Enhanced Digital Human Signature Verification over Web and Mobile Interfaces

Vijila Rexline X
Department of computer Science and Engineering, University College of Engineering, konam, Nagercoil.

K. L. Neela
Asst. Prof, Department of computer Science and Engineering, University College of Engineering, konam, Nagercoil.

Abstract – Digital signature verification technologies merging continuously. To achieve the goal an enhanced effective method for signature verification implemented from the simple existing mechanism. An online signature is represented with a discriminative feature vector derived from attributes for several histograms that can be computed in linear. The resulting signature template is compact and requires constant space. The algorithm was first tested on the well-known MCYT-100 and SUSIG datasets. There results show that the performance of the proposed technique is comparable and often superior to state of the art algorithms is simplicity and efficiency. In order to test the proposed method over finger drawn signatures on touch devices or a web or pc interfaces, datasets were collected from uncontrolled environments and multiple sessions. Experimental results on third data set confirm the effective of the proposed algorithm in mobile settings. There results demonstrate the problem of within user variation of signatures cross multiple sessions and the effectiveness of cross session training strategies to all deviate the problems.

Index Terms – Signature authentication, Manhattan distance method, Histogram, Feature Extraction, Template generator.

1. INTRODUCTION

Signature is a biometric attribute. It is used to confirm various financial transactions, officially approve contents of some documents, etc. Signature verification is generally done by considering just the visual appearance of the signature. However the image or the visual appearance of the signature is not enough for verification. Signature is the only biometric entity that provides dynamic characteristics along with morphological characteristics. It is difficult to construct a signature with similar shape and identical dynamic characteristics at the same time. This paper aims at creating a module which can verify a signature on the basis of its time based features by digitizing the signature. This will reduce forgeries and fraud cases. Online signature verification can be used in various applications where handwritten signatures are currently collected such as cashing a check, authenticating legal documents and other banking transactions where PIN codes are used. In addition, a signature template is stored in an irreversible form thereby providing privacy protection to an original online signature. The proposed method was evaluated on public datasets as well as new dataset collected in in uncontrolled setting from user owned mobile devices.

2. RELATED WORK

Vector quantization (VQ), nearest neighbor (NN), dynamic time warping (DTW) and hidden Markov models (HMM). The VQ and NN algorithms have been neglected so far, but have been useful in the past for other biometric traits, such as speech, especially for short training and testing sets. The merits of this paper are that it avoids the submission of the whole original dynamic signature information. It also reduces a computational burden [2].

In periocular refers to the facial region in the immediate vicinity of the eye. Acquisition of the periocular biometric is expected to require less subject cooperation while permitting a larger depth of field compared to traditional ocular biometric traits (viz., iris, retina, and sclera). The feasibility of using the periocular region as a biometric trait. Global and local information are extracted from the periocular region using texture and point operators resulting in a feature set for representing and matching this region effect of template aging on matching performance[10].

Method for signature verification and recognition based on the symbolic representation are also proposed. The notions of writer-dependent threshold and introduce the concept of feature-dependent threshold to achieve a significant reduction in equal error rate. An online signature is a behavioral biometric used for personal authentication to complete automated transactions, gaining control of computing facilities or physical entry to protected areas. A new method of symbolic representation for online signatures is the methods for signature verification and recognition, based on a novel similarity measure. It exploitation of the concept of writer-dependent threshold [4].

The performance of a protected on-line signature recognition system employing the proposed Bio Convolving approach is evaluated, both in terms of authentication rates and renewability capacity, using the MCYT signature database. The concept is proposed protection approaches have been applied to an on-line signature based authentication system, where HMMs are employed for template matching. The proposed approach can be therefore applied to a variety of

biometric modalities, for example, speech biometrics where spectral or temporal analysis of the voice signal produces discrete sequences, or to signature and handwriting recognition, where the extracted sequences are related to the pen's position, applied pressure, and inclination [6].

3. PROPOSED MODELLING

A handwritten signature is an efficient method and there are two types of handwritten signature verification systems: off-line and online systems. In an off-line system, just an image of the user's signature is acquired without additional attributes, whereas, in an online system, a sequence of x-y coordinates of the user's signature, along with associated attributes like pressure, time, etc., are also acquired. As a result, an online signature verification system usually achieves better accuracy than an off-line system.

The increasing number of personal computing devices that come equipped with a touch sensitive interface and the difficulty of entering a password on such devices have led to an interest in developing alternative authentication mechanisms on them.

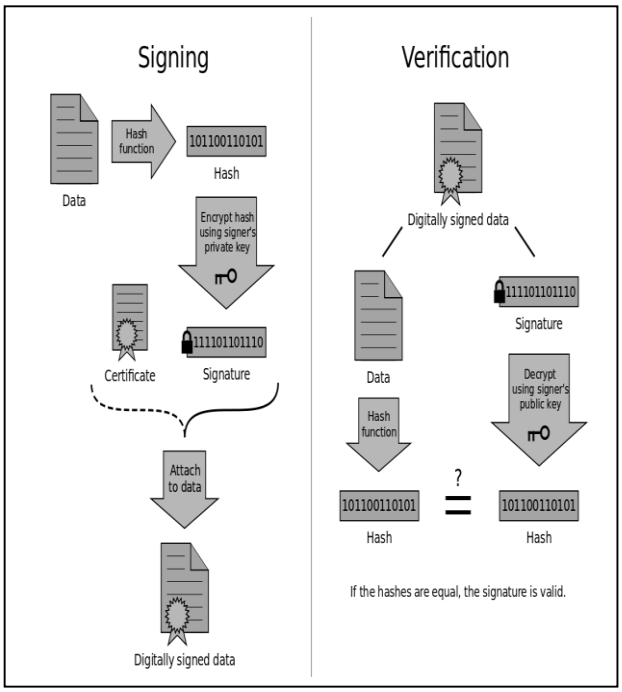


Fig: Architecture Diagram

In this context, an online signature is a plausible candidate given the familiarity users have with the concept of using a signature for the purpose of authentication. There has been much work on online signature verification systems. However, none of this has been directed to the context of authentication on mobile devices.

An "Online Signature" is a biometric modality that uses, for verification purposes, the anatomic and behavioral characteristics that an individual exhibits when signing his or her name.

The following list of modules are used for online signature verification are given below

- Enrollment time sample signature Preprocessing
- Enrollment time sample signature feature extraction
- Template histogram generation
- Query signature processing
- Manhatten distance based Matching process

3.1. Enrollment Time Sample Signature Preprocessing

The variation in the number of strokes per signature and sampling rate introduced in the dataset can affect verification performance. Hence, all signatures were pre-processed by time normalization and stroke concatenation before extracting histogram features.

Signature Stroke Concatenation: As shown in the above Figure most of the signatures in this dataset have multiple strokes. Signatures with multiple strokes may pose a challenge to verification algorithms by introducing positional variation for each of the strokes. This variation could become larger when the signatures are signed on touch devices using a fingertip since each touch point may not coincide with user's intention.

3.2. Enrollment Time Sample Signature Feature Extraction

The feature extraction process of the proposed system begins by converting the time-series data of a signature in to a sequence of Cartesian vectors and attributes, as well as their derivatives. This subsection describes how a set of histograms are computed from an online signature. These histograms are designed to capture essential information of an online signature attributes as well as the relationships between these attributes.

Histograms are widely used as feature sets to capture attribute value distribution statistics in many recognition tasks, for instance, in object recognition and off-line signature verification .Then, each Cartesian vector is also converted to a vector in the polar coordinate system. Finally, histograms from these vector sequences are derived. These include x-y trajectories, speed, angles, and their derivatives.

3.3. Template Histogram Generation

A user template is generated during the enrollment process where multiple signatures are acquired from a user and a feature set is computed from each of the samples. Finally, the average of these feature vectors is used as the template F^u for that user.

During verification, a user claiming an identity u is asked to produce one instance of an online signature which is again represented by the set of features. Next, the system compares this feature vector against the stored feature vector template, F^u. The signature is accepted if the Euclidian distance between these two vectors is less than a predefined threshold, otherwise it is rejected.

3.4. Query Signature Processing

The variation in the number of strokes per signature and sampling rate introduced in the dataset can affect verification performance. Hence, all signatures were pre-processed by time normalization and stroke concatenation before extracting histogram features.

Histograms are widely used as feature sets to capture attribute value distribution statistics in many recognition tasks, for instance, in object recognition and off-line signature verification .Then, each Cartesian vector is also converted to a vector in the polar coordinate system. Finally, histograms from these vector sequences are derived. These include x-y trajectories, speed, angles, and their derivatives.

3.5. Manhatten Distance Based Matching Process

The matching processes do the authentication process for signature using Manhatten distance method. The matching process is done for query signature against the template signature. If the matching score is less than an optimal threshold then the query signature is a authenticated one otherwise not. The system then accepts the sample if the dissimilarity score is less than a predefined threshold, otherwise it rejects.

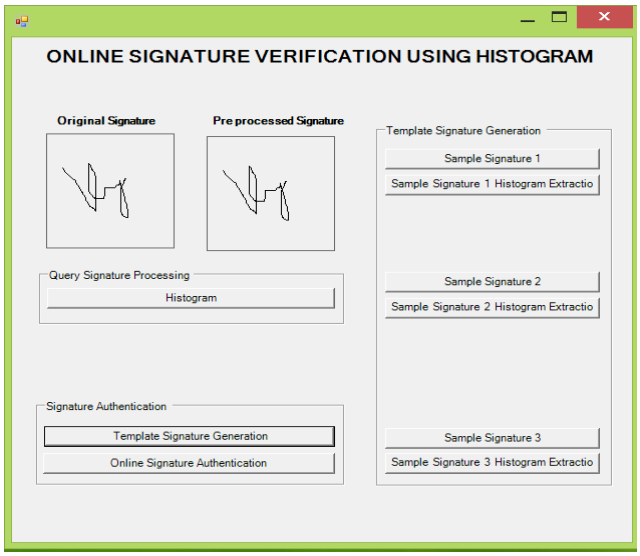
Manhatten distance is the square root of the sum of absolute differences between corresponding elements of the two vectors. Here high similarity means low distance value and low similarity means high distance value. If the distance value is less than the optimal threshold and difference is less than the threshold then the query signature verification is announced as an authenticated one, otherwise it is announced as a unauthenticated one.

This paper proposes an efficient method for online signature verification. The x difference, y difference, angle and speed properties are extracted to generate histogram features. The matching process is done using Manhattan distance method. The template signature and query signature can be used to verification process. This method is well suitable for mobile devices which have touch interfaces because of online verification support. The proposed scheme has the best performance and accuracy than the existing system.

4. RESULTS AND DISCUSSION

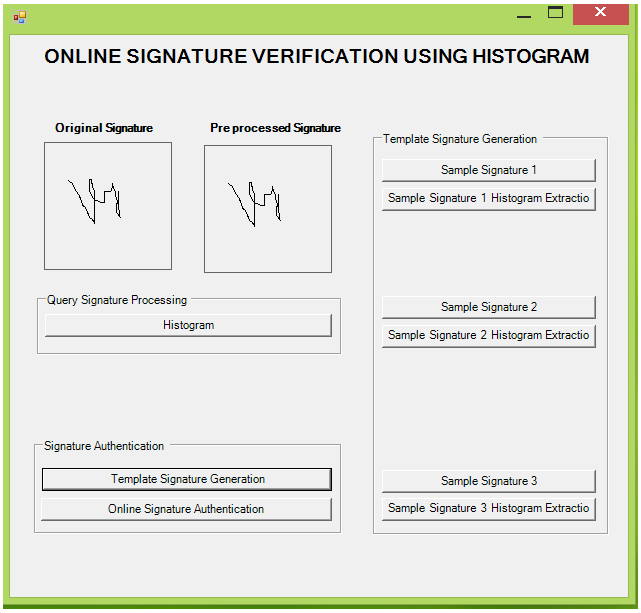
4.1 INPUT IMAGE

Preprocessing stage to concatenate the signature and analyses the pixel value. Time normalization and stroke concatenation before extracting histogram features.



(A) Pre processing Image

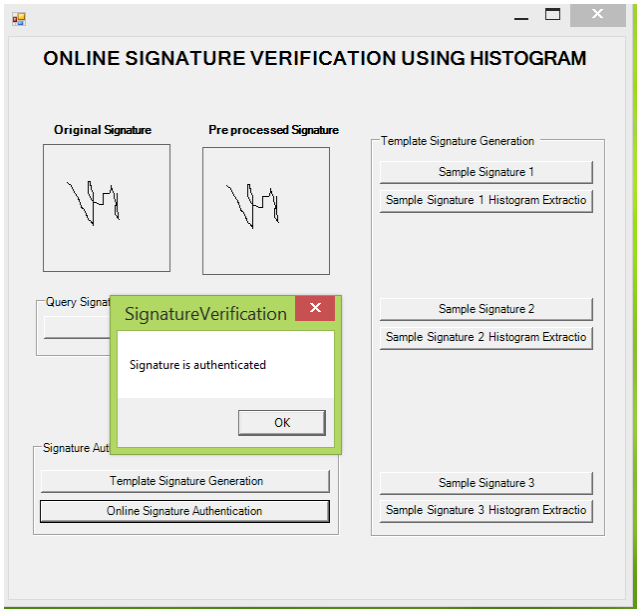
The variation in the number of strokes per signature and sampling rate introduced in the dataset can verification performance.



(B) Template Generation

The matching processes do the authentication process for signature using Manhatten Distance method. The matching

process is done for query signature against the template signature.



(C) Signature Authentication

5. CONCLUSION

The x difference, y difference, angle and speed properties are extracted to generate histogram features. The matching process is done using Manhattan distance method. The template signature and query signature can be used to verification process. This method is well suitable for mobile devices which have touch interfaces because of online verification support. The proposed scheme has the best performance and accuracy than the existing system. The main contribution of our method is to consider the geometric properties of a signature in recognition problems, using the segmented dissimilarity scores for verification. Thus the proposed method utilizes the dynamic features of signatures, which ensured the high security of identification systems. Furthermore the proposed algorithm need not know any information about the characteristics of the forgeries; the decision boundary is constructed wholly from the signature in enrollment procedure. Also experimental results demonstrated good performance of the proposed algorithm.

REFERENCES

[1] ArgonesRua E, MaioranaE,Alba J Castro, and P. Campisi,(2012) "Biometric template protection using universal background models: An application to online signature," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 269–282.

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

[3] Feng H and Wah C,(2003) "Online signature verification using a new extreme points warping technique," Pattern Recognit. Lett., vol. 24, no. 16, pp. 2943 2951.

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

[5] Kholmatov and Yanikoglu B,(2005) "Identity authentication using improved online signature verification method," Pattern Recognit. Lett.,vol. 26, pp. 2400–2408.

[6] Maiorana E,Campisi P, J. Fierrez, J. Ortega-Garcia, and Neri A, (2010)"Cancelable templates for sequence-based biometrics with application to on-line signature recognition,"IEEETrans. Syst., Man, Cybern. A, Syst., Humans, vol. 40, no. 3, pp. 525–538.

[7] Nanni L and Lumini A,(2008) "A novel local on-line signature verification system," Pattern Recognit. Lett., vol. 29, no. 5, pp. 559–568.

[8] Nelson W, Turin W, and Hastie T,(1994) "Statistical methods for on-line signature verification," Int. J. Pattern Recognit. Artif. Intell., vol. 8, no. 3, pp. 749–770.

[9] Odinaka,LaiP,KaplanA,Sullivan J O,Sirevaag E, and Rohrbaugh J, (2012) "ECG biometric recognition: A comparative analysis," IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1812–1824.

[10] Park U, Jillela R, Ross A, and Jain A K,(2011) "Periocular biometrics in the visible spectrum," IEEE Trans. Inf. Forensics Security, vol.6, no.1, pp. 96–106.

[11] Plamondon L G and Plamondon R,(1989) "Automatic signature verification and writer identification—The state of the art," Pattern Recognit., vol. 22, no. 2, pp. 107–131.

[12] Qiao Y, Liu J, and Tang X (2007) "Offline signature verification using online handwriting registration," in Proc. IEEE Conf. CVPR, pp. 1–8.

[13] Sae-Bae N, Memon N, Isbister K, and Ahmed K,(2014) "Multitouchgesturebased authentication," IEEE Trans. Inf. Forensics Security, vol. 9,no. 4, pp. 568–582.

[14] Uludag U, Ross A, and Jain A,(2004) "Biometric template selection and update: A case study in fingerprints," Pattern Recognit., vol. 37, no. 7, pp. 1533–1542.

[15] Yanikoglu B and Kholmatov A,(2009) "Online signature verification using Fourier descriptors," EURASIP J. Adv. Signal Process., vol. 1, p. 260516.