International Journal of Security and Its Applications
Vol.9, No.9 (2015), pp.141-150
http://dx.doi.org/10.14257/ijsia.2015.9.9.13

Comparative Analysis of Offline Signature Verification System

Deepti Yadav[1] and Ranbeer Tyagi[2]

[1]*Research Scholar of EC, MPCT College, Gwalior, India*
[2]*Assistant Prof.,Department of EC, MPCT College, Gwalior, India*
deepti02yadav@gmail.com[1], ranbeertyagi85@gmail.com

Abstract

A digital signature is a mathematical structure for indicating the validity of digital information or any document. A message is created by a known sender whose digital signature provides a recipient reason, such that the sender cannot reject having sent the message confirmation and that the message was not changed in transportation integrity. The Signature recognition and verification are a behavioral biometric. It can be operated in two various types: one is the Off-Line or Static Signature Verification Technique and another is the On-line or Dynamic Signature Verification Technique. In this paper, we are studying about Off-Line or Static Signature Verification Technique. In this method, users write their own signature on the blank paper and then digitize it with an optical scanner or a camera, and then the biometric system identifies the signature by analyzing its shape and this collection is also called as "off-line" Signature verification. Signature authentication can be divided into three main classes. These classes are based on how alike a forgery is in relation to signature and are identified as random, simple and skilled. In the random forgery the forger does not know about the signer's shape or signature name. In the simple forgery or unskillful forgery, the forger knows the name of the actual signer but don't know how his signature looks like. And in the skilled forgery, the forger knows both the information of the signer.

Keywords: *Digital signature, biometric techniques, offline signature, feature extraction, Applications*

1. Introduction

In our society, classical and conventional means for a human being to recognize and validate himself either to any other person or to a computer system is the based on any or more of these three common main beliefs:

- What the human being knows
- What person possesses or
- What person is?

The handwritten signature is observed as the means of recognizing the signer of the written data which is based on the embedded hypothesis that the person's common signature modifies little by little and it is harder to remove, modify or forge without discovery. The handwritten signature is the one of the means to approve transactions and validate the person's uniqueness matched with another electronic ID technique like fingerprints scanning, face recognition, and a retinal vascular design showing. It is simple for a person to migrate from using the common pen-and-paper signature to the one where the handwritten signature is then caught and confirmed electronically. The signature of the human being is one of the most important biometric element of the person and is then used for the purpose of the authorization. Several methods are probable for signature recognition with many possibilities of study. Here, we deal with the off-line signature recognition method. Signatures are self-possessed of a superior character and flourishes and, therefore, most of the time period they can

ISSN: 1738-9976 IJSIA

unreadable. Also, interpersonal differences and interpersonal changes create a need to examine them as complete images and not as a letter and words put together [1].Classical bank checks, bank credits, credit cards and several allowed data are the essential portion of the contemporary economy. They are the main channels by which persons and administrations transfer money and also pay bills. And even today all of these transactions, particularly monetary need our signatures to be authenticated. The unavoidable side-effect of the signatures is that they can be misused for the purpose of the feigning a data authenticity. Hence, the requirement for the examination in well-organized automatic resolutions for the signature recognition and confirmation has improved in later years for the purpose of avoiding the risk of fraud [2-5]. In signature confirmation, forged signatures can be cracked up into the three various classes. These classes are based on how alike a forgery is in relative to the unaffected signature and are well-known as skilled, random and simple. In the random forgery, the forger doesn't discern about the signer's name or the signature shape. In unskilled forgery or simple forgery, the forger knows the name of the actual signer but don't know how his signature appearances like. While in skilled forgery, a closed imitation of the unaffected signature is then created by the forger who has seen and have skillful writing of the unaffected signature. It is these skilled forgeries that this paper will attention on for the signature confirmation [6].

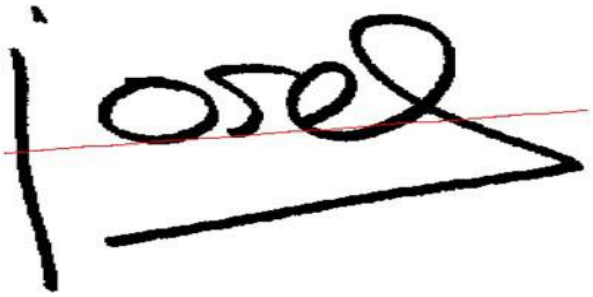

Figure 1. Example of Offline Signature

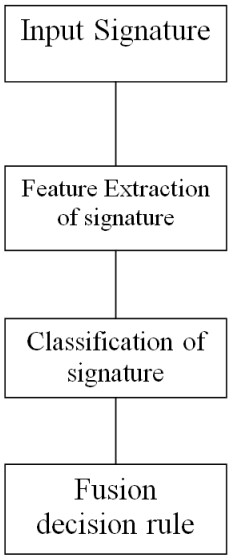

Figure 2. Block Diagram of Signature Verification System

2. Type of Signature Verification

Based on the definitions of the signature, it leads two methods of the signature verification.

2.1. Off-line or Static Signature Verification Method: This method is based on the static characteristic signature, which are invariant [1]. In this logic signature confirmation, becomes a classical configuration recognition mission knowing that differences in the signature pattern are unavoidable; the mission of signature verification can be lessened to sketching the threshold of the series of the unaffected difference. In the offline signature verification methods, images of the signatures written on the paper are achieved applying camera or a scanner.

2.2. On-line or Dynamic Signature Verification Method: This is another kind of signature verification method. This method is based on the dynamic characteristics of the procedure of signing. This confirmation uses signatures that are captured by heaviness subtle tablets that mine dynamic properties of a signature in addition to its shape. Dynamic features include the no. of order of the strokes, on the basis of the pen pressure and speed of signature at every point that create the signature much unique and more severe to forge. Application of particular areas of Accessible online Signature Verification contain safety of minor particular policies (e.g. PDA, laptop), permission of computer users for accessing sensitive data or programs and authentication of entities for access to η kind of forgeries. The central mission of some signature confirmation organizations is to notice whether the signature is unaffected or counterfeit. Forgery is a crime that the goals at devious person. Since real forgeries are challenging to find, the tool and the results of the verification depend on the kind of the forgery [9].

3. Feature Extraction

Feature mining, as the well-defined by the Devijver and Kittle [8] is "Mining the data from the raw document which is much more pertinent for organization phase. This document can be lessened within-class design difference and growths the inter-class differences." Therefore, attaining a great recognition act in a signature recognition system is extremely influenced by the selection of efficient feature mining techniques, taking into the consideration and the domain application and the kind of classifier used [9]. An efficient feature removal procedure should be required two selves: Invariance and the reconstruct-ability on the features [9] that are the invariant to the definite conversions on the signature which would be able to recognize many variations of these signatures. Such transformations include translation, scaling, rotation, stretching, skewing and mirroring. On the other hand, the ability to reconstruct the signature from their extracted features ensures that complete information about the signature shape is the existing in these features. In this feature mining step, the known feature collection in the define pattern gratitude is used. In one is depends on the invariant dominant minute planned by Hu's [10] which is used for the scale and conversion normalization and the another is the altered Zernike moment[11] which is used for rotation normalization.

3.1. Invariant Central Moment : The moments of the order (u + v) of an image collected of binary pixels, B(x, y) are proposed by [12], [13] as shown in the eq. (1).

$$m_{u,v} = \sum_x \sum_y x^u y^v B(x,y)$$
$$u, v = 0,1,2,3,4 \ldots\ldots\ldots\ldots \quad (1)$$

Body's area A and the image's center of mass $(\bar{x}, \bar{y})$ is found from eq. 6.

$$\bar{x}=\frac{m_{10}}{m_{00}},\ \bar{y}=\frac{m_{01}}{m_{00}} \quad (2)$$

The central moments, which are translation Invariant, are given by eq. 7.

$$\mu_{u,v}=\sum_{x}\sum_{y}\overline{x-(x)^{u}}\,\overline{y-(y)^{v}B(x,y)} \quad (3)$$

Finally, the normalized central moments, which are translation and scale invariant, are derived from the central moments as shown in eq. 8.

$$\eta_{u,v}=\frac{\mu_{u,v}}{(\mu_{u,v})^{k}} \quad (4)$$

Where

$$k=1+\frac{(u+v)}{2}\,for u+v\geq 2$$

3.2. Zernike Moments : Zernike polynomials are a set of complex polynomials which form a complete orthogonal set over the interior of the unit circle [14].The form of polynomial is shown by eq.

$$V_{nm}(p,\theta)=V_{nm}(p,\theta)=R_{nm}(p)exp(jm\theta) \quad (5)$$

Where $j=\sqrt{-1}$, n≥0,$n-|m|iseven|m|\leq n,p$ is the Length of the vector from the origin to the point (x,y),θ is the angle between this vector and the x axis in the Counterclockwise direction and the radial polynomial$R_{nm}(\rho)$is

$$R_{nm}(\rho)=\sum_{s=0}^{n-|m|/2}\frac{(-1)^{s}\rho^{n-2s}(n-s)!}{s!\left(\frac{n+|m|}{2}-s\right)!\left(\frac{n-|m|}{2}-s\right)!} \quad (6)$$

Zernike moments are the projections of the image function onto these orthogonal basis functions. The Zernike moment of order n with repetition m for a digital image is given by

$$A_{nm}=\frac{n+1}{\pi}\sum_{x}\sum_{y}B(x,y)[V_{nm}(\rho,\theta)] \quad (7)$$

Where, * is the complex conjugate operator and

$$x^{2}+y^{2}\leq 1$$

To calculate the Zernike moments for a given image, its pixels are mapped to the unit circle

$x^{2}+y^{2}\leq 1$This is done by taking the geometrical center of the image as the origin and then scaling its bounding rectangle into the unit circle, Due to the orthogonally of the Zernike basis, the part of the original image inside the unit circle can be approximated using its Zernike moments A_{nm}up to a given ordern_{max}using

$$\hat{B}(x,y)=\sum_{n=0}^{n_{max}}\sum_{m}A_{nm}V_{nm}\,(\rho,\theta) \quad (8)$$

Where$n-|m|isevenand|m|\leq n$

The orthogonality property of Zernike moments, as expressed in the eq.8, allows easy image reconstruction from its Zernike moments by simply adding the information content of each individual order moment. Moreover, Zernike moments have simple rotational transformation properties interestingly enough the Zernike moments of a rotated image, have identical magnitudes to those of the original one, where they merely acquire a phase shift upon rotation.

4. Literature View

Pradeep Kumar (2013) *et al.* Present that the off-line signature recognition and confirmation using neural network is the proposed, where the signature is captured and

obtainable to the user in an image design. Signatures are confirmed based on the parameters mined from the signature using numerous image processing methods. The Off-line Signature Recognition and Confirmation are affected using MATLAB. This work has been verified and found suitable for its purpose. This paper presents a method of handwritten signature verification using a neural network approach. The method uses features extracted from preprocessed signature images. The extracted features are used to train a neural network using error back-propagation training algorithm [15]. Nilesh Y. Choudhary (2013) et al. Present that the off-line signature recognition, confirmation using back propagation neural network is the projected, in where a signature is taken and obtainable to the user in an image organization. Signatures are confirmed based on the features mined from the signature using Invariant Central Instant and Altered Zernike instant for its invariant feature mining because the signatures are Hampered by the treat quantity of difference in the size, conversion and the rotation and also shearing parameter. In this study, obtainable Off-Line Signature Recognition and Confirmation System using the back propagation neural network which is based on the steps of image processing, invariant central moment invariants, Zernike moment & some global properties and back propagation neural networks[16].

Ali Karouni (2011) *et al*. Presents that the technique for Off-line Verification of signatures using a collection of simple shape based on the geometric features. The geometric features that are used are a Centre of gravity, Area, Eccentricity, Kurtosis, and Skewness. Earlier mining features, preprocessing of the scanned image is needed to separate the signature portion and to eliminate any fake sound attained where the system is originally educated applying the database of the signatures found from those entities whose signatures have to be authenticated by the system. The information of preprocessing as well as the features depicted above is designated throughout the conversation. Then ANN (artificial neural network) was used to confirm and classify the signatures: mine or forged, and an organization ratio of about the 93% was found under the threshold of 90% [17].

George S. Eskander (2014) *et al.* presents that the FV system based on offline signature images is planned. A two-step BFS(boosting feature selection) method is proposed for the choosing a compact and discriminate user-specific feature representation from a great no. of feature removals. The first step pursues dimensionality discount through learning a population- based representation, which discriminates between various users in the population [18].

Indrajit Bhattacharya (2013) -It presents that Offline Signature verification is an authentication method that uses the dynamics of a person's handwritten signature measure and analyzes the physical act of signing. The core of a signature biometric system is behavioral, and in this paper, we have proposed an off-line signature verification and recognition system using pixel matching techniques. PMT (Pixel Matching Technique) is used to verify the signature of the user with the sample signature which is stored in the database. The performance of the proposed method has been compared with the existing ANN (Artificial Neural Network's) back-propagation method and SVM (Support Vector Machine) technique. The signature authentication machine is implemented to provide a simple, safe, fast biometric behavioral security system. By using some equations from coordinate geometry, makes this method faster than other methods. The color matching technique makes it more secure. The Interface of this application is very simple which makes it user-friendly and easy.

The implemented system has the following limitations:

• Our system only able to identify the static changes in a signature, it cannot identify any dynamic changes in a signature.

• This signature authentication system works off-line. No on-line device is connected

with thissystem. And The methods of signature authentication tested only off-line [19]. Sabri A. Mahmoud (2014) et al present that an official confirmation method is implemented to Align the handwritten text with the ground truth at form, section, and line levels. The verified ground truth the database holding meta-data describing the written text the page, section, and line levels in text and XML organizations. Tools to remove paragraphs from pages and subdivision paragraphs into lines are developed. In addition, they are representing experimental results on the database using two classifiers, viz. Hidden Markov Models (HMM)and our novel syntactic classifier [20]. Yaregal Assabie (2011) et al presents those two methods for Amharic word recognition in unrestricted handwritten text using HMMs. The top method builds word prototypes from concatenated features of principal appeals and in another technique HMMs of constituent characters are concatenated to form word model. In these two cases, the features used for training and recognition are a collection of primitive strokes and their spatial relationships. The recognition system does not need division of characters, but needs text line finding and mining of structural features, which is done by making use of direction field tensors [21].

5. Methodology

5.1 Hidden Markov Models Approach

Hidden Markov Model (HMM) is one of the most widely used models for sequence analysis in signature verification. Handwritten signature is a sequence of vectors of values related to each point of signature in its trajectory. Therefore, a well-chosen set of feature vectors for HMM could lead to the design of an efficient signature verification system. These Models are stochastic models which have the capacity to absorb the variability between patterns and their similarities. In HMM stochastic matching (model and the signature) is involved. This matching is done by steps of the probability distribution of features involved in the signatures or the probability of how the original signature is calculated. If the results show a higher probability than the test signatures probability, then the signatures is by the original person, otherwise the signatures are rejected. In a paper [6], a system is introduced that uses only global features. A discrete random transform which is a sinograph is calculated for each binary signature image at a range of $0 - 360$, which is a function of total pixel in the image and the intensity per given pixel calculated using non-overlapping beams per angle for X number of angles. Due to this periodicity, it is shift, rotation and scale invariant. An HMM is used to model each writer's signature. The method achieves an AER of 18.4% for a set of 440 genuine signatures from 32 writers with 132 skilled forgeries.

5.2 Neural Networks Approach

The main reasons for the widespread usage of neural networks (NNs) in pattern recognition are their power and ease of use. A simple approach is to firstly extract a feature set representing the signature (details like length, height, duration, etc.), with several samples from different signers. The second step is for the NN to learn the relationship between a signature and its class (either “genuine” or “forgery”). Once this relationship has been learned, the network can be presented with test signatures that can be classified as belonging to a particular signer. NNs, therefore, are highly suited to modeling global aspects of handwritten signatures. The proposed system in [7] uses structure features from the signature contour, modified direction feature and additional features like surface area, length skew and a centroid feature in which a signature is divided into two halves and for each half a position of the center of gravity is calculated in reference to the horizontal axis. For classification and verification, two approaches are compared the Resilient Back propagation (RBP) neural network and Radial Basic

Function(RBF) using a database of 2106 signatures containing 936 genuine and 1170 forgeries. These two classifiers register 91.21% and 88 % true verification respectively.

5.3 Template Matching Approach

Fang *et al.* [8] Proposed two methods for the detection of skilled forgeries using template matching. One method is based on the optimal matching of the one-dimensional projection profiles of the signature patterns and the other is based on the elastic matching of the strokes in the two-dimensional signature patterns. Given a test signature to be verified, the positional variations are compared with the statistics of the training set and a decision based on a distance measure is made. Both binary and gray-level signature images are tested. The average verification error rate of 18.1% was achieved when the local peaks of the vertical projection profiles of gray-level signature images were used for matching and with the full estimated covariance matrix incorporated.

5.4 Statistical Approaches

Using statistical knowledge, the relation, deviation, etc between two or more data items can easily be found out. To find out the relation between some set of data items we generally follow the concept of Correlation Coefficients. In general statistical usage refers to the departure of two variables from independence. To verify an entered signature with the help of an average signature, which is obtained from the set of, previously collected signatures, this approach follows the concept of correlation to find out the amount of divergence in between them. A unique method is introduced in [9]. In this approach, various features are extracted which include global features like image gradient, statistical features derived from the distribution of pixels of a signature and geometric and topographical descriptors like local correspondence to trace of the signature. The classification involves variations between the signatures of the same writer and obtaining a distribution in distance space. For any questioned signature, the method obtains a distribution which is compared with the available known and a probability of similarity is obtained using a statistical Kolmorogorv-Smirnov test. Using only 4 genuine samples for learning, the method achieved 84% accuracy which can be improved to 89% when the genuine signature sample size is increased. This method does not use the set of forgery signatures in the training/learning.

5.5 Support Vector Machine

Support Vector Machines (SVMs) are machine learning algorithms that use a high dimensional feature space and estimate differences between classes of given data to generalize unseen data. The system in [10] uses globally, directional and grid features of the signature and SVM for classification and verification. The database of 1320 signatures is used by 70 writers. 40 writers are used for training with each signing 8 signatures thus a total of 320 signatures for training. For initial testing, the approach uses 8 original signatures and 8 forgeries and achieves FRR 2% and FAR 11%.

Table 1. Comparison of Various Techniques

Approach	FAR(%)	Accuracy
Back-Propagation Neural Network Prototype	10.00%	
Generic Algorithm	01.80%	86.00%

Virtual Support Vector Machine	13.00%	
Wavelet Based Verification	10.98%	
Signature Recognition using Clustering Technique	2.5%	95.08%

Table 2. Application of Biometric System

Fingerprint	Finger lines ,pore structure
Signature	Various features based on writing of a person
Facial geometry	Distance of specific facial features (eyes, nose, mouth)
Iris	Iris pattern
Retina	Eye background (pattern of the vein structure)
Hand geometry	Measurement of fingers and palm
Finger geometry	Finger measurement
Vein structure of back of hand	Vein structure of the back of the Hand
Ear farm	Dimensions of the visible ear
Odor	Chemical composition of the one's odor
DNA	DNA code as the carrier of human hereditary

6. Conclusion

In this paper, we are studying about digital signature, which is a mathematical structure for the purpose of authentication of the user for their validity, purpose and also studying about Off-Line or Static Signature Verification Technique. In this method, users write their own signature on the blank paper and then digitize it by an optical scanner or a camera, and then the biometric system identifies the signature analyzing by its shape and this collection is also called as "off-line" Signature verification. In the future work, we will try to classify offline signature with different types of signature and apply attacks such as cropping, noise, etc. And verify the image quality of the signature after applying attacks.

References

[1] S. Srihari. K. M. Kalera and A. XU, "Offline Signature Verification and Identification Using Distance Statistics", International Journal of Pattern Recognition And Artificial Intelligence, vol. 18, no. 7, (**2004**), pp. 1339–1360.

[2] K. R. Radhika, M. K. Venkatesha and G. N. Sekhar, "Off-Line Signature Authentication Based on Moment Invariants Using Support Vector Machine", Journal of Computer Science, vol. 6, no. 3, (**2010**), pp. 305-311.
[3] R. Ebrahimpour, A. Amiri, M. Nazari and A. Hajiany, "Robust Model for Signature Recognition Based on Biological Inspired Features", International Journal of Computer and Electrical Engineering, vol. 2, no. 4, (**2010**), August.
[4] A. PiyushShanker and A. N. Rajagopalan, "Off-line signature verification using DTW", Pattern Recognition Letters.
[5] A. Zimmer and L. L. Ling, "Offline Signature Verification SystemBased on the Online Data", EURASIP Journal on Advances in Signal Processing, vol. (**2008**), Article ID 492910, 16 pages.
[6] L. Basavaraj and R. D S. Samuel, "Offline-line Signature Verification and Recognition: An Approach Based on Four Speed Stroke Angle", International Journal of Recent Trends in Engineering, vol 2, no. 3, (**2009**) November.
[7] B. Herbst. J. Coetzer and J. Preez, "Online Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model", EURASIP.Journal on Applied Signal Processing, vol. 4, (**2004**), pp. 559–571.
[8] P. A. Devijver and J. Kittler, "Pattern Recognition: A Statistical Approach", PrenticeHall, London, ISBN: 10: 0136542360, (**1982**).
[9] O. D. Trier, A. K. Jain and T. Taxt, "Feature extraction methods for character recognition-a survey", Patt. Recog., vol. 29, pp. 641-662.
[10] M. Hu, "Visual pattern recognition by moment invariants", IRE Trans. Inf. Theory, IT-8, pp. 179–187.
[11] A. Khotanzad and Y. H. Hong, "Invariant image recognition by Zernike moments", IEEE Trans. Patt.Anal. Mach. Intell., 12: pp. 489- 497, DOI: 10.1109/34.55109.
[12] S. Theodoridis and K. Koutroumbas, "Pattern Recognition", 3rd Edn., Academic Press, ISBN: 10: 0123695317, (**2006**), pp. 856.
[13] T. H. Reiss, "The revised fundamental theorem of moment invariants", IEEE Trans. Patt.Anal. Mach. Intell., 13: 830-834. DOI: 10.1109/34.85675, (**1991**).
[14] A. Khotanzad and Y. H. Hong, "Invariant image recognition by Zernike moments", IEEE Trans. Patt.Anal.Intell, (**1990**) March, pp. 489-497.
[15] P. Kumar, "Hand Written Signature Recognition & Verification using Neural Network", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 3, (**2013**) March.
[16] N. Y. Choudhary," Signature Recognition & Verification System Using Back Propagation Neural Network", International Journal of IT, Engineering and Applied Sciences Research, vol. 2, no. 1, (**2013)** January**.**
[17] A. Karouni, "Offline signature recognition using neural networks approach", Procedia Computer Science, vol. 3, (**2011**), pp. 155–161.
[18] G. S. Eskander, "A bio-cryptographic system based on offline signature images", Information Sciences, vol. 259, (**2014**), pp. 170–191.
[19] I. Bhattacharya, "Offline Signature Verification Using Pixel Matching Technique", International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) (**2013).**
[20] S. A. Mahmoud, "KHATT: An open Arabic offline handwritten text database", Pattern Recognition, vol. 47, (**2014**) pp. 1096–1112
[21] Y. Assabie, "Offline handwritten Amharic word recognition", Pattern Recognition Letter, vol. 32, (**2011**), pp. 1089–1099.

Authors

Deepti Yadav, she was born in India on May 31,1989. She received her B.E degree in Electronics and Communication from Government Engineering college ,Rajkot ,Saurashtra University, Gujarat,India in year 2010 and currently is a M.Tech student in Maharana Pratap College of Technology, Gwalior, Madhya Pradesh, India. **Mailid – deepti02yadav@gmail.com**

Ranbeer Tyagi, he obtained Master of Engineering degree from SGSITS Indore, Madhya Pradesh, India in year 2010, and B.E. in Electronics and Communication Engineering from RGPV University, Bhopal, Madhya Pradesh, India in year 2008. He is currently working as an Assistant Professor in Electronics and Communication Department at Maharana Pratap College of Technology, Gwalior, Madhya Pradesh, India. His areas of interest are Image Processing, Speech Processing, Communication, Acoustic Echo Cancellation, and Signal Processing. He has more than 5 years experience in teaching and research. He is Reviewer of International Journal of Advanced Technology & Engineering Research (IJATER).