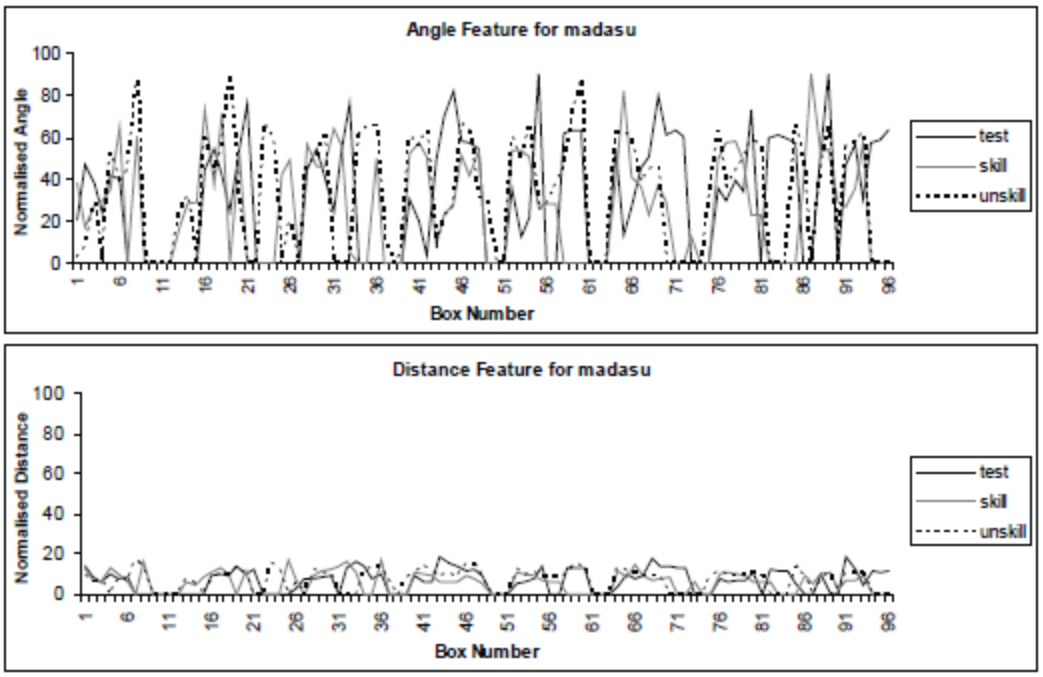


Figure 8. Preprocessing and feature extraction

Table 2. Angle features of one of the signatures used for training

Partition Cluster	1	2	3	4	5	6	7	8	9	10	11	12
1	21.1	46.8	38.1	23.9	41.6	40.1	0	0	0	0	0	0
2	0	0	0	44.8	54.8	41.7	24.7	54.5	76.1	0	0	0
3	0	0	40.1	46.9	39.8	0	72.4	60.2	21.0	46.1	56.4	0
4	0	0	30.5	20.5	3.7	49.4	70.2	81.9	58.0	57.5	54.2	0
5	0	0	35.6	12.7	21.3	90	0	0	61.6	63.3	63.3	0
6	0	0	54.7	13.6	26.9	45.6	50.6	79.9	60.9	63.3	60.5	0
7	0	0	36.1	30.1	39.4	33.9	73.4	0	59.6	61.3	59.6	57.4
8	0	0	52.1	90	0	47.1	56.6	30.7	57.4	59.1	63.3	0

The verification system is based on the Takagi- Sugeno (TS) fuzzy model (Takagi & Sugeno, 1985). A Takagi-Sugeno fuzzy inference system is well suited to the task of smoothly interpolating the linear gains that would be applied across the input space; it is a natural and efficient gain scheduler. It is also suitable for modeling nonlinear systems by interpolating multiple linear models. A graphical representation of a TS model is illustrated in Figure 10.

Signature verification and forgery detection are carried out using angle features extracted from the signature grid. Each feature corresponds to a fuzzy set over all the samples of the training set. The features are fuzzified by an exponential membership function involved in the TS model, which is modified to include structural parameters to account for variations in signing styles.

The membership functions constitute weights in the TS model. The optimization of the output of the TS model with respect to the structural parameters

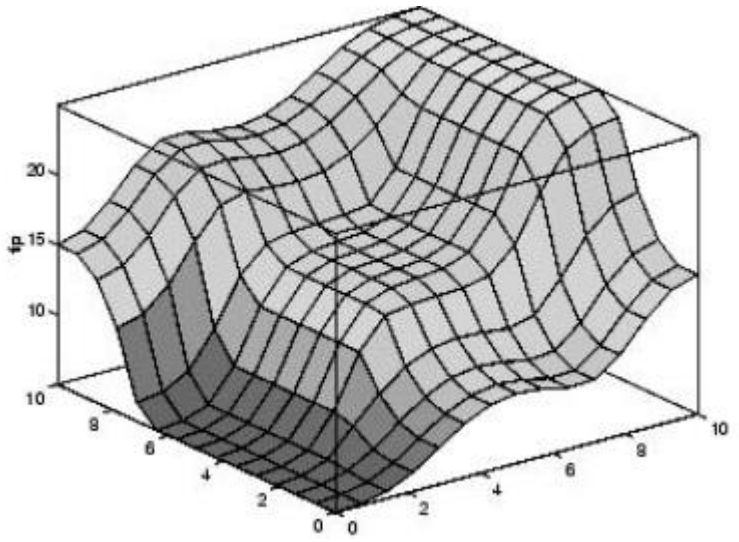


Figure 10. Takagi-Sugeno fuzzy model

yields the solution for the parameters. The simplified form of the TS model is derived by fixing the coefficients of consequent parts of the rules made up of all input features and also by considering a single rule for all input features.

4.1 System Design

The proposed system includes both signature verification and forgery detection modules. The difference between them is that verification is based on inherent characteristics of a signer, whereas detection is based on specification of a limit, which exceeds the inherent variation in the genuine signatures of a signer. Various categories of forgery arise, depending on the limit of variation allowed over the inherent variation. The various phases of the verification and detection are discussed in the following sections.

4.2 Model Formulation

Since the main thrust here is to establish the genuineness of the signature, thereby detecting the forgeries, we have employed the additive fuzzy model for this purpose. In this study, we consider each feature as forming a fuzzy set over large samples, because the same feature exhibits variation in different samples

giving rise to a fuzzy set. So our attempt is to model the uncertainty through a fuzzy model such as the additive fuzzy model. The overall system organization is depicted in Figure 11.

4.3 The First Formulation

Let x_k be the *k*th feature in a fuzzy set A_k, so the *k*th IF THEN fuzzy rule in the TS model has the following form:

Rule k: IF x_k is A_k

THEN $y_k = c_k + c_{k1} x_k$ (7)

Each feature will have a rule, so we have as many rules as the number of features. The fuzzy set A_k is represented by an exponential membership function (MF) that includes two structural parameters, *sk* and *tk*. This membership function is expressed as:

$$\mu_k(x_k) = \exp - \left[\frac{(1 - s_k) + s_k^2 \mid x_k - \overline{x_k} \mid}{(1 - t_k) + t_k^2 \sigma_k^2} \right] \quad (8)$$

where $\overline{x_k}$ is the mean, and σ_k^2 is the variance of *k*th fuzzy set.

The structural parameters are included in the TS model so as to track the intra-class variations in *Figure 10. Takagi-Sugeno additive fuzzy model*

Parameter		Simplified TS Model Initial Values		TS Model Initial Values
s		0.1		1
t		1.4		2
c_0		1/96		1/96
c_1		0		0
ε_1		-		0.00000001
ε_2		0.01		0.01
ε_3		0.01		0.01
Precision		**0.01**		**0.01**

Table 3. Initial values of the structural and learning parameters

Signature Type	Total	Accepted	Rejected
(a) *J*			
Genuine	200	200 (100%)	0 (0%)
Skilled forgery	200	0 (0%)	200 (100%)
Unskilled forgery	200	0 (0%)	200 (100%)
Random forgery	200	0 (0%)	200 (100%)
(b) *Average J*			
Genuine	200	184 (92%)	16 (8%)
Skilled forgery	200	44 (22%)	156 (78%)
Unskilled forgery	200	8 (4%)	192 (96%)
Random forgery	200	0 (0%)	200 (100%)
(c) *Maximum J*			
Genuine	200	200 (100%)	0 (0%)
Skilled forgery	200	42 (21%)	158 (79%)
Unskilled forgery	200	6 (3%)	194 (97%)
Random forgery	200	0 (0%)	200 (100%)

Table 4. Results using formulation 1 with fixed consequent coefficients

Signature Type	Total	Accepted	Rejected
(a) Average J			
Genuine	200	172 (86.0%)	28 (14%)
Skilled forgery	200	47 (23.5%)	153 (76.5%)
Unskilled forgery	200	8 (4%)	192 (96.0%)
Random forgery	200	0 (0%)	200 (100%)
(b) Maximum J			
Genuine	200	200 (100.0%)	0 (0%)
Skilled forgery	200	44 (22%)	156 (78%)
Unskilled forgery	200	6 (3%)	194 (97.0%)
Random forgery	200	0 (0%)	200 (100%)

Table 5. Results using formulation 1 with coefficients adapted

Signature Type	Total	Accepted	Rejected
(a) *Fixed Consequent coefficients*			
Genuine	200	125 (62.5%)	75 (37.5%)
Skilled forgery	200	68 (34%)	132 (66%)
Unskilled forgery	200	51 (25.5%)	149 (74.5)
Random forgery	200	50 (25%)	150 (75%)
(b) *Adapted Consequent coefficients*			
Genuine	200	107 (53.5%)	93 (46.5%)
Skilled forgery	200	84 (42%)	116 (58%)
Unskilled forgery	200	68 (34%)	132 (66%)
Random forgery	200	45 (22.5%)	155 (77.5%)

Table 6. Results using formulation 2

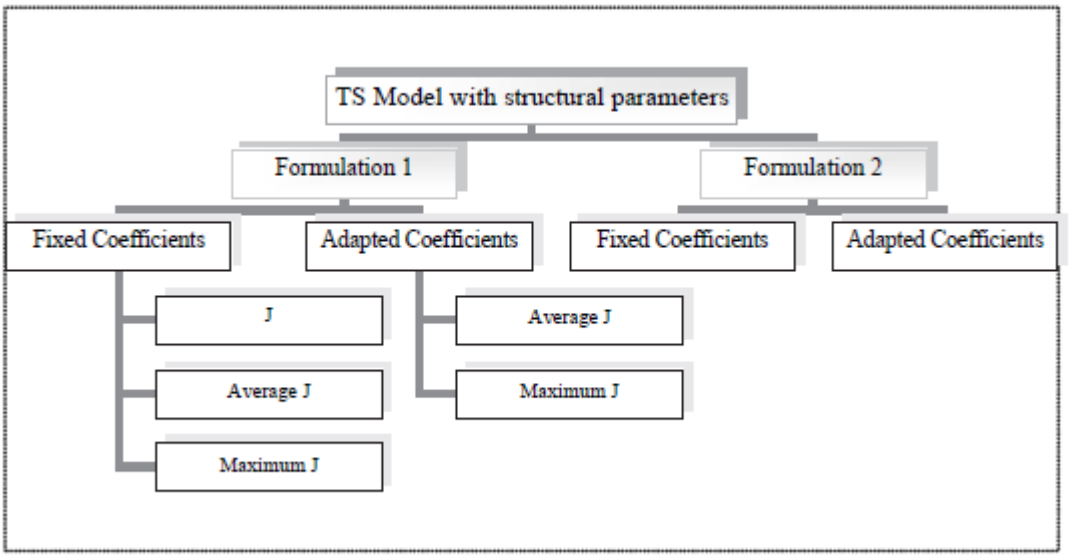


Figure 11. System organization

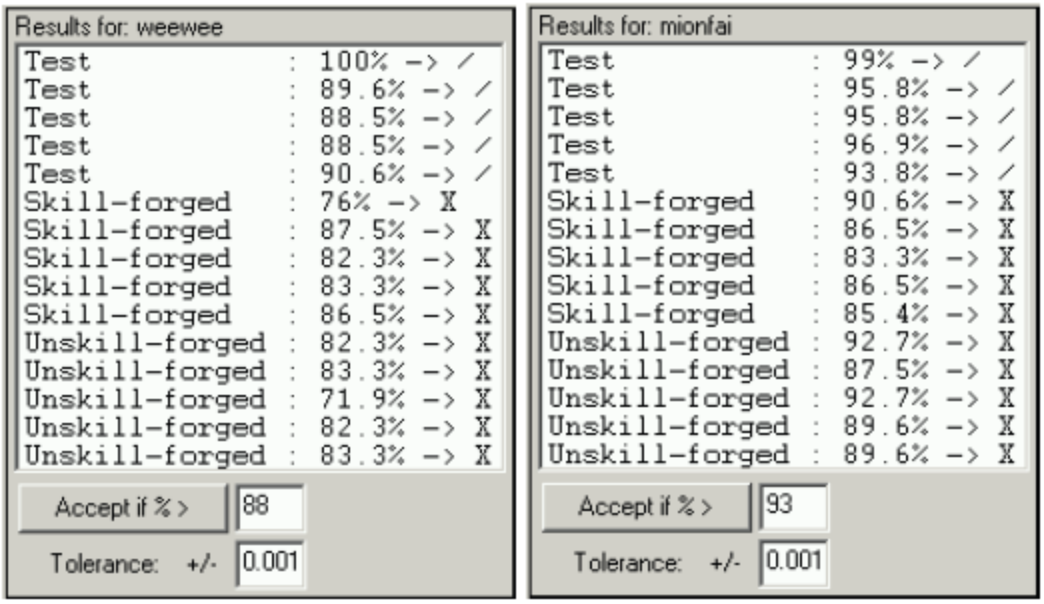
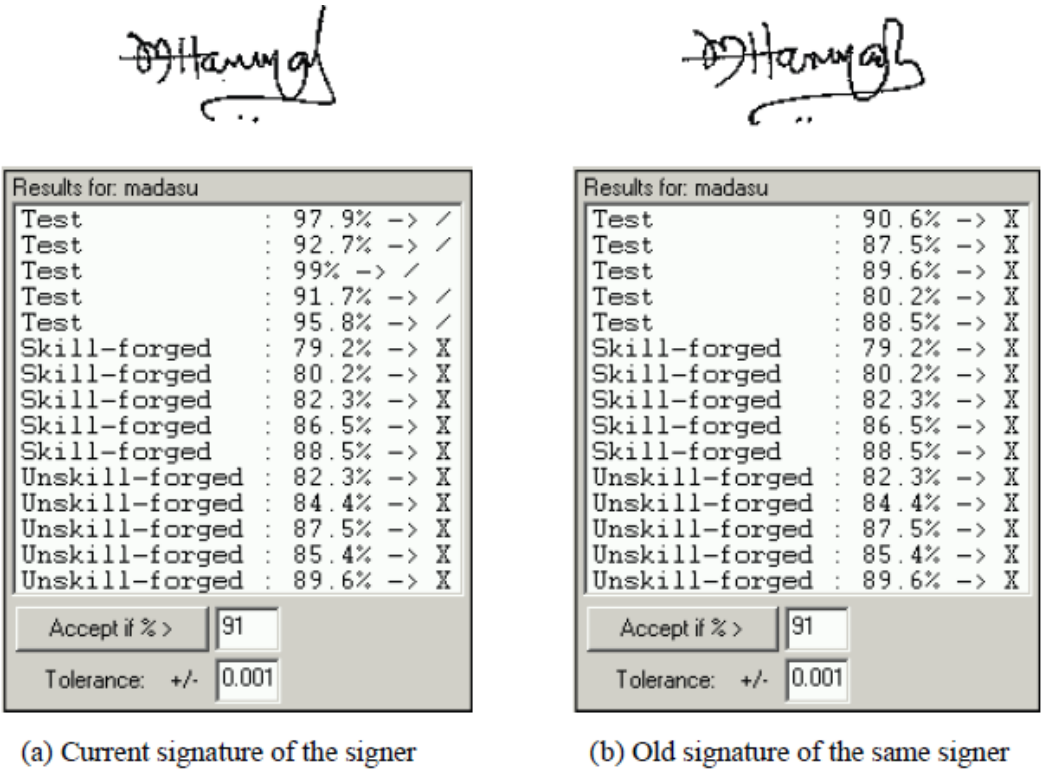


Figure 13. Sample outputs from the program for the signer (a) Weewee (b) Mionfai



(a) Current signature of the signer

(b) Old signature of the same signer

Figure 14. Sample outputs from system showing the old signatures are treated as forged when the thresholds of the current signatures are applied

5.0 Conclusion

In this paper, an off-line signature verification and forgery system based on additive fuzzy and TS modeling is presented. The handwritten signature images are preprocessed and angle features extracted from them via a novel grid method. These features are then modeled using the Takagi-Sugeno fuzzy model, which involves two structural parameters in its exponential membership function. Each angle feature yields a fuzzy set when its values are gathered from all samples because of the variations in handwritten signatures. Two cases are considered. In the first case, the coefficients of the consequent part of the rule are fixed so as to yield a simple form of the TS model, and in the second case, the coefficients are adapted. In this formulation, each rule is constituted by a single feature. In the second formulation, we consider only one rule encompassing all the features. Here again, we have derived two models(Additive Fuzzy and TS), depending on whether coefficients of the consequent part are fixed or adapted. However, this formulation is not implemented, as the membership values are found to be very small for some fuzzy sets.

The efficacy of this system has been tested on a large database of account owner signatures. The verification system achieved 100% success in verifying genuine signatures and detecting all types of forgeries (i.e., random, unskilled, and skilled) on a signature database consisting of 1,200 signature samples. A simple form of the TS model in the first formulation is found to be better than that with coefficients adapted. We have also demonstrated the effectiveness of the intuitive approach for signature verification over other approaches using the performance index.

References

[1]. Ammar, M. (2015). Progress in verification of skillfully simulated handwritten signatures. International Journal of Pattern Recognition and Artificial Intelligence, 5(1-2), 337–351.

[2]. Ammar M., Yoshida, Y., &. Fukumura, T. (2016). Structural description and classification of signature images. Pattern Recognition, 23, 697–710.

[3]. Bajaj, R., & Chaudhury, S. (2017). Signature verification system using multiple neural classifiers. Pattern Recognition, 30(1), 1–7.

[4]. Blatzakis, H.,& Papamarkos, N. (2011). A new signature verification technique based on a two stage neural network classifier. Engineering Applications of Artificial Intelligence, 14, 95–103.

[5]. el-Yacoubi, A., Justino, E.J.R., Sabourin, R., &Bortolozzi, F. (2015). Off-line signature verification using HMMS and cross-validation.

[6]. Felipe and Busses 2020 Proceedings of the Ninth IEEE Workshop on Neural Networks for Signal Processing, 859–868.

[7]. Fadhel, E.A., &. Bhattacharyya, P. (2016). Application of a steerable wavelet transform using neural network for signature verification. Pattern Analysis and Applications, 2, 184–195.

[8]. Fang, B., Leung, C.H., Tang, Y.Y., Tse, K.W., Kwok, P.C.K., & Wong, Y.K. (2013). Offline signature verification by tracking of feature and stroke positions. Pattern Recognition, 36, 91–101.

[9]. Harrison, W.R. (2015). Suspect documents: Their scientific examination. London: Sweet &Maxwell Ltd.

[10]. Murshed, N.A., Sabourin, R., & Bortolozzi, F. (2017). A cognitive approach to offline signature verification. In H. Bunke & P.S.P. Wang (Eds.), Automatic bankcheck processing (pp. 339–364). Singapore: World Scientific Publishing.

[11]. Nagel, R.N., & Rosenfeld, A. (2016). Computer recognition of freehand forgeries. IEEE Transactions on Computers, 26(9), 895–905.

[12]. Nemcek, W.F., & Lin, W.C. (2015). Experimental investigation of automatic signature verification. IEEE Transactions on Systems, Man and Cybernetics, 4, 121–126.

[13]. Shih, F.Y., & Wong, W.-T. (2015). A new safe-point thinning algorithm based on the mid-crack code tracing. IEEE Transactions on Systems, Man and Cybernetics, 25(2), 370–378.

[14]. Suen, C.Y., Xu, Q., & Lam, L. (2014). Automatic recognition of handwritten data on cheques—Factor fiction? Pattern Recognition Letters, 20, 1287–1295.

[15]. Takagi, T., & Sugeno, M. (2015). Fuzzy identification of systems and its application to modeling and control. IEEE Transactions on System, Man and Cybernetics, 15, 116–132.

[16]. Xiao, X., & Leedham, G. (2012). Signature verification using a modified Bayesian network. Pattern Recognition, 35(5), 983–995.

