GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

RESEARCH ON- SIGNATURE VERIFICATION ON SMART PHONE USING DWT

Kiran P. Nagbhidkar*[1] and Prof. Vijay Bagdi[2]
*[1,2]Department of Master of Engineering(Wireless Communication and computing)Nagpur, India

ABSTRACT

Handwritten signature is the most widely accepted to identity verification. Online Signature is highly appreciated and recommended due the security and authentication that it provided to various fields. Signature gives the unique identity to the person to prove its identity that iss why in every area signature has important role to authenticate the person. Handwritten signature is traditional way to prove the identity of person and at the same time to authenticate the person but there are certain limitations and drawbacks associated with it. Thus to overcome those drawbacks ,the target of research is to present online handwritten signature verification system based on number of parameters that application will calculate when the user sign on the application. The target of research is to collect the templates of signature and then comparing those with the actual signature. Certain techniques are also included to provide more security.

Keywords- *Feature Extraction, Change Detection, Foreground, Background.*

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 individuals 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 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 many practical 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 is to present online handwritten signature verification system that will calculate number of parameters associated with signature just like pen up, pen down, speed of the pen and number of strokes that will be produced during signature. The new thing that will be included in this research is that the name of the person will be stored in encrypted form in database so that if any person come to know the exact signature he or she will not be able to disclose the person of the signature.

II. LITERATURE SURVEY

Napa Sae-Bae et al [1] proposed online signature verification on touch interface-based mobile devices. A simple and effective method for signature verification is developed. An online signature is represented with a discriminative feature vector derived from attributes of several histograms that can be computed in linear time. The resulting signature template is compact and requires constant space. The algorithm was first tested on the well-known MCYT-100 and SUSIG data sets. The results show that the performance of the proposed technique is comparable and often superior to state-of-the-art algorithms despite its simplicity and efficiency. In order to test the proposed method on finger drawn signatures on touch devices, a data set was collected from an uncontrolled environment and over multiple sessions. Experimental results on this data set confirm the effectiveness of the proposed algorithm in mobile settings. The results demonstrate the problem of within-user variation of signatures across multiple sessions and the effectiveness of cross session training strategies to alleviate these problems.

Zimmer 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.

Systems using digital tablets seem more practical than those based on cameras; however, they are expensive and require more dedicated material for the exploitation of acquired data. Other types of acquisition systems based on a data glove (conceived initially for virtual reality) have also been developed for the same purpose. The latter are powerful, but very constraining and not suitable fora general public use. It would also be possible to have a system in which the user signs with an ink-less pen, leaving no trace of the signature in order to prevent possible forgers from knowing it. The article shows it is possible to have a system in which the user signs with his hand, leaving no trace of the signature in order to prevent possible forgery. Indeed ,by regarding the signature as a specific dynamic hand activity and not as the result of this activity on paper or digital support, we have been able to propose a new online signature acquisition device allowing the construction of low-cost and non constraining signature authentication systems.

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 given on the large MCYT signature database (330 signers, 16500 signatures) for random and skilled forgeries. Feature selection experiments based on feature ranking are carried out. It is shown experimentally that the machine expert based on local information outperforms the system based on global analysis when enough training data is available. Conversely, it is found that global analysis is more appropriate in the case of small training set size. The two proposed systems are also shown to give complementary recognition information which is successfully exploited using decision-level score fusion.

Global analysis is based ona novel feature-based description of signatures and non-parametric statistical modeling based on Parzen windows. Local analysis relies on a function-based approach and parametric statistical modeling through Hidden Markov Models. The machine expert based on global information is shown to outperform the system based on local analysis in the case of small training set size and user-independent thresholds. It has been also found to be quite robust to the severe user-dependencies encountered in signature.

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. The resulting system performs reasonably well with an overall error rate of 3:3% being reported for the best case. In order to learn the signature verification system to distinguish between genuine signatures and forgeries, we must provide it with samples of the two types. Many authors used the parametric approach to incorporate the usage of neural networks for the verification of online signatures. Several static and dynamic features are extracted and used to train the neural network. Several Network topologies are tested and their accuracy is compared. First, cluster analysis is applied to segment the feature space into sub-regions of "similar" signatures to facilitate the classification and verification tasks. Then, a two-layer sigmoidal perception was used to approximate the classification function. The authors also applied an adaptive radial-basis network called the RCE network. Finally, the two networks are 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.

Hidden Markov Models (HMM) were introduced in the pattern recognition field as a robust method to model the variability of discrete time random signals where time or context information is available. HMMs are widely used in classification of input patterns and they have a great ability to model stroke-based sequences. These models have found to be well suited for signature modeling since they are highly adaptable to personal variability. The underlying assumption of the HMM is that the signal can be well characterized as a parametric random process, and that the parameters of the stochastic process can be estimated in a precise, well-define manner. In HMM, the probability of moving from one state to another depends on both the transition probabilities and the previously visited states. The left -to-right topology is the most applicable in DSV systems since it is considered well suited for signature modeling. some of the techniques that used Ergodic topology found in compared between different topologies used for DSV and reported that the worst results were obtained using Ergodic or generalized models, in which transitions between all the states are allowed. An algorithm such as Viterbi algorithm can be combined with HMMs to find the most likely state sequence that generates the observed sequence. Other algorithms such as the Baum-Welch or the Segmental K-means can be used to update the parameters of the model to maximize the probability of the sequence generated by the model.

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.

The handwritten signature is a biometric attribute. Biometric identification and verification systems are being and relatively expensive hardware to capture the image. An important advantage of the signature over other biometric attributes is its long standing tradition in many commonly encountered verification tasks. It has been used for decades in civilian applications while other methods . Signature verification is already accepted by the general public. While we are unaware of any studies that show that an individual's signature is unique, itis generally accepted that this is the case. Signatures are easier to forge than other biometric attributes. While attributes like iris, retina and fingerprints do not change over time and thus have low intra-class variation, they require special the dynamics of writing are also captured in on-line signatures, which is not present in the 2-D representation of the signature and hence it is difficult to forge. Automatic signature verification can be used in all applications where handwritten signatures are currently collected such as cashing a check, signing a credit card transaction or authenticating a legal document. The ability to capture the signature and have it immediately available in a digital form for verification also opens up a range of new application areas. The system implemented here uses a digitizing tablet (IBM Cross Pad) from the A.T. Cross company as the data capturing device. The IBM Cross Pad has a sampling rate of 100–150 samples per second and records the x- and y-coordinates of the points in the signature. The pen has a touch sensitive switch in its tip such that only pen-down samples (i.e., when the pen touches the paper) are recorded .Evaluating a verification system requires the analysis of two types of errors. The percentage of genuine signatures that are incorrectly rejected by the system is called the false reject rate or type I error. The percentage of incorrectly accepted forgeries is called the false accept rate or type II error. The two types of errors usually have different costs associated with them depending on the security requirements of the application. The performance of a system is often measured by its equal error rate, which is the point where the false accept rate and the false reject rate are the same. .

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). We have used a database of 330 users which includes 25 skilled forgeries performed by five different impostors. This database is larger than the typical ones found in the literature. Experimental results reveal that the first proposed combination of VQ and DTW (by means of score fusion) outperforms the other algorithms (DTW, HMM) and achieves a minimum detection cost function (DCF) value equal to 1.37% for random forgeries and 5.42%for skilled forgeries.

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. These 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. We have checked that they yield worse results than a more complex system such as DTW, which takes into account the temporal evolution of the signature signal. However, they provide quite good results for themselves, and that can help to improve privacy and recognition accuracy in our novel proposed scheme. In addition, an another combination scheme, named DTW(VQ) which enables improvement of privacy for remote authentication systems, avoiding the submission of the whole original dynamical signature information is proposed. This system achieves similar performance than DTW when using codes system achieves similar performance than DTW

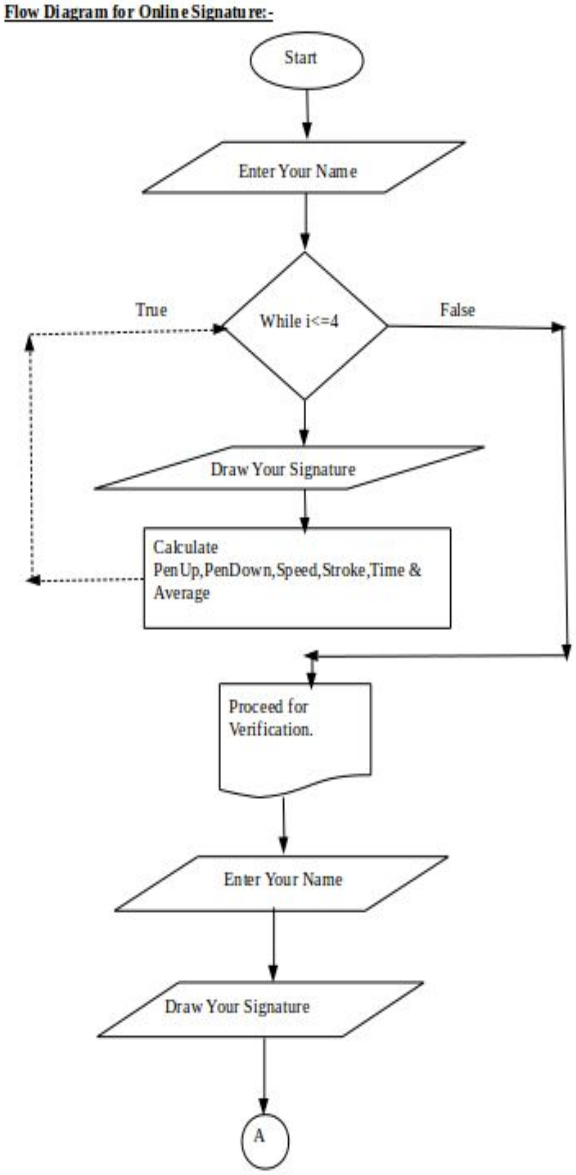
Luan L. Lee et al [8] proposed line dynamic signature verification systems A data base of more than 10,000 signatures in (I, y(t))-form was acquired using a graphics tablet. We extracted a 42-parameter feature set at first, and advanced to a set of 49 normalized features that tolerate inconsistencies in genuine signatures while retaining the power to discriminate against forgeries. An algorithm for selecting and perhaps orthogonalizing features in accordance with the availability of training data and the level of system complexity is proposed. For decision making we studied several classifiers types. A modified version of our majority classifier yielded 2.5% equal error rate and, more importantly, an asymptotic performance of 7% false acceptance rate at zero false rejection rate, was robust to the speed of genuine signatures, and used only 15 parameter features.

In correspondence an approach to design ingrediable and effective on-line signature verification which includes: construction of a reliable data base, selection of optimum feature sets with or without forgery data available, finding classifier independent feature selection procedures, obtaining reliable asymptotic global and individual performance, obtaining a suitable statistical model for signatures, minimizing the effects both of the inconsistency of genuine signatures and of the variety of forgeries, and adapting to practical limitations such as on-line response and limited memory size is proposed. We introduce new techniques for on-line human signature verification that are responsive to all these issues and yield performance satisfactory for point-of-sale (RX) applications.

III. PROPOSED APPROACH

In proposed system first of all we will calculate number of parameters associated with the signature. This parameters include number of penup that is number of times the pen has up. Similarly number of pen down that is the number of times the pen has down. Others parameter include speed that is the speed of signature. Time will also be considered that is time in seconds require to draw the signature. Based on all this parameter we will make some templates and store in the database. In proposed system we will be storing four templates. Each templates having its own sets of parameter that is penup, pendown, speed, stroke and time. Based on this parameter the final signature will be compared whether that signature is belong to actual person or not. Final signature will be considered as genuine if it gets matched with some of the defined parameters of each template else the signature will get rejected. Additionally to increase the security the name of the person will be stored in database in encrypted form. Name of the person is stored along with all different parameters in database. Main aim to store the name in unreadable format is that if somebody succeeded to get access to database he will not be able to disclose the name of the person to whom the signature belongs. This is how the proposed system will work.Following points shows how this application works:-

1.User require to enter the name in the application.
2. User need to enter the signature four times so that it will be act as template.
3. Finally user enter his signature that will be compared with the templates.


Flow Diagram for Online Signature:-
Start
Enter Your Name
True
While i<=4
False
Draw Your Signature
Calculate PenUp,PenDown,Speed,Stroke,Time & Average
Proceed for Verification.
Enter Your Name
Draw Your Signature
A

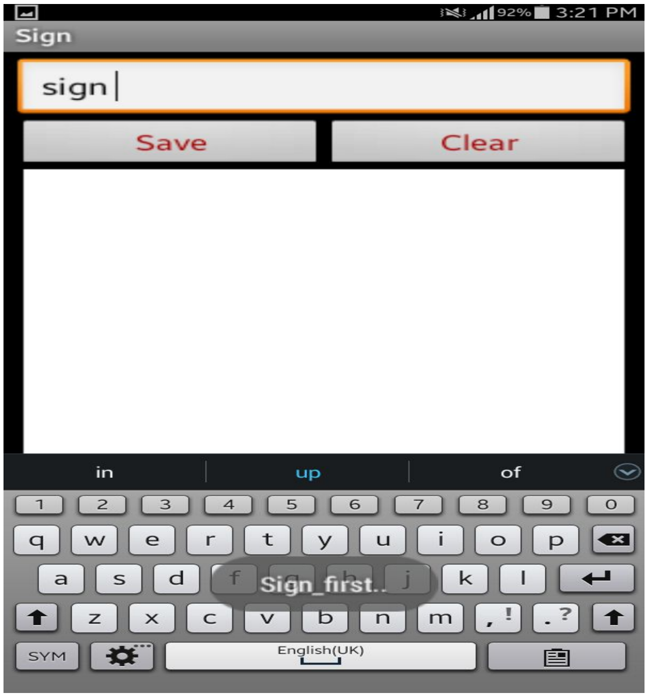


Fig 2: Signature Screen

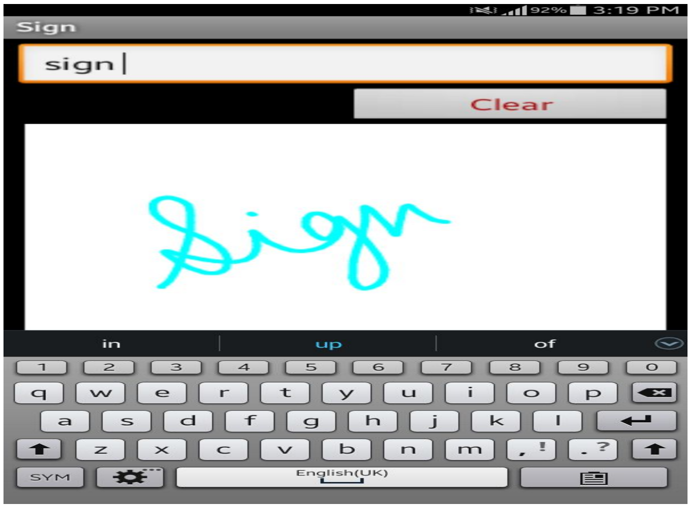
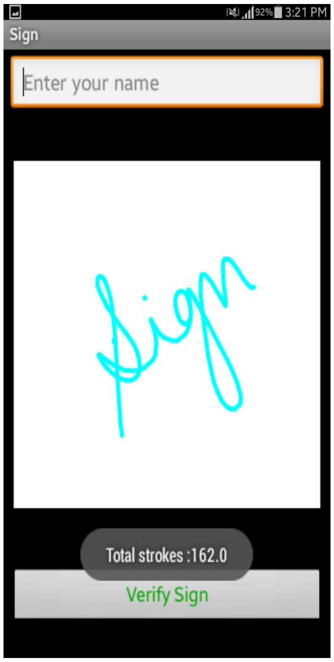
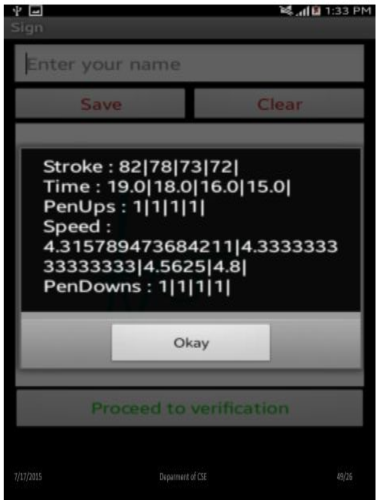


Fig 3: sign and name



Total strokes :162.0

Fig 4: Total strokes Calculation



```
Stroke : 82|78|73|72|
Time : 19.0|18.0|16.0|15.0|
PenUps : 1|1|1|1|
Speed :
4.315789473684211|4.3333333
33333333|4.5625|4.8|
PenDowns : 1|1|1|1|
```

Fig 5: Calculation of all the parameters

IV. CONCLUSION AND FUTURE WORK

This paper proposes a simple and effective online signature verification system that is suitable for user authentication on a mobile device. The benefits of the proposed algorithm are as follows. First, a histogram based feature set for representing an online signature can be derived in linear time and the system requires a small and fixed-size space to store the signature template. In addition, since the feature set represents only statistics about distribution of original online signature attributes, the transformation is non-invertible. As a result, the privacy of the original biometric data is well-protected. Second, a user-specific classifier comprising of a user-specific quantization step size vector and its associated quantized feature vector can be trained using only enrollment samples from that user without requiring a training set from a large number of users. One interesting area for future work is the design of an enrollment protocol that can capture a intra-user variation effectively within a single session. In addition, it is currently possible to match different signature templates generated from the same online signature samples and thereby learn that two leaked biometric templates belong to the same user. Further investigation includes the use of other biometric key binding approaches, like fuzzy commitment, in order to strengthen security of the system, even when stored templates, helper data etc., are compromised, while preserving verification performance. Lastly, it is possible to derive a fusion approach by combining the proposed method with other existing approaches, e.g., DTW, HMM-based, etc., in order to improve verification performance, especially for applications where privacy of the signature traits is less critical.

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*