“Online Signature Verification on smart phone using discrete wavelet transforms.”

Kiran P. Nagbhidkar1, Prof Vijay Bagdi2
Department of Computer Science and Engineering,
Abha Gaikwad Patil college of engineering,Nagpur ,India.

ABSTRACT

Handwritten signature is the most widely accepted to identity verification. The target of research is to present online handwritten signature verification system based on discrete wavelet transform (DWT) features extraction. Steps for verifying online handwritten signature in this system start with extracting pen position data (x and y positions) of points that forming the signature. Pen-movement angles are then derived from pen position data. To reduce variations in pen-position and pen-movement angles dimensionality, data are normalized and resampled.

To enhance the difference between a genuine signature and its forgery, the signature is verified in DWT domain. Low frequency sub-band signals (approximations) of pen-position parameter and pen-movement angle parameter are considered as intrapersonal features. These are used for suppressing variations between different genuine signatures and enhancing the interpersonal variations, hence are given higher scores within total recognition process. Both of pen-position and pen-movement angle features are then associated for obtaining a decision about online handwritten signature verification.

I. INTRODUCTION

There exist a number of biometrics methods at present, e.g. Signatures, fingerprints, iris, etc. Fingerprints and iris verification require the installation of costly equipments and hence cannot be used at day to day places like banks, etc. There is considerable interest in authentication based on handwritten signature verification system as it is the cheapest way to authenticate a person. Banks and Government bodies recognize signatures as a legal means of authentication. Signature verification technology utilizes the distinctive aspects of the signature to verify the identity of individuals. Criminal experts cannot be employed at every place and hence there has been considerable effort towards developing computerized algorithms that could verify and authenticate the individual’s identity. A handwritten signature is biologically linked to a specific individual. Modern forensic document examiners commonly compare a suspect signature with several examples of known valid signatures. They look for signs of forgery which include:

Signatures written at a speed which is significantly slower than the genuine signatures, frequent change of the grasp of the writing implement, rounded line endings and beginnings, poor line quality with hesitant and shake of the line, retracing and patching, and stops in places where the writing should be free. Compared with other electronic identification methods such as fingerprints scanning and retinal vascular pattern screening, it is easier for people to migrate from using the popular pen- and paper signature to one where the online handwritten signature is captured and verified electronically. Many times the signatures are not even readable by human beings. Signature verification problem therefore is concerned with determining whether a particular signature truly belongs to a person or not. There are two approaches to signature verification, online and offline differentiated by the way data is acquired.

In offline case, signature is obtained on a piece of paper and later scanned. Offline signature verification deals with a 2D static image record of the signature. It is useful in automatic signature verification found on bank checks and documents authentication. Offline verification techniques are based on limited information available only from shape and structural characteristics of the signature image. A fundamental problem in the field of offline signature recognition is the lack of a significant shape representation or shape factor.

In contrast, online signature verification systems are extremely precise. It require the presence of the author during both the acquisition of the reference data and the verification process. This restrict their use to specific applications. Online handwritten signature is usually obtained on an electronic tablet and pen. Automatic online signature verification is an

interesting intellectual challenge with manypractical applications. This technology examines the behavioral components of the signature such as: stroke order, speed, and pressure, as opposed to comparing visual images of signatures. Unlike traditional signature comparison technologies, online signature verification measures the physical activity of signing. The target of this research ispresent online handwritten signature verification system based on DWT features extraction and neural network classification.

The paper is organized in following sections. Section1: gives a brief introduction; Section 2: overview near sets; Section 3: will focus on proposed approach followed by experimentation and simulation result, conclusion and future scope.

II. RELATED WORK

Napa Sae-Bae et al [1] proposed online signature verification ontouch interface-based mobile devices. A simple and effective method for signature verification is developed. An online signatureis represented with a discriminative feature vector derivedfrom attributes of several histograms that can be computed inlinear time. The resulting signature template is compact andrequires constant space.

Alderson et al [2] proposed a new hybrid handwritten signature verification system where the on-line reference data acquired through a digitizing tablet serves as the basis for the segmentation process of the corresponding scanned off-line data. Local foci of attention over the image are determined through a self-adjustable learning process in order to pinpoint the feature extraction process. Both local and global primitives are processed and the decision about the authenticity of the specimen is defined through similarity measurements.

Loris Nanni et al [3] proposed an on-line signature verification system exploiting both local and global information through decision-level fusion is presented. Global information is extracted with a feature-based representation and recognized by using Parzen Windows Classifiers. Local information is extracted as time functions of various dynamic properties and recognized by using Hidden Markov Models. Experimental results are givenon the large MCYT signature database (330 signers, 16500 signatures) for random and skilled forgeries.

Trevathan Jarrod et al[4] proposed a method for verifying handwritten signatures where 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. In this paper a method for verifying handwritten signatures by using a 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 is proposed. Several Network topologies are tested and their accuracy is compared. The most successful version of the NN based HSV system uses a single MLP with one hidden layer to model each user's signature. It is trained using five genuine signatures and one hundred zero-effort forgeries. .

McCabe et al [5] proposed an handwritten signature verification system based on a Hidden Markov Model approach for representing and verifying the hand signature data. The paper presents a HSV system that is based on a Hidden Markov Model (HMM) approach to representing and verifying the hand signature data. HMMs are naturally suited to modelling flowing entities such as signatures and speech. The resulting HSV system performs reasonably well with an overall error rate of 3.5% being reported in the best case experimental analysis.

D. Guru et al [6] proposed a method for on-line handwritten signature verification . The signatures are acquired using a digitizing tablet which captures both dynamic and spatial information of the writing. After preprocessing the signature, several features are extracted. The authenticity of a writer is determined by comparing an input signature to a stored reference set (template) consisting of three signatures. The similarity between an input signature and the reference set is computed using string matching and the similarity value is compared to a threshold.

M Zanuy et al [7] proposed pattern recognition algorithms for on-line signature recognition: vector quantization (VQ), nearest neighbor (NN), dynamic time warping (DTW) and hidden Markov models (HMM). An another combined DTW–VQ scheme which enables improvement of privacy for remote authentication systems, avoiding the submission of the whole original dynamical signature information (using code words, instead of feature vectors) is proposed .Several algorithms for on-line signature recognition have been analyzed. Some algorithms that do not take into account the temporal evolution of the signal are: VQ and NN. This system achieves similar performance than DTW when using codes system achieves similar performance than DTW

Luan L. Lee et al [8] proposed line dynamic signature verification systems A data base of more than 10,000 signatures in (I, y(t))-form was acquired using a graphics tablet An algorithms for selecting and perhaps orthogonalizing features in accordance with the availability of training data and the level of system complexity is proposed .

Maiorana et al [9] proposed an approach, reffered as BioConvolving, that is able to guarantee security and renewability to biometric tem- plates. BioConvolving approach is evaluated, both in terms of authentication rates and renewability capacity, using the MCYT signature database. The reported extensive set of experiments shows that protected and renewable biometric templates can be properly generated and used for recognition, at the expense of slight degradation in authentication performance.

III. BASIC TERMINOLOGY

Signature Verification:

Signature verification in the system is done in following manner:

1. Data Acquisition:
Signature signals are captured using a digitizing device or touch screen as a PDA or Tablet-PC. The signature signal is sampled and stored as discrete time series. While some digitizing tablets provide pressure or pen angle information, these are not commonly available in handheld devices. Pre-processing tasks such as noise filtering and alignment may be carried out in this phase.
2. Feature Extraction:
Two main approaches have been followed in this step: *feature-based* systems extract global features (e.g. signature duration, num- ber of pen-ups, average velocity) from the signature in order to obtain a holistic feature vector. *Function-based* systems use the signature time functions (e.g. position, pressure) for verification.
3. Enrollment:
In *model-based* systems a statistical user model is computed using a training set of genuine signatures which is used for future comparisons in the matching step. *Reference-based* systems store the features of each signature of the training set as templates. In the matching process the input signature is compared with each reference signature.
4. Similarity Computation:
This step involves *pre-alignment* if necessary and a *matching* process, which returns a *matching score*. In feature-based systems, statistical techniques like Mahalanob is distance, Parzen Windows or Neural Networks are used for matching [9]. Function-based systems use other techniques like Hidden Markov Models (HMM) [10], or Dynamic Time Warping (DTW) [11] to compare signature models.
5. Score Normalization:
The matching score may be normalized to a given range. More sophisticated techniques like target- dependent score normaliza- tion can lead to an improved system performance [12]. An input signature will be considered from the claimed user if its matching score exceeds a given threshold.

III. PROPOSED APPROACH

The proposed online handwritten signature recognition system consists mainly of three phases: Signal modeling, feature extraction, and feature matching. The x and y positions of signature points are extracted and each is represented as 1D time domain signal. Pen moving angles are derived from pen position data points. It is then used as the third time domain signal. These signals are then normalized and resampled. This is to overcome the problem of different sizing and different number of points exists in every signature even for the same user.

Discrete wavelet transform is used to extract features from these signals. Sub-band decomposition is used to extract intrapersonal features from the DWT features to enhance signature individuality. The extracted feature vectors are used to train back propagation neural networks bank that are used within multi matcher as a classifier. In the testing phase, signals which were captured from a signature of unknown person are subjected to feature extraction. The resulting features are inputted to the bank of the trained neural networks of multi matcher. The resultant outputs are allowing the unknown signature to be identified if it is a genuine handwritten signature or not.

To summarize, two algorithms are of critical importance to handwritten identification system. The first is feature extraction process (obtained from discriminatory information). The second is classification process (using the features to determine the correct signal, which corresponds to the correct handwritten signature). The proposed handwritten signature verification system is shown in Fig. 1.

Features extraction process of handwritten signatures
The feature extraction process in this research starts with pen position data. Two factors are considered: pen positions in x direction and pen position in y direction. Pen movement angles are derived from pen position data as a third factor. The number of points in a captured handwritten signature varies with respect to its size and speed of writing even for the same individual. To overcome different sizes of signature, data points that represents x position and y position are normalized.

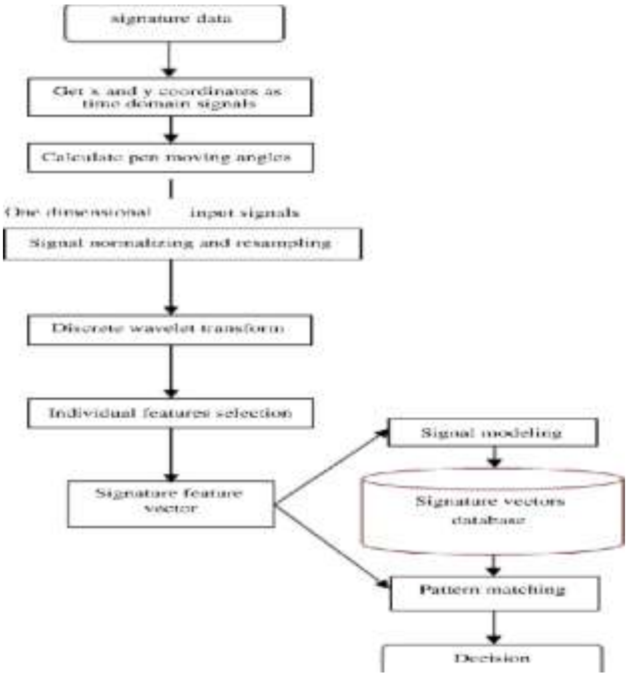
signature data
Get x and y coordinates as time domain signals
Calculate pen moving angles
One dimensional input signals
Signal normalizing and resampling
Discrete wavelet transform
Individual features selection
Signature feature vector
Signal modeling
Signature vectors database
Pattern matching
Decision

Fig : Online handwritten signature verification system based on extracting DWT features and neural network classification.

To overcome different sizes of signature, data points that represents x position and y position are normalized. It is difficult to train a neural network for such large variations in number of points represent a signature. Hence, it is desirable to resample the signature contour to obtain fixed number of points. As a consequence, each of the three factors should be normalized and resampled . The feature extraction process then ends with taking out DWT coefficients for pen positions in x direction, and pen positions in y direction, and pen movement angles.

V. OBJECTIVE OF THE PRESENT WORK

- Extract the various features of stored images.
- Use these features to train the classifier
- Employ unknown Signature image and extract its features.
- Perform the pattern matching with data set
- Do the classification and classify as genuine or forged.

VI. CONCLUSION

Online handwritten signature verification system based on extracting sub-bands that represent intrapersonal features of signature from DWT representations of that signature is presented in this paper. Both extracted pen position and derived pen-movement angle parameters of handwritten signature data were decomposed into sub-band signals by DWT. Low frequency (approximations) and high frequency (details) sub band signals were extracted for these parameters. Low frequency sub-band signals (approximation) are found consistent as features to enhance the difference between a genuine signature and its forgery. This is at least when using it in the recognition process with the signature database used in this research.

The signature database consists of 20 genuine signatures for each of five users as well as 20 skilled forgeries for each user. A multi matcher (recognizer) consisting of six neural networks is used to recognize online handwritten signature. The inputs to this multi matcher are approximations and details of DWT coefficients for each of the three used parametersof a signature. The results show that success rate of the recognizer is 100% when tested with signatures it has been trained to recognize. When only selected DWT features (that enhance interpersonal and suppress intrapersonal variations) are used in training and recognition processes, it results in improving the accuracy. Success rate of the recognizer is up to 95% when tested with untrained genuine signatures.

Also, the rate of recognizing forgery signature as a genuine one is down to 8%. System performance could be improved if genuine signatures are more correlated and intrapersonal variations among it is low. Zero misclassification is required in such applications even if it is in the expense of high recognition rate. Other required target is that the recognition probability of forgery signature as if it is a genuine one is zero. Future work targets at further improving resultant system accuracy by fine tuning the selection of individual features(coefficients) that enhance the variation between genuine and forgery signatures. Also ,improving the performance by selecting correlated genuine signatures as the training samples. Moreover, looking for better methods for selecting coefficients that represent intrapersonal features and hence could improve system performance. Furthermore, to compare performance of this system to performance of other systems when using same online handwritten signatures databases.

VII. References

[1] Napa Sae-Bae and Nasir Memon. Online Signature Verification on Mobile Devices. VOL. 9, NO. 6, June 2014

[2] Zimmer Alessandro, Ling Lee Luan. A hybrid on/off line handwritten signature verification system. In: Seventh international conference on document analysis and recognition (ICDAR'03), vol. 1; 2003. p. 424.

[3] Julian Fierrez-Aguilar1, Loris Nanni2, Jaime Lopez-Pe˜nalba1, An On-Line Signature Verification System Based on Fusion of Local and Global Information.

[4] Trevathan J. Markov model-based handwritten signature verification. In: International conference on embedded and ubiquitous computing (IEEE/IFIP); 2008.

[5] Tolba AS. GloveSignature: a virtual-reality-based system for dynamic signature verification. Digital Signal Process 1999;9(4): 241–66.

[6] D. Guru and H. Prakash, "Online signature verification and recognition: An approach based on symbolic representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 6, pp. 1059–1073, Jun. 2009.

[7] M. Faundez-Zanuy, "On-line signature recognition based on VQ-DTW," *Pattern Recognit.*, vol. 40, no. 3, pp. 981–992, 2007.

[8] Lee Luan L, Berger Toby, AviczerErez. Reliable on-line human signature verification systems. IEEE Trans Pattern Anal Mach Intell 1996;18(6):643–7

[9] E. Argones Rua, E. Maiorana, J. Alba Castro, and P. Campisi, "Biometric template protection using universal background models: An application to online signature," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 269–282, Feb. 2012