www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 5 May 2016, Page No. 16365-16368

Authentication System for Any Touch Devices Using DWT

Vasundhara M. Goslar(M.E.), Mangala Madankar
Deptt. Of Wireless computing and communication
G.H. Raisoni College of Engineering
Nagpur, India.
vasugolar@gmail.com

(Assistant Professor)
Deptt. Of Wireless computing and communication
G.H. Raisoni College of Engineering
Nagpur, India.

Abstract— In today's world, the identification techniques based on human biometric features gaining much more importance. For e.g. Iris recognition system, face recognition system, finger print recognition system, retina scanning system, etc. Some important area of other techniques is also to recognize the human hand signature. Also, there is the requirement of some techniques which works automatically based on some standard computer algorithms for recognition. For e.g. to identify the criminal identity automatically based on biometric features. The aim of research is to develop an on-line system for signature verification using Discrete Wavelet Transform (DWT). Discrete Wavelet Transform (DWT) algorithm is used for features extraction. In online signature dynamic features are usually available. Genuine or Forgery signature is substantiating based features comparison. Each feature of an input signature is extracted using various steps discrete wavelet transform algorithm are matched against a reference signature to identify the genuine signature. The final decision of verification is made based on the matched features of both the signatures.

Keywords: Discrete Wavelet Transform (DWT),feature comparison, feature extraction.

General Teams

DWT……Discrete wavelet transform.
HMM……Hidden Markov Models
DTW……Dynamic Time Warping
NN……Neural Network
1D……One dimensional
2D……Two dimensional

I. INTRODUCTION

There has been much work on on-line signature verification systems. However, not even one of this has been directed to the context of authentication on mobile devices [3]. An example of finger drawn signatures on mobile devices work has addressed on-line signatures acquired using traditional digitizers in a controlled environment [4]. These are different from those acquired using mobile devices in a dynamic environments. First, on mobile devices, a user signatures is never same all the type and hence is different in different contexts, i.e, standing, mobile or immobile, or holding a device at different angles and orientations.

In addition, other characteristics of the system, i.e., a template aging and effectiveness of cross-sessions trainings, may be different when signatures are obtained from a mobile device. This paper proposes an online authentication system algorithm that is suitable to deploy on mobile devices [1]. It is computationally space efficient algorithm for verifying signatures.

In addition, template of signature is stored in an irreversible form for providing privacy and protection to an original on-line signature. The proposed method was evaluated on public datasets as well as on new datasets collected in uncontrolled setting from user owned touch devices. The verification performance obtained promising results. [9] The contributions of this paper are as follows:

1) A method to extract a model free from non-invertible feature set using an online signature is proposed. The feature set comprises sets of histograms that capture whose Personal use is accessed, but republication requires IEEE permission. By evaluating the proposed method on public datasets, its validation performance is higher in rank to several state of the art algorithms.

2) A new dataset was collected from 180 users in mobile device verification environment. Signatures in this dataset were drawn with a fingertip, in an uncontrolled setting on user owned ions devices and over six separate sessions with an intervals ranging from 12 to 96 hours.

3) The technical design applied on the given set of data, the following aspects of on-line signature verification on any touch devices were investigated:

• impact of template ageing on on-line signatures, effectiveness of using a cross-session samples, or multiple sessions patterns, to train a classifier,

• security of the system against forgery user or 0-effort attack and its comparison to that of 4-digit PIN.

A process of deriving a set of histograms from an online signature serves the details of the proposed system of online signature verification pattern , and analyzes its complexity. It provides experimental results on public datasets.

II .LITERATURE REVIEW

Lots of the signature verification work has been already done in the past years approaches. Automatic online handwritten signature verification system is used for prevention of the system for the dentition fraud to verify the authenticity of such as signatures on Australian passports is presented. In previous system following survey are done.

A. Automatic Handwritten Signature Verification system for Australian Passports:

Author MadasuVamsi K, Lovell Brian C, Kubik Kurt propose Automatic handwritten signature verification system is to prevent the system from fraud by verifying the authenticity of signatures . An automatic handwritten signature verification system and genuine or forgery authentication system is presented. The system is based on Takagi- Sugeno fuzzy model and involves structural parameters in its exponential function. The features consisting of each of the angles that are extracted using box approach windowing technique. Each feature corned to provide a fuzzy set with the classified techniques when all the training samples are considered for the observation because of the variations in a person's signatures the are having varying system [6].

B. A Hybrid On/Off Line Handwritten Signature Verification System:

Author Alessandro, Ling Lee Luan proposes a new hybrid of online signature verification system where the online system that merges the inputed data with generalised filter give output as the basis for the segmentation process of the respective scanned offline data system. The focal image are determined through a self recognised learning material process of the system in order to represent the feature extraction process. Both local and global task primitives are referred and processed for the system evaluation sheet and the decision are taken about the authenticity of the signature of the system . The global performance of the system is compared and measured using two different classifiers [5].

C. Neural network with handwritten signature verification System:

Author [10] proposes the method for verifying handwritten signatures where various kinds of static management (height and slant height) and dynamic kinds of management for e.g., velocity, pen tip pressure, etc signature features kinds are user specific are extracted and used to train the Neural network algorithm. Several Network topologies are tested and accuracy of his topology is compared. The resulting system performs agreeably well with an overall error rate of erroneous kinds of the issuing the system.

D. Markov model- with handwritten signature verification system:

Author [7]. Propose handwritten signature verification system based on the Hidden Markov Model for representing and verifying the hand signature data. This paper presents a HSV system that is based on the Hidden Markov Model (also called as HMM) approach to represent the data for streaming the verifying the signature. HMMs are naturally suited to modelling flowing entities such as signatures and speech. The new version of the imputed system reported in the best case experimental analysis [4].

III. ONLINE SIGNATURE VERIFICATION ALGORITHM

The proposed system comprises of three main components: a feature extractor, template generator and matcher. First, an online signature is processed by the feature extractor in order to compute a set of histograms using which a feature vector is derived. Then, the template generator constructs a user-specific template using the feature sets extracted from multiple enrolled signatures. This template is later used by the matcher to check a test signature. The rest of this section describes these three components in detail and analyzes system complexity. (For more details, please refer to [6] for the earlier version of this

DOI: 10.18535/ijecs/v5i5.09

work.) A. Feature Extractor In the proposed system, an online signature is to serve by a set of histograms.
These histogram features are designed to capture essential attributes of a signature as well as relationships between these attributes.For instance, in object [1] Fig. 2. The proposed online signature verification system recognition [8] and off-line signature verification [3]. Using histograms for online signature verification was first suggested by Nelson etal [4]. They have also been used as part of the feature set in [1] and [5]. However, in [1] and [9], the use of histograms is limited only to angles obtain from vectors connecting two consecutive points.

In fact, as is shown below, much more information can be used to produce from histograms useful in online signature verification. These include x-y trajectories, speed, angles, pressure, and their derivatives. Then, each Cartesian vector is also converted to a vector in the polar coordinate system. Details of the feature extraction process are as follows.

Let X = {x1, x2, . . . ,xn}, Y = {y1, y2, . . . , yn}, and P = {p1, p2, . . . , pn}, pressure attribute, respectively, of a signature with length n sampled at times T = {t1, t2, . . . , tn}.Datasets used for the first experiment, all signatures were patterned at a same rate. Hence the time is implicit and is thus it is ignored. Note, if time intervals are not an Obsolete, the process using information from T can be normally applied to the sequences X, Y, and P prior to being processed by the system. To start with, the vectors X1, Y 1, and P1 including their derivatives are computed as follows,
X1 = {x1 I |x1 I = xi+1 − xi }, (1a)
Y 1 = {u1i
|y1 I = yi+1 − yi}, (1b)
P1 = {pi }, (1c)
And Xk= {xki|xki= xk−1i+1− xk−1i}, (1d)
Y k = {yki|yki= yk−1i+1− yk−1i}, (1e)
Pk= {pki|pki= pk−1i+1− pk−1i}, (1f)
wherek >1 and i= 1, 2, . . . , n − k.

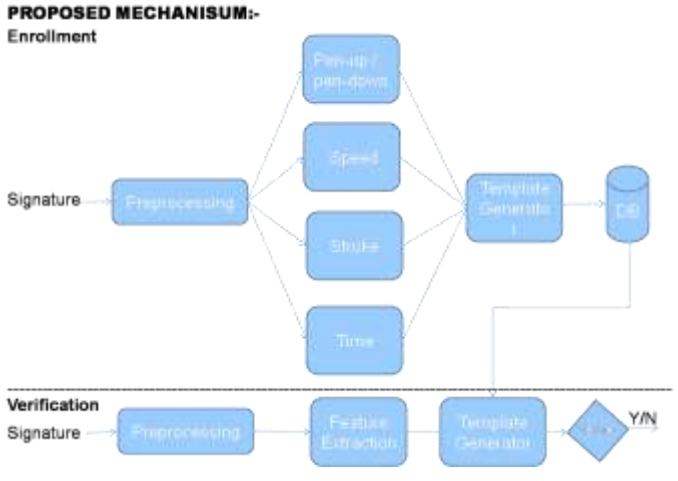

Fig 1. Flowchart of the proposed system

IV. HISTOGRAMS DESCRIPTIONS THAT ARE USED IN THE PROPOSED TECHNIQUE

The histograms are computed by the range of attribute values which are separated, into a number of equal width bin intervals, and counting the number of elements . For an angle attribute and its derivative, the histogram range is defined as [−π, π]. An outline process with cutoff at three standard deviations from its mean is applied preceding computing the mean and standard deviation of the attribute in order to derive its implicit range described, by forming a 24 bin histogram with equal width bin intervals starting from −π to π and counting the number of elements, {θ,1,i}, that fall into each of a 24 bins.

A. User Template Generator

User template generated during the enrollment process number of signatures are acquired from a user and a feature set is computed from every samples. Then, an instance of difference of each feature component is calculated and is used to construct a user-specific uniform quantize for each feature element resulting in a quantization step size vector Qu that is used to quantize every feature vectors derived from the enrollment samples. Let S be total number of enrolled samples and M be the total number of features for every sample. And let Fs j ={ f s j |i= 1, . . . , M} be a feature vector of the enrolled samples j of the user u where j = 1, . . . , S. The quantization step size vector of an user u, Qu = {qui| i= 1, . .M}, is obtained by computing the standard deviations over all the enrolled samples for each feature.That is, quI = β____1 SS_j=1 f s jI − µf (u)i 2, i= 1, . . . , M (3)
whereµf (u)
i= 1S
Sj=1 f s j i , β is experimentally fixed at 1.5.
Then, the quantized feature vector of each enrolled sample s of the user u, ˆF(s j |u) = { f ̃s ji|i=1, . . . , M} is derived from the quantization step sizes qui in Qu (adding a small _
to prevent division by zero) as follows, f ̃(s j |u)
i=f s j
i qui + _ , i= 1, . . . , M (4)
where_ is at 0.002 and 0.8 for histograms with absolute and relative frequencies, respectively.
at last, the user-specific feature vector template, ¨F u = { ¨f ui |i= 1, . . . , M}, is derived by averaging the quantized feature vectors of all the enrolled online signature samples from an user u.¨ f ui = ⌈⌊_Sj =1f ̃(s j |u)iS⌋⌉, i= 1, . . . , M (5)
A pair _Qu ,¨F u_ comprising of the quantization step size vector and its combined feature vector template is then stored and later used to verify signature of the user u.

B. Matcher

During the verification process it is given that t is maintain as a fact to be online signature sample from user u, ˆF (t |u)

is calculated using Qu. Then the system derives a difference score using manhattan distance between ¨F u and ˆF (t |u) as, Score = M, i=1f˜(t |u)i− ¨ f uI | (6)
The system then accepts the sample t if the difference between score is less than a form of threshold,otherwise it rejects.

CONCLUSION

Thus the system proposes a simplified version with effective technique of online signature verification system that is advisable for user authentication on a mobile device. The benefits of the proposed algorithm are as follows. First histogram based features set for representing an online signature can be derived in linear time and the system desire a little and established-size space to store the signature template. In addition, since the feature set represents apart statistics about the position, arrangement, or frequency of occurrence of original online signature attributes, the transformation is non-invertible. As a result, the confidentiality of the original biometric data is well-preserved. Second an user-specific classifier comprising of an user-specific of quantization step size vector and its combine quantized feature vector can be trained by using only enrollment samples from which user without involving a training set from a large number of users. Several experiments performed on MCYT and SUSIG datasets determine capability of the proposed process in terms of authentication performance as compared to existing algorithms.

REFERNCES

[1] MadasuVamsi K, Lovell Brian C, Kubik Kurt. Automatic handwritten signature verification system for australian passports. In: Science, engineering and technology summit on counterterrorism technology, Canberra, 14 July, 2005. p. 53–66.

[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] Trevathan Jarrod, Read Wayne, McCabe Alan. Neural network based handwritten signature verification. J Comput 2008;3(8): 9–22.

[4] McCabe A, 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] Gu¨ ler _Inan, MeghdadiMajid. A different approach to off-line handwritten signature verification using the optimal dynamic time warping algorithm. Digital Signal Process 2008;18(6):940–50.

[7] Bandyopadhyay SK, Bhattacharyya D, Das P. Handwritten signature recognition using departure of images from independence. In: 3rd IEEE conference on industrial electronics and applications (ICIEA 2008), Singapore, 2008.

[8] Zimmer Alessandro, Ling Lee Luan. Offline signature verification system based on the online data. EURASIP J Adv Signal Process 2008;2008:Article No. 112.

[9] Garcia-Salicetti S, Houmani N, Dorizzi B. A novel criterion for writer enrolment based on a time-normalized signature sample e ntropy measure. EURASIP J Adv Signal Process 2009;2009:Article No. 9.

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