Digital Verification with Advance Techniques

Supriya Singh
EXTC Department
SLRTCE, Mira Road, India
supriyasingh0889@gmail.com

Prof. Manjiri Gogate
Assistant Professor
EXTC Department
SLRTCE, Mira Road, India
manjiri_3980@rediffmail.com

Prof. Sheetal Jagdale
Assistant Professor
EXTC Department
SLRTCE, Mira Road, India
sheetal.jagdale2@gmail.com

***Abstract*—**Authentication of persons has been supported as paramount object in society. Signature verification is mostly used for individual verification. But, it has an ultimate problem of getting destitute for forgery as a consequence an automatic signature recognition and verification system is required. Verification can be accomplished either Online or Offline based application. Offline systems work on the scanned image of a signature. Online systems consider dynamic information like pressure, speed etc. of a signature at the time when the signature is made. The current verification schemes could overlook the signature eventually though it may be genuine. Though diverse techniques are accessible for verification of cheques earlier Clearing, there are possibilities of necessary errors. In this paper we represent an offline signature verification technique using different features. Support Vector Machine (SVM) is used as to verify the signature using features like Local Binary Pattern (LBP) and Local direction Pattern (LDP) and also a verification algorithm is based on Static feature of signature such as Texture & Topological feature using Hamming distance. 1D-log Gabor wavelet and Euler number are used to analyze the textural and topological features of the signature respectively.

Keywords *– online signature; LDP; LBP; Hamming distance; SVM;*

*****

I. INTRODUCTION

Handwritten signature is generally used for the identification of the particular person. Signature of an individual is recognized as the primary mechanism for both authentication and authorization in legal transactions and help in personal identification. It provides authentication and security to various assets of the signer[1] . In the era of advanced technology security is the notable issue to avoid fakes and forgeries. Automatic recognition of signature, fingerprint, voice and face image is considered as a branch of pattern recognition and biometrics. It aims to recognize people from their biometric characteristics [8]. Recognition systems based on biometric data are categorized into physiological (fingerprint, retina etc) and behavioral (handwritten signature, voice etc) biometrics. Identification and verification are two different tasks in recognition. Identification determines which user presents a given parameter among a set of known users.

However, of a person as a form of behavioral biometrics. The problem of handwriting recognition still remains a challenge for the scientific community [2]. The verification of signature is classified into two categories: On-line signature verification and Off-line signature verification.

In Online verification, a signer signs on electronic devices such as Tablet PC, touch screen with an electronic pen, and characteristics like pressure exerted, stroke length, writing speed are used for the verification in online signature verification.
In offline signature verification, the signature is done on the paper and is scanned to convert it into digital form. Since the data is in the form of 2-D image, the extraction of dynamic data is a challenging issue where signature verification is done by comparing the signed signature with the template signature already stored in the database at the time of training data[2].
Example of training set of signature is as shown in Fig. 1

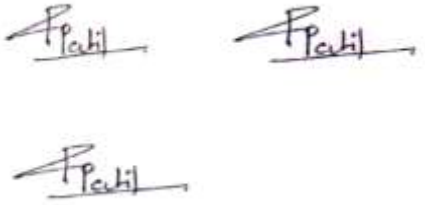


Fig. 1 Test signature

There are two types of variation in the signature, intra variation and inter variation [7]. In intra variation a signature of the same person varies due to abnormal conditions whereas the variation in the original and forged signature is termed as inter variation. In case of forgery, a person try to copy the signature of another person. The forgery signature can be classified into three following way:

- *Random forgery*: In Random forgery the signer knows only the name of the person whose signature is to be signed and uses his own style to sign the document and can be detected by naked eye.
- *Simple forgery*: In this case the signer has seen the signature pattern but does not have any prior experience of signing the signature of the victim.
- *Skilled forgery*: Here the signer knows the signature as well as the pattern very well and has experience in forgery. The signer signs exactly the same as the victim and it is very difficult to distinguish between original and forged signature [1].

Fig. 2 Example of a) Skilled forgery (b) Random forgery
(c) Causal forgery

In this paper an off-line signature verification system using support vector machine (SVM) & Hamming Distance is proposed. The SVM, a learning method introduced by Vapnik, tries to find an optimal hyperplane for separating two classes Therefore, the misclassification error of data both in the training set and test set is minimized. The best hyperplane for an SVM means the one with the largest margin between the two classes. Margin means the maximal width of the slab parallel to the hyperplane that has no interior data points.The support vectors are the data points that are closest to the separating hyperplane; these points are on the boundary of the slab.

II .OVERVIEW OF PRIOR WORK

A. Artificial Neural Network Approach

Artificial Neural Network Approach describes the wide usability of neural network approach since it is very simple and powerful. There are 2 steps usually. In the first step features representing the signature are extracted. And a classification is performed on the samples. After the classification it is easily possible to determine if a signature is matching with any of the classes.
It performs a study on two approaches. It is basically determination of a class then the match the signature. The two approaches are: 1) The Resilient Back propagation (RBP) neural network. 2) Radial Basic Function (RBF). Around two thousand test signatures are available in the database which is mixture of genuine and forgeries with a ratio of 4:6.[1]

B. Hidden Markov Models Approach

Hidden Markov Models Approach describes about an online signature verification system that is based on Hidden Markov Modeling (HMM) technique. Set of localized direction features are extracted from a scanned signature image and this technique is applied on them. There is an elaboration on understanding HMM as stochastic models and their ability to determine distinctness and similarity of the patterns. Also speaks about how HMM states can be varied to analyze the state transition topology. Around samples of 100 users are used containing genuine and skilled random forged signature samples to do the testing [4].

C. Template matching techniques

Template matching techniques developed a system that uses a closed contour tracing algorithm to represent the edges of each signature with several closed contours. The curvature data of the traced closed contours are decomposed into multiresolutional signals using wavelet transforms. The zero crossings corresponding to the curvature data are extracted as features for matching. A statistical measurement is devised to decide systematically which closed contours and their associated frequency data are most stable and discriminating. Based on these data, the optimal threshold value which controls the accuracy of the feature extraction process is calculated. Matching is done through dynamic time warping. For each experiment, twenty-five writers are used with ten training signatures, ten genuine test signatures, ten skilled forgeries, and ten casual forgeries per writer [10].

D. Statistical approach

Statistical approach performs a study on statistical approach. Here patterns are considered as the features which is nothing; but a point in a Dimensional space. In a d-dimensional feature space the pattern vectors are kept in a close and disjoint regions hence categorizing the pattern vectors separately. A set of properly detached patters is considered as useful. A Hidden Markov Model (HMM) and Bayesian models used for pattern recognition are very popular examples of statistical approach. A Statistical approach is better than template matching approach in detecting even the adept forgeries [3][4].

III. PROPOSED APPROACH

For automatic processing of signature following steps are involved. Fig. 3 shows the main steps of signature recognition

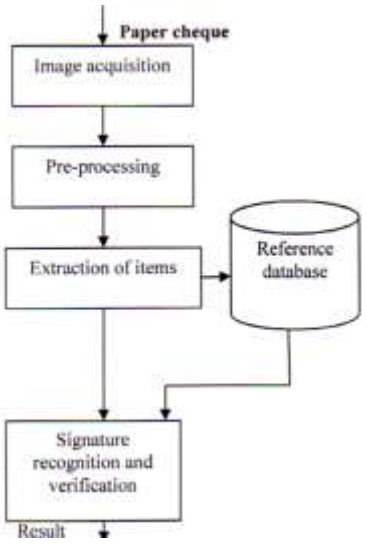


Fig. 3 Steps for signature recognition

A. Image Acquisition

Signature acquisition is the process in which the signature is digitized or scanned using a scanner or photographed with a camera of high resolution. A digital 2D image of the signature is the input to the signature verification system [11]. A camera will be a high definition USB portable which is to be initialize in MATLAB.

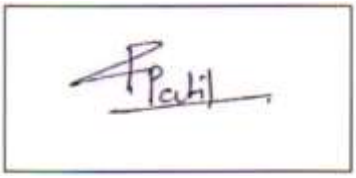


Fig. 4 Image acquired

B. Pre-processing

Preprocessing help us to improve the property of signature. The scanned signature image may carry spurious noise and has to be removed to avoid errors and make the signatures ready for feature extraction in both training and testing phase. The prepossessing stage includes following steps.

Step 1: RGB to gray scale conversion

In this step RGB image is converted into gray scale intensity signature image to eliminate the hue and saturation information while retaining the luminance Fig. 5.

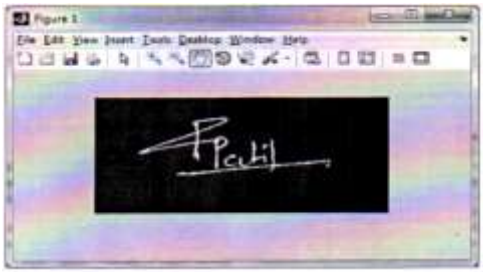


Fig.5 RCB to Gray converted image

Step 2: *Background elimination*

Data area cropping must be done for extracting features. In this we use image morphing instead of cropping so that noise reduction in great extent. P-tile thresholding was chosen to capture signature from the background. After the thresholding the pixels of the signature would be "1" and the other pixels which belong to the back-ground would be "0", as shown in fig. 6

Fig. 6 Morphed image

Step 3: Noise Reduction

A noise reduction filter is applied to the binary image for eliminating single black pixels on while background. 8-neighbors of a chosen pixel are examined. If the number of black pixels is greater than number of white pixels, the chosen pixel will be black otherwise it will be white [2].

Step 4: Resize

Each signature should be of same size, this reduces the area of signature to be used for further processing.

C. Feature Extraction

Feature Extraction is an important phase in recognition process. The objective of this phase is to extract the features of the test image that will be compared to the features of original image for verification purpose.

Some extracted features are:-

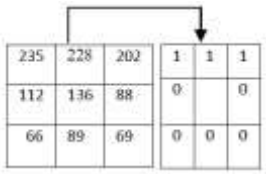
1) Local Binary Pattern (LBP) and Local Directional Pattern (LDP)

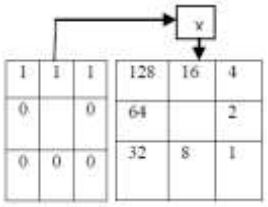
The Local Binary Pattern (LBP) operator is defined as gray level texture measure in a local neighbourhood. The most important property of the LBP operator is its invariance against monotonic gray level changes. Equally important is its computational simplicity. LBP operator describes the surroundings of a pixel. Each ILBP(x, y) code is worked out as follows: the eight neighbouring pixels are binarized using as threshold the center gray level value I(x, y), generating a binary 1 if the neighbour is greater than or equal to the center; otherwise it generates a binary 0. The eight binary number are represented by 8-bit number and saved in ILBP(x, y), the range which is $0 \leq ILBP(x, y) \leq 255$

$$I_{LBP}(x,y) = \sum_{n=0}^{7} s(I_N(n) - I(x,y)).2^n$$

Where, s(I) =1 if I >0
=0 if I <0

Eg. of LBP operator
Thresholding





Hence we get 128+16+4=148
In this case I (x,y) =136.
$I_N(n)$ ={69,88,202,89,228,66,112,235 },
$I_N(n) > I(x,y)$ =1 or else 0.
so we get the set as {0,0,1,0,1,0,0,1},
so ILBP(x,y)=4+16+128=148.

LBP could also be extended to rotation constant operator and generalized gray level operator. The major limitation of LBP is it gets easily susceptible to noise and pen. All the users must use the same pen since LBP is more proficient to gain the distribution of personal ink when all users use the same pen. But when the personal ink distribution involves changes of pen, in such a cases the efficient algorithm could be LDP.

2) COMBINATION OF LBP AND LDP

LBP components of image are acquired and given as information to Local Directional Pattern and elements are extricated, utilizing these separated elements Hamming Distance is ascertained for match of signature. Blend of LBP and LDP exploits both force data and directional edge reaction [11].

3) Signature extraction

The textural and topological features of a signature are extracted using algorithms based on lD log Gabor and Euler numbers respectively. The resultant image generated by encoding the textural features is called Signature Code – log Gabor (SCLG). Euler numbers give a distance matrix which contains values extracted from the topological behavior of the signature. This Distance matrix is called Signature Code. In this we use distance matrix model with row-column order penalty factor is proposed. This model integrates the characteristics of vector detection, hamming distance and the longest common substring and carries out detection specific to near-synonyms, word deletion and changes in word order by redefining distance matrix and adding ordinal measures, making word similarity detection in terms of semantics and backbone word segmentation more effective and the returned results of retrieval better meet the requirements of users. In the process of text similarity calculation, segmentation preprocessing must be carried out in the first place, since participial accuracy determines that of paper similarity calculation [2].

For generating the Signature Code using 1D - log Gabor wavelet (SCLG), 2D normalized pattern is decomposed into a number of 1D signal. lD signal arc convolved with the 1D log-Gabor wavelets. A Gabor function is a harmonic wave modulated by a Gaussian function. Log-Gabor filters are used for natural textures which often exhibit a linearly decreasing log power spectrum. In the frequency domain, log-Gabor filter bank is defined as:

$$G_{ij}(\omega_r, \omega\phi) = G(\omega - \omega r_i^{\alpha}, \omega_{\phi i}^{\alpha})$$

Where, (r, ϕ) are polar coordinates,

ωr_i^{α} is the logarithm of the center frequency at scale i,
$\omega_{\phi i}^{\alpha}$ is the jth orientation
and G (ω_r , ωϕ) is defined as:

$$G(\omega_r, \omega_\phi) = \exp\left(\frac{\omega_r^2}{2\sigma_n^2}\right)\exp\left(\frac{\omega_\phi^2}{2\sigma_{\phi j}^2}\right)$$

where, σ_n^2 and $\sigma_{\phi j}^2$ are parameters of Gaussian functions.

4) Signature identification

Matching of the signatures includes matching of SCLG, with stored signature data. For matching SCLG, Hamming distance based matching algorithm is used. Hamming distance (HD) for the two SCLG is calculated using the equation below

$$HD = \frac{1}{N}\sum_{i=1}^{N} A_i \oplus B_i \text{ and } MS_{SCLG} = (1 - HD)$$

Where Ai and B, are the two bit-wise SCLGs to be compared. N is the number of bits represented by each SCLG. HD gives the matching score (MSSCLG) for SCLG. For handling rotation, templates are shifted left and right bit- wise and a number of HD values are calculated from successive shifts . The bit-wise shifting in the horizontal direction corresponds to rotation of the original signature template at an angle based on the angular resolution.

IV. MATCHING ALGORITHM

1) Support Vector Machine (SVM)

After the feature extraction stage, superiority of features extracted is quantified calculate the accuracy of the classifier. Classification is the final step of signature identification. For classification of signature classes, a layer of SVM classifier has used. An SVM is a classifier derived from statistical learning theory. The number of SVM classifiers in the classification layer is equal to number of signature classes. Vapnik introduced the beginning of SVM in late of 1970's. SVM, based on a solid mathematical foundation, which attempt resolve a universal problem of classification. The basic proposal of SVM is deceptively simple. Given a set of vectors in Rn, labeled +1 or -1 that is separable by a hyper plane, SVM finds the hyper plane with the maximal margin. In this mode, the kernel of SVM classifier is a one order polynomial classifier.

2) Hamming Distance

The Hamming distance between two strings of equal length is the number of positions at which the corresponding symbols are different. In another way, it measures the minimum number of substitutions required to change one string into the other, or the minimum number of errors that could have transformed one string into the other.

V. EXPECTED RESULT

LBP (Local Binary Pattern) is efficient when there are a group of signatures to be tested which are signed using the same pen and has less presence of noise. If the signature to be tested is signed with different pens then LDP (Local Directional Pattern) is useful. So LDPs give more accurate result than LBPs when there is no pen dependence.

We proposed offline signature verification based on LBP & LDP using SVM as classifier and Signature Extraction and identification by Hamming distance.

REFERENCES

[1] [1] Subhash Chandra, Sushila Maheskar, "*Offline signature verification based on geometric feature extraction using artificial neural network*",3rd Int'l Conf. on Recent Advances in Information Technology (RAIT), Dhanbad, 2016, pp. 410-414

[2] Raghvendra Shyamrao Patil, Sachin.B. Takale, "*Signature Verification by Distance Matrix* Method for Bank Cheque Process " International Conference on Electrical, Electronics Signals Communication and Optimization (EESCO) ,2015 pp 1-5.

[3] Asma Shakil, Sharifah Mumtazah Syed Ahmad, Rina Bt. Md. Anwar, Mustafa Agil Muhamad Balbed, "Analysis of the Effect of Different Features' Performance on Hidden Markov Modeling based Online and Offline Signature Verification Systems ", Digital Image Computing: Techniques and Applications (DICTA), 2008, Canberra, ACT, 2008, pp. 572-577.

[4] J. Coetzer, B. M. Herbst, J. A. du Preez, "Offline Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model" EURASIP Journal on Applied Signal Processing 2004:4, pp. 559–571

[5] Sarfraz and S.M.A.J. Rizvi, "An intelligent system for Online Signature Verification", 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), Cape Town, 2015, pp. 17-22.

[6] Mayank Vatsa, Richa Singh, Pabitra Mitra, Afzel Noore, " Signature verification using static and dynamic features", Springer,ICONIP 2004,LNCS 3316, pp. 350-335.

[7] Takashi Ito, Wataru Ohyama, Tetsushi Wakabayashi and Fumitaka Kimura, "Combination of signature verification techniques by

SVM" 2012 International Conference on Frontiers in Handwriting Recognition

[8] Mayank Vatsa, Richa Singh, Pabitra Mitra, and Afzel Noore, "Signature Verification Using Static and Dynamic Features" ICONIP 2004, LNCS 3316, pp. 350.355, 2004. Springer-Verlag Berlin Heidelberg 2004.

[9] N. Aqili, A. Maazouzi, M. Raji, A. Jilbab, S. Chaouki, A. Hammouch, "On-line signature verification using Point Pattern Matching Algorithm" 2nd International Conference on Electrical and Information Technologies ICEIT'2016 IEEE.

[10] Sanjay S. Gharde a , Harsha G. Chavan ,"Support Vector Machines for Off-Line Signature Verification and Identification using Contour let Transform " ELSEVEIR.

[11] D. Ashok Kumar and S. Dhandapani , " A Novel Bank Check Signature Verification Model using Concentric Circle Masking Features and its Performance Analysis over Various Neural Network Training Functions", Indian Journal of Science and Technology, Vol 9(31), DOI: 10.17485.

[12] Gurusiddayya hiremath, "Verification of offline signature using Local Binary and directional pattern", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. Issue 1, January 2016.

[13] MettaMadhavi, 2Manoj Reddy Yaram, Dr.R.V.Krishnaiah, "Effective Implementation techniques in Offline Signature Verification", IOSR Journal of Computer Engineering (IOSRJCE) Volume 5, Issue 4 (Sep-Oct. 2012), PP 25-30.