International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 2 Issue 4, April 2015

ISSN: 2394-4404

Comparative Study Of Signature Verification

Anuja Kore

Swati Kadam

Aishwarya Jagtap

Pritam Kulthe

Vpcoe, Baramati, Pune University, India

***Abstract:** Today in the world of profit aiming mind, fake signatures are used, therefore trust of people is at high risk. The fraudulent signature thus needs to be verified using verification techniques. The signature forgery can be restricted by either online signature verification or offline signature verification techniques. Online signature on one hand verifies the signature by performing a match with the pre-processed signature dynamically by detecting the motion of stylus during signature while on other hand, offline verifies by performing a match using the two dimensional scanned image of the signature. This paper studies about the various techniques available in offline signature verification along with their shadows.*

***Keywords:** Signature, Verification, Forgeries.*

I. INTRODUCTION

In real time instances, authentication of the person was needed for person identification. This type of authentication is generally occurs by signature from past incidents. But still nowadays, especially in financial institutions, there is compulsion of signature authentication. So that, with this increasing number of transactions, desire of automatic signature verification will take place for authenticating the individual persons which was signed. Signature verification is not only used to identity two individual accurately but also their strongly related tasks. On one side, the first task is to identify the signature owner; on the other side, the second task is to take the decision, whether the signature is genuine or forged. Signature verification is divided into two categories: One is online signature verification and other is offline signature verification. Where online signature verification scans the user signature by tracing the different motion on the stroke of the signature and identifies it against pre-processed signature information.

On other hand, Offline signature verification gives static signature verification information, in which signature is scanned from document and it is verified against 2D scanned image of the signature. In this paper, the variations offered in offline signature verification methods are discussed. The methods vary from Support vector machines (SVM), Dynamic time warping (DTW), Neural network (NN), Multi-set features (MSF), Associative Memory Net (AMN), Robust hybrid method, Automatic signature verification (ASV).

A. SUPPORT VECTOR MACHINE

SVM is a new learning method introduced by V. Vapnik et al. With a set of examples from two classes, a SVM finds the hyper plane, which maximizes the distance from either class to the hyper plane and separates the largest possible number of points belonging to the same class on the same side [1]. SVM is based on the structural risk minimization principle (SRM). SVM becomes very popular because of its success in hand written digit recognition. SRM consists of two main principles: The first principal is to control the risk on the training set and the second principle is to control the capacity of decision function used to obtain this risk value. SVM consist of two classes: Linear separable and Classification problem. Linear separable find the hyper plane with maximum Euclidean distance from the training set. There will be just one optimal hyper plane with the maximal margin d, defined as the sum of distances from the hyper plane to the closest points of the classes. This linear classifier threshold is the optimal separating hyper plane [2]. SVM is to solve the optimization problem, where the original input space is mapped into a higher dimensional feature space by the function ϕ[2]. Then SVM can find an optimal linear separating hyper plane with the maximal margin in this higher dimensional feature space. C is the penalty parameter of the error term. For a two-class problem, the nonlinear decision function derived from the SVM classifier can be formulated as the kernel function. The kernel is not positive definite but offer some theoretical and empirical explanations.

B. DYNAMIC TIME WARPING

DTW is an algorithm which is related to measurement of time and speed of two sequences. DTW is applicable to video, audio, and graphics, and many more application such as automatic speech recognition. DTW algorithm is used to establish linear and non-linear dimensions of the sequences. The basic principle of this method is permitting a range of 'steps' in the space of (time frames in sample as well as in template) and to find the maximum length path between the aligned time frames, subject to the constraints implicit in the allowable steps. The total similarity cost found is used to determine the best matching template and sample. Consider two signatures aligned between L and L' ,known as warping path, denoted as T, and two warping function: mean that the point in L corresponds to the element in L'. The matching cost between L and L' is calculated by using online context. The optional warping path is the one which minimize the above cost function. The optimization problem of DTW can be solved efficiently using dynamic programming.

C. NEURAL NETWORK

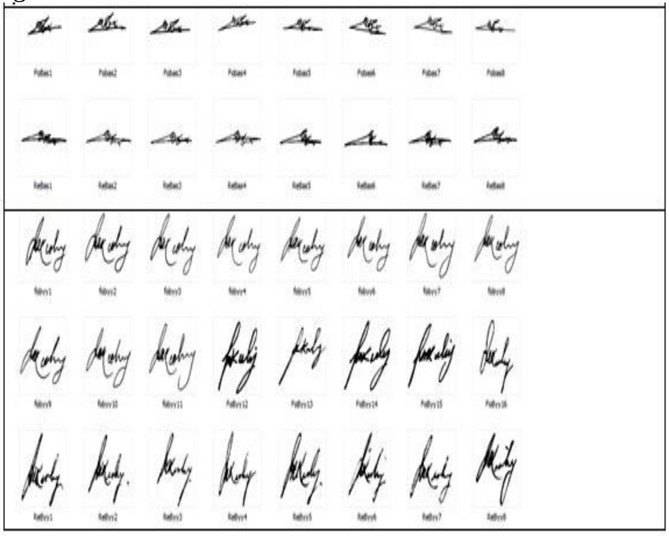
NN is used in signature verification for the purpose of hand written signature and verify its authenticity. But neural network is mainly used in pattern recognition. The signature verification process parallels this learning mechanism. Neural network based on two processes: training and learning [3]. The first step is training with the help of extraction method a feature set representing the signature with several samples from different signers. The second step is learning the relationship between a signature and its class. Once this process is done then the network can be classified to a particular signer. NNs therefore are highly suited to modelling global aspects of handwritten signatures. Alan McCabe et al. proposed a method for verifying handwritten signatures by using NN architecture. Various static (e.g., height, slant, etc.) and dynamic (e.g., velocity, pen tip pressure, etc.) signature features are extracted and used to train the NN. Several Network topologies are tested and their accuracy is compared. The resulting system performs well with an overall error rate of 3.3% being reported for the best case. Rasha Abbas in his earlier research investigated the suitability of using back propagation neural networks for the purpose of offline signature verification however later on multi-layered feed forward neural network was investigated.

D. MULTI-SET FEATURE

Off-line signatures are signatures which usually use in paper works like letters, contracts, and bank checks. This method is related to offline signatures specially. According to Edson J. R. Justino and F. Bortolozzi[4,5], ASV is processed with the one feature set but to increase the usability of designed ASV in the sense of increasing security best feature set of signatures is used in this technical method. This method is popularly known as new novel MSF based ASV technique. At first, features are examined in two ways these are shape features like handwriting slants and pseudo dynamic features. Distance measure and verification threshold are also calculated. By taking these values for comparison, at the second stage, probability of forgery is decided if DM<VTH. In this condition, signature is processed with the n X n matrix. By fitted signature in the matrices are n X n matrix, three resulted matrices are calculated which are backbone of MSF technique, SR (System Reliability), PCR (Per cent Correct Rejection), PCA (Per cent Correct Acceptance). As the system reliability PCR, PCA has high values, and then signature ids totally matched to best features set that particular sign. There are mainly two steps in MSF technique:

a. DATA SIGNATURE

560 genuine signatures are used in MSF technique and forgery signatures are obtained from different 26 writers. The number of genuine signatures and forgeries differ from one person to another. Signatures were extracted from various documents like business documents, bank checks so that the signature data is naturally written under widely different conditions. Reason behind such an extraction of signatures is that forgeries were created with a good attention in order to have convincing forgeries, and some forgeries are real ones obtained from actual caseworks. The complete set of genuine and forgery samples of person as an example is as shown in figure below



b. SIGNATURE VERIFICATION AND FEATURE SELECTION

2.1. Feature extraction: This stage of the signature verification and feature selection includes pre-processing. Features in off-line systems have two types mainly. These are

- ✓ Shape features like handwriting slants which can be positive, vertical, negative, and horizontal etc. and relative measures of signature height and width, middle zone width and signature width
- ✓ Pseudo dynamic feature is nothing but High Pressure Factor. These both type of features are extracted in two ways such as globally on the signature as a whole and locally on the signature divided into specific parts.

2.2. Distance measure: Distance Measure (DM) is used to calculate similarity between input signature and reference by using the Euclidean distance. Distance Measure (DM) is calculated by using the formula

DM = $(1/n\sum_{i=1}^{n}(fi-\mu i/\sigma i)^{2})^{1/2}$

Where:

fi: the i feature of test signature

n: number of used features.

μi: the mean the ith feature computed on the set of genuine samples of the specific user.

σi: the standard deviation of the ith computed feature.

2.3. Threshold value: The value of the threshold VTH is calculated by feature selection technique that selects the best feature set which minimizes the error rate as well as maximizes the correct decisions.

2.4. Verification decision: The verification decision to determine whether signature is reliable is proceed with the help of calculated distance measure and threshold value. There are two cases for determination of genuine signature.

- ✓ DM > VTH, the input signature is genuine.
- ✓ DM < VTH, it is judged to be an attempted forgery.

CMBFST is a very fast one and gives a clear idea of the effectiveness of the individual features, and their contribution to the effectiveness of the different feature sets, if augmented by, to form a new one. Since this CMBFST is used to develop the MSF technique for ASV in current method. By using CMBFST n x n feature sets are generated but mainly the same, n x n (n-1) different feature sets are to be generated. For this purpose first the best feature set is to be decide among the n x n (n-1) sets and the signature data is judged using generated feature sets which forms result matrices termed as,

SR (System Reliability = (PCA+PCR)/2).

PCA (Percentage of Correct Acceptance that is percentage of genuine signatures accepted as genuine) and PCR (Percentage of Correct Rejection that is percentage of forgeries rejected and classified as attempted forgeries).

MSF helps to improve the forgery detection, where all the terms below are used

CVFI: correctly verified forgery samples by using the feature set number i.

C VFBFS: correctly verified forgery samples by using the best feature set.

CVFMFS: correctly verified forgery samples by using

MSF = $\bigcup_{i=1}^{n} cvf$

Where,

n: number of feature sets.

CVFMFS > CVFBFS

In other words, the MSF technique is a process of collecting the sparse effectiveness that can be provided by the EFS but cannot be captured by the best feature set.

E. ASSOCIATIVE MEMORY NET

The Associative Memory Net (AMN) is used to detect the forged signature quickly. To handle the cost function detail parametric studies and parallel processing using OpenMP [7] is must. These algorithms are used to verify actual signature and tested with a reference of 10 nearly similar signatures. The AMN technique finds forgery with accuracy 94.3%, which can be compare with other methods.

A step-wise method has been followed in this work.

STEP 1: Collecting the reference and extracted signature.

STEP 2: Signatures should be in pixel format.

STEP 3: Implementation of AMN in ‘C’ language.

STEP 4: Signature should be genuine for training of the networks.

STEP 5: The target is the genuine signature.

STEP 6: If the targeted output is equal to the obtained output

6.1. The signature is matching completely

Else the targeted output is not equal to obtain output then

6.2. The signature is not matching completely.

STEP-7: Testing of the developed AMN.

The developed and trained AMN network was then trained with 12 references of Forged signatures.

7.1. Calculation of mismatch: The numbers of YJ which are -1 are counted (count). The percentage of mismatch can be calculated using the following:

Mismatch = [count/Total Number of Pixels] × 100 (1)

7.2. Set the threshold of mismatch Threshold is the minimum mismatch percentage after which the extracted signature could be termed as illegal. This is for to increase stricter security and safety applications, set the threshold as less as 25% to avoid skilled forgery. Note that, such less threshold setting must be situation specific.

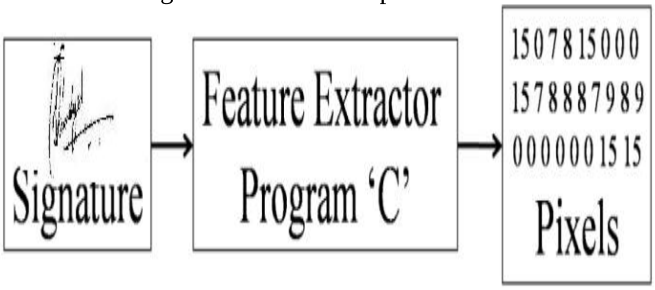


Figure 1

a. SERIAL IMPLEMENTATION OF THE NETWORK

It will be wise to mention that training of the AMN had been done with the genuine sample only.

- ✓ Initialize weight= 0
- ✓ Give input as the original signature to AMN.
- ✓ Apply the LFT (Linear Transfer Function) to give final output.

  In LTF the input =output (for original signature)
- ✓ For (i=1; i<n; i++)

```
    Do
     For (j=1; j< n; j++)
```

```
        Do
         The weight is calculated as
    Wij (new) = Wij (old) + INPUT i×  TARGET j
       End //loop j ends here
     End//loop I ends here
✓   For (i=1; i<n; i++)
        Do
         For (j=1; j< n; j++)
          Do
             5.1 The net input to each output node is calculated as,
    $Yin_j = \sum_{i=1}^{n} x_i W_{ij}$
             5.2 If (Yin j > 0)
    Yj is +1;
               Else
    Yj is -1;
          End //loop j ends here
        End//loop i ends here.
✓   If (the TS = FS)
    Then the signature is completely matched.
    Else
    The signature not matched.
```

b. *PARALLEL IMPLEMENTATION OF THE NETWORKS*

Using OpenMp (www.openmp.org) here we can develop a parallel version of all the above algorithms using. By doing this, three main factors can be achieve system efficiency.

- ✓ Reduction in computation time,
- ✓ Utilization of all the processor of the system
- ✓ Inherent parallelism property of NN could be used.

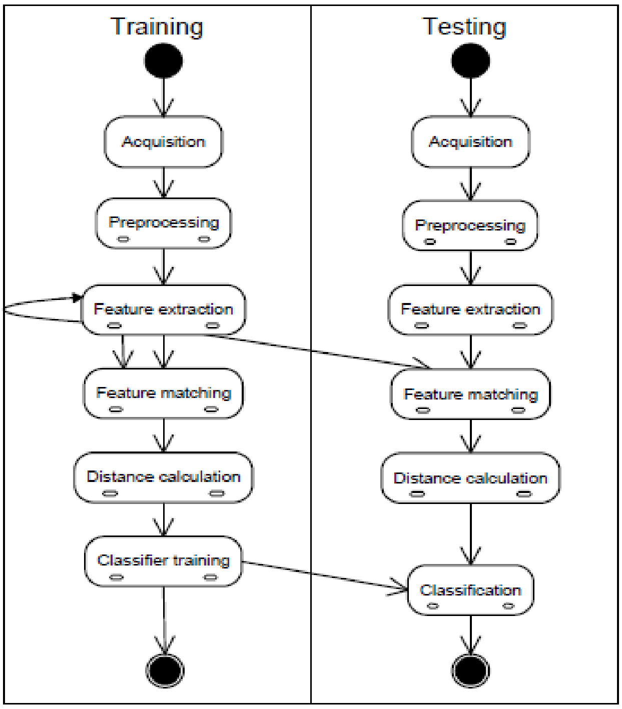


Figure 2: Generalized view of an offline signature verification system

F. ROBUST HYBRID TECHNIQUE

Robert Sabourin, in this method, various phases are present. Some of them are carried out offline while some of them are Online. There are three phase architecture which is proposed for the verification of signature. As in first phase of signature processing , three features of signature are examined which are total signing time, the consistency between questions signature and extracted signature from database and binary pattern of the pen movement. This phase is mandatory. In linear predictive coding method, pattern recognition of signature is done by using the committee of five neural networks, which checks speed profile of questionable signatures. This is the second phase which is online[6]. In this phase of architecture, recognition part comes which is harder than the verification. If recognition can be done then there is no need of third phase. If recognition in third phase gets fails, then third phase is carried out which is offline process. In Offline process, verification of questionable signatures is done by comparing with database stored all signatures one by one which is time consuming. This system has some drawbacks that the two phases are online and one is offline due to that no consistency in process. But our proposed system is throughout online in each phase.

G. REAL-TIME FEATURE BASED AUTOMATIC SIGNATURE VERIFICATION

There are various methods for ASV implementation but there is only one or two signature references used by considering memory storage as well as current image based verification speed. There will be 20 signature references. Each reference signatures is converted to a small number of pre-computed features resulting in verification speeds in excess of 60 verifications per second. These features of specific signer signature are stored in the database. There are features like edge distribution, pixel distribution, slant, pixel density, aspect ratio of signature are stored in dataset. Even if fraudster stole this featured information then also he cannot predict the how is the signature actually. So, important data is being safe and loss can be avoided.

The proposed system matches tested signature with reference signature. Test signature features are considered as x and n is reference signature feature stored in database, where n<=20. System first extract features of the tested signature and that features match with the extracted features of reference signatures. Various extracted features are used for calculating matching function. Algorithms like four-dimensional chain code, normalization are used for computing features of signature. As per the value of matching function, signature is real or fake is decided by system.

A step-wise method has been followed in this work.

STEP 1: Take signature as input from document which has to be verified.

STEP 2: All the pre-computed features of reference is stored in database.

STEP 3: Extract the features of current input signature like Pixel Distribution, Chain Code, Pixel Density or Aspect ratio by processing it through various stages.

STEP 4: For pixel distribution, normalise the signature into values 1-1000 to calculate cost and set signature into box size of 75X300 accurately.

STEP 5: Calculate chain code for fitted signature in size of box by using two terms weighted distance and Euclidian distance.

STEP 6: Apply the Gaussian Filter Formula on the previous resulted image in step 5.

STEP 7: Calculate pixel density cost and Aspect Ratio cost for signature has to be verified by using reference.

STEP 8: Calculate Average Match Function for number of references by using formula (as above formula).

STEP 9: If value is 0 then signature is fake and if 100 then its accurate matched.

STEP 10: By normalising Match function by using formulae of average and standard deviation, it becomes a Match Function.

STEP 11: If value of Match Function is in between 0 to 1 then signature is totally matched. This is not necessary all time.

II. CONCLUSION

We have studied various methods of Signature Verification on the basis of various factors related to it like, no. of references, security, memory management, accuracy which plays important role in verification of signature.

REFERENCES

[1] E.Ozgunduz, T.Senturk and M.E Karsligil, "Off-Line Signature Verification and Recognition by Support Vector Machine", *Proceedings of Europian Signal Processing, 2005.*

[2] M.S Arya and V. S Inamdar, "A Preliminary Study on Various Off-line Hand Written Signature Verification Approaches", *Proceeding of International Journal of Computer Applications, vol. 1, no.9, 2010.*

[3] S.A. Daram T. S. Ibiyemi ola, "Offline Signature Recognition using Hidden Markov Model", *Proceeding of International Journal of Computer Applications, vol. 10, no.2, 2010.*

[4] K. Huang and Y. Hong, Off-line signature verification based on geometric feature extraction and neural network classification, Patten Recognition, *Vol. 30, No. 1, pp. 9-17, 1997.*

[5] C. Sansone and M. Vento, Signature verification: increasing performance by a multi-stage system, Pattern Analysis and Applications, *Vol. 3, pp. 169-181, 2000.*

[6] F. Leclerc and R. Plamondon, Automatic Signature Verification: The state of the art, *International Journal of pattern recognition and artificial intelligence*, vol,8, no.3, pp.643-660.

[7] Anu Rathi, Amrita Ticku, Niti Gupta, Accuracy enhancement in offline signature verification with the use of associative memory, *IJCSNS International Journal of computer science and network security*, vol14, no.3,March 2014.

[8] E.J.R.Justino, F.Bortolozzi, R. Sabourin, "Off-line signature verification using HMM for random, simple and skilled forgeries" *Proceedings of Sixth International Conference on Document Analysis and Recognition, pp.1031–1034, 2000.*

[9] Dr. Maan Ammar, "Using Multi-Sets of Features to improve the Performance of Automatic Signature Verification Systems", *Damascus University Journal Vol.(26) – No.(2) 2010.*

[10] Ashraf A. Zaher And Abdulnasser Abu-Rezq, "A Robust Hybrid Method For Signature Verification Using Intelligent Encoding Of Spatiotemporal Data", *International Journal of Innovative Computing, Information and Control Volume 7, Number 4, April 2011.*

[11] Suhail Odeh And Manal Khalil, "Apply Multi-Layer Perceptron Neural network for Offline Signature Verification and Recognition", *IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 2, November 2011.*

[12] B.Majhi, Y.S Reddy, D.P Babu, "Novel Features for Offline Signature Verification", Proceeding of International Journal of Computers, Communications & Control, vol. I, no. 1, pp.1724, 2006.

[13] A.P.Shanker,A.N.Rajagopalan, "Offline signature verification using DTW", Proceeding of Pattern Recognition Letters,vol. 28,pp. 14071414, 2007

[14] J.W.Hong and H.Q.Hua, "Signature Verification Using Wavelet Transform and Support Vector Machine", ProCeeding of Advances in Intelligent Computing, vol. 3644, pp. 671678, 2005.

[15] M.S Arya and V. S Inamdar "A Preliminary Study on Various Off line Hand Written Signature Verification Approaches", Proceeding of International Journal of Computer Applications, vol. 1, no.9, 2010.