IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 82-89
www.iosrjournals.org

Biometric Online Signature Verification

Fincy Francis1, Aparna M.S, Anitta Vincent
[1,2,3]*(Embedded System, Sahrdaya College of Engineering and Technology, India)*

ABSTRACT: *Person identification can be done precisely by Biometrical method, where physiological or behavioral characteristics are used for this purpose. Handwritten signature is a behavioral trait it can be used for person identification accurately. There are two types of identification modes either online or offline mode. Which depends upon the signature acquisition method. In offline acquisition method the shape of the signature is used for authenticating signer. While in online signature verification uses dynamic characters that is dynamic time dependent of the signature to authenticate the signer. This paper describes the implementation on field programmable gate arrays (FPGAs) of an embedded system for online signature verification. The online signature recognition algorithm mainly consists of three stages. Initial pre-processing is the first stage which is applied on the captured signature for removing noise and normalizing information related to horizontal and vertical positions. Dynamic time warping algorithm is used to align this processed signature with its template previously stored in a database. Finally, a set of features is extracted and passed through a Gaussian Mixture Model. Degree of similarity between both signatures can be find out from this. For fast computation of floating point calculations vector floating point unit is used (VFPU). Additionally system consists of a microprocessor which interacts with the VFPU. All the procedures of verification can be done in software. Furthermore this paper studies about 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.*

Keywords*- Biometrics, embedded systems, field-programmable gate arrays (FPGAs), handwritten recognition, online signature verification.*

I. INTRODUCTION

In everyday life there are many places where we are needed to give person’s identification to gain access. Its examples include internet account, credit cards, ATM, etc. We have to first provide our identification and then we can access them.

Biometrics refers to a field of study that is concerned with any characteristic or personal trait that can be used to identify or verify a person. The characteristics include face, fingerprints, hand geometry, iris, handwriting, retina, voice, dental record, DNA and signature. The more distinctive feature for a characteristic selection is, it should be time independent and unique one. Signatures can be considered as a special class of handwriting but there may not be consists of legible letters or words**.** Hand written signature verification is a legally and socially accepted scheme for authenticating an individual. So it is used to provide a secure way for authentication, and authorization in legal, banking or other high security environments.

Typically, 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 applied while putting a signature, time required for signature completion, etc., are also acquired. These dynamic features give the interclass variability between genuine and impostor signatures. As a result, an online signature verification system usually achieves better accuracy than an off-line system.

There have been many developments on personal computing devices in the past few years. they are come equipped with a touch sensitive interface .Thus entering a password on such devices is much difficulty which lead to an interest in developing alternative authentication mechanisms on them [7]. This paper mainly deals with the discussion for design of an embedded system for biometric online signature verification and the usage in mobile devices. Paper title (11italic)
www.iosrjournals.org 2 | Page

1.1 Previous work

Since then, many researchers have proposed different techniques for online signature verification

1.1.1 Feature selection: There are mainly three direct approaches for the selection of features. One is based on point to point local feature comparison, relating position, acceleration, pressure etc.[6]. The second one deals with the global features like writing time pen up time, maximum/minimum pressure, number of breakpoints and speed, pen pressure at crucial points like starting and final points. In the third case the shape of the signature is verified. There are different techniques using local features in signature verification. The most commonly used methods are matching by dynamic time warping and by using Hidden Markov Model.

1.1.2 Signature verification techniques: Generally Signature verification techniques classified into three template, statistical and structural matching .Template matching techniques is dynamic time warping (DTW) algorithm. Neural networks (NN), hidden Markov models (HMM)[3] or Gaussian mixture models (GMM)[4] are examples of statistical matching. Structural matching system architecture contains a single coprocessor, which accelerates all floating-point computations involved in the whole signature verification algorithm.

II. ONLINE SIGNATURE VERIFICATION ALGORITHM

The system uses the digitized form of a signature of an individual but the signature is acquired in real time. The acquisition process can be carried out by means of stylus operated PDAs. The most peculiar dynamic information we have to collect include information like position in x-axis, position in y-axis, pressure applied by the pen, angle of the pen with respect to the tablet. Using this set of dynamic data, further information can be found, such as velocity, instantaneous trajectory angle, acceleration, tangential acceleration, instantaneous displacement, etc. The prime use of dynamic features is it harder to forge. Even if a skilled forger is able to copy the shape of the signature, it is very unlikely that he can simultaneously reproduce all the dynamic features as well.

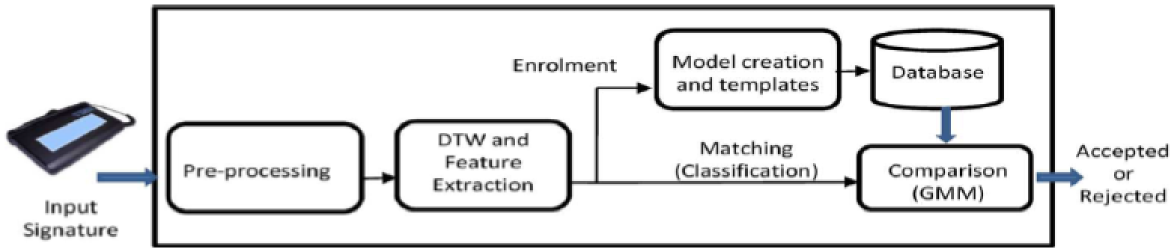

Fig. 1: General architecture of online signature verification system

2.1. Signature Acquisition

Signature acquisition process can performed by electronic devices such as pen tablets (i.e.,WacomIntuos 2), touch- screens or PDAs.[5] . Stroke of the signature refers spatial information represented by the horizontal and vertical pen position. To retrieve online data, pressure sensitive tablet can be used and signal conditioning element can extract the pressure distribution characteristics of the written signature.

2.2. Pre-processing

Signature normalization is achieved through Preprocessing. Which reduces noise and normalize the signature stroke. It creates the link between real world data and recognition & verification system. The preprocessing stage is carried out by following steps:

Filtering: Signals acquired by the electronic device are smoothed by applying a low-pass filter that reduces

noise introduced in the capturing process.

Equally-spacing: The average signals are transformed to an equally-spaced 256-point temporal sequence by using a linear interpolation.

Location and time normalization: The x-axis and y-axis temporal functions are normalized by centering the origin of coordinates at the signature center of mass with a specific rotation.

Size normalization: The x and y strokes of the signature are normalized by using the norm of the 2 dimension vector [x,y] . Normalization process can be done by using the following equation

$$Xi = \frac{xi' - x\min}{x\max - x\ min} X\ M \qquad Yi = \frac{yi' - y\min}{y\max - y\ min} X\ M$$

In these equations: Xi, Yi- pixel coordinates for the normalized signature, xi,’ yi ‘- - pixel coordinates for the original signature, M- one of the dimensions (width or height) for the normalized signature

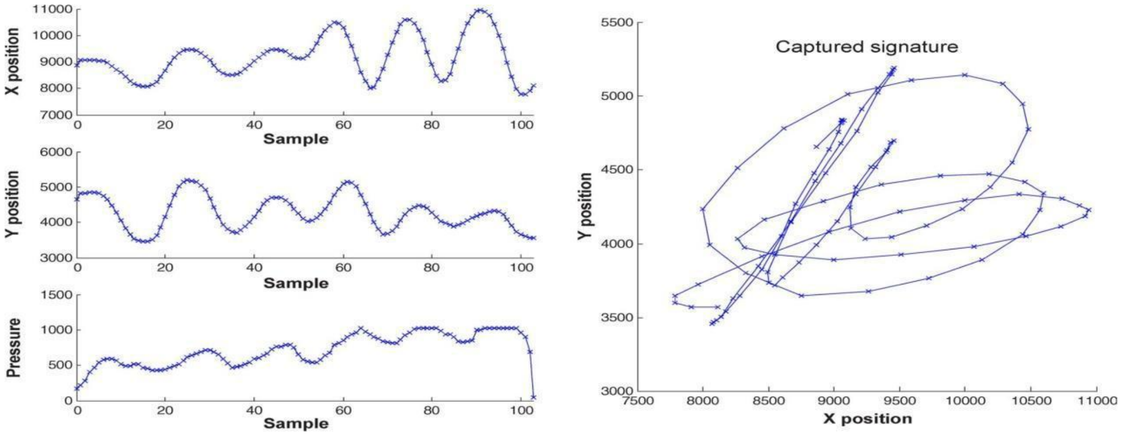

Fig. 2. Representation of signature captured by a commercial device.

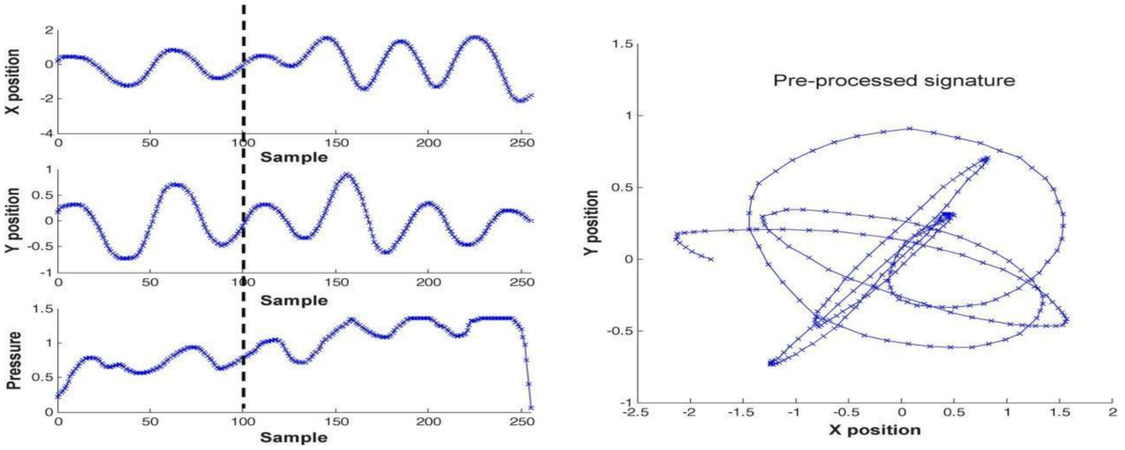

Fig.. 3 Captured signature after applying the pre-processing stage.

Conversion from Color Image to Gray Scale Image: A color image consists of a coordinate matrix and three color matrices. Coordinate matrix contains X, Y coordinate values of the image. The color matrices are labelled as red (R), green (G), and blue (B). The scanned or captured color images are initially converted to grey scale using the following equation Gray color = 0.299*Red + 0.5876*Green +0.114*Blue

Background Elimination: To separate an objects from the image background ‘thresholding’ is used. Thresholding is choosing a threshold value H (brightness threshold)and assigning 0 to the pixels with values smaller than or equal to H and 1 to those with values greater than H .

If f(x, y) ≥ H then

f(x, y) = Background

else f(x, y) = Object

2.3 Dynamic time warping (DTW)

A DTW algorithm is used to align the captured signature with its template. After making proper alignment, a set of features are extracted which is given as input for a GMM matcher .Expectation-maximization (EM) algorithm is used to obtain a model for GMM matcher.

2.3.1 Signatures are characterized as a sequence of bidimensional points that represent the horizontal x and vertical y pen position:

S=s1,s2,…..sj…..sN ;with sj=(sx[j],sy[j]), T=t1,t2,…..ti……tN; with ti=(tx[i],ty[i]) , i , j € [1: N]

where S and T denote the captured and template signatures to be aligned, respectively.

2.3.2. From these two sequences a distance matrix C € R^{NXN} built.

C(ti,sj)$= \sqrt{(tx[i]-sx[j])^2+(ty[i]-sy[j])^2)}$; i ,j € [1,N]

2.3.3. The warping path P, which is built starting from matrix C, is defined as any sequence of points P=(p1,p2,p3…pk) with pm=C(ti,sj), m €[1:k],p1=C(t1,s1) and pk=C(tN,sN) . Cost function related to warping path P

DP(T,S)$= \sum_{m-1}^{k} Pm$

2.3.4 The optimal warping path P0 is defined as the warping path which has a minimal cost function

P0=P|D0(T,S)=min{Dp(T,S)}

As Fig 4. shows, time misalignment between signatures is represented by small deviations of the optimal warping path from the diagonal line.

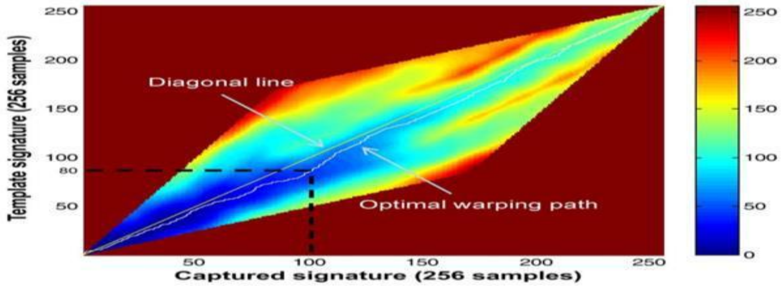

Fig.4 represents the position (x and y) and pressure of both signatures on the same graphic.

2. 4.Gaussian Mixture Model

2.4.1 GMM Model representation:

This probability is defined by a weighted sum of Gaussian probabilistic density functions as where are the weighted coefficients, M represents the number of Gaussians and is the particular density function for each multivariable Gaussian function:

Nc
(N$\bar{X} = \frac{\exp(-0.5(\bar{x}-\bar{\mu}i)T \sum_{i}^{-1}(\bar{x}-\bar{\mu}i)}{(\pi 2)^{L/2}\sqrt{||\Sigma i||}}$

bi( )

In this case M is set at 3 and refers to the feature vector of length L. Along with the weighting factors , the user'smodel is represented by µi and , which refer to the mean vector and the covariance matrix of the template signature, respectively. These parameters are calculated by using a set of training signatures and their derived feature vectors. The expectation-maximization (EM) algorithm was used for this purpose[5].

2.4.2 Feature Extraction: An efficient feature extraction algorithm should require two characteristics: Invariance and reconstruct-ability .The feature vector is used as input of the GMM model.

Regression formula

Reg (zj(t),µ)= $\sum_{K=1}^{\mu}(k(zj(t,k) - zj(t-k))_{/2}\sum_{k=1}^{\mu}(k^2)$, jƐ[1,W]

III. VECTOR FLOATING-POINT UNIT ARCHITECTURE

3.1. Main features of VFPU

The main features of VFPU can be summarized as follows.

- The internal architecture of the VFPU is designed to optimize computations, which are defined as a set of basic floating-point operations. In this way, these computations can be performed avoiding additional accesses to external memory.
- The VFPU executes computations on scalar numbers or vectors of arbitrary length using operands of single precision defined by the standard IEEE-754.
- Computations can be performed with vectors stored in external memory, scalar numbers provided by the microprocessor or any combination of them. Likewise, the result of any operation can be placed on external memory or read by the microprocessor.

3.2. Internal architecture of the VFPU

The internal architecture of the VFPU, which is divided in 5 blocks: FIFO memory, bus interface, register file, control unit and FPU. The role of FIFO memory is acting as connection with the memory controller for managing the reading and writing of data vectors in external RAM. The elements of these vectors are temporarily stored in the FIFO memory as input operands which could be subsequently used by the FPU. Likewise, this memory can also store any result that should be transferred to external memory. The bus interface carries out a similar role as the FIFO memory, but in this case managing the reading and writing of scalar numbers between the VFPU and the microprocessor.

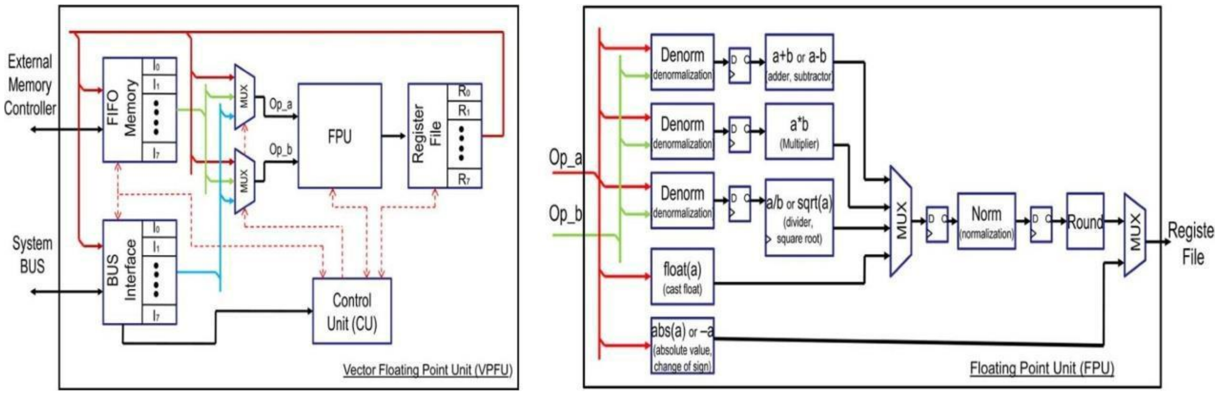

Fig.5 Architecture description for both VFPU (left) and FPU (right)

The register file consists of eight 32-bits registers that store the result provided by any operation performed by the FPU. These registers can also be used as operands in subsequent operations. Two multiplexors, which are managed by the control unit, select the proper operands of the FPU from the register file, the FIFO memory or the bus interface. Thus, the VFPU is able to carry out operations using any combination of vectors or scalar numbers. Additionally, the VFPU is arranged with a control unit that is configurable at run-time. This configuration allows the VFPU to be adapted to any of the stages involved in the algorithm to accelerate the execution time. The FPU performs the following basic operations: addition, subtraction, multiplication, square root, division, absolute value and negative sign, casting from integer to float.

IV. IMPLEMENTATION ON FPGA

Here we are going to implement an embedded online signature verification system on a low-cost FPGA. The system architecture contains a single coprocessor, which accelerates all floating-point computations involved in the whole signature verification algorithm. The coprocessor represents a vector floating-point unit (VFPU), which can be configured at run-time for resolving specific blocks of operations that use as input operands vectors of variable length.

The complete embedded system was implemented on a XC3S2000 low-cost Spartan 3 FPGA of Xilinx operating at 40 MHz. The system architecture consists of a Microblaze microprocessor, a soft-core developed by Xilinx suitable for designing embedded systems. The VFPU is connected to the Microblaze through the system bus available for this purpose. Data and program are stored in a 2MB SRAM external memory. A memory controller (MC) drives the SRAM and provides access from the microprocessor and the VFPU. Besides, other peripherals such as timers, UARTs, input-output ports, etc., are also implemented as part of the embedded system.

V. ONLINE SIGNATURE VERIFICATION ON MOBILE DEVICES

Fig. 6. An example of finger drawn signatures on mobile devices

Here proposes a simple and effective online signature verification system that is suitable for user authentication on a mobile device. The advantage 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. Moreover privacy of the original biometric data is well-protected, because feature set represents only statistics about distribution of original online signature attributes. Furthermore, it consists of a user-specific classifier comprising of a user-specific quantization step size vector and its associated quantized feature vector can be trained using only enrolment samples from that user without requiring a training set from a large number of users. Template updating mechanism is needed in order to stabilize the performance because there may chance of lower the verification performance while comparing the older the training samples with the test samples[2].

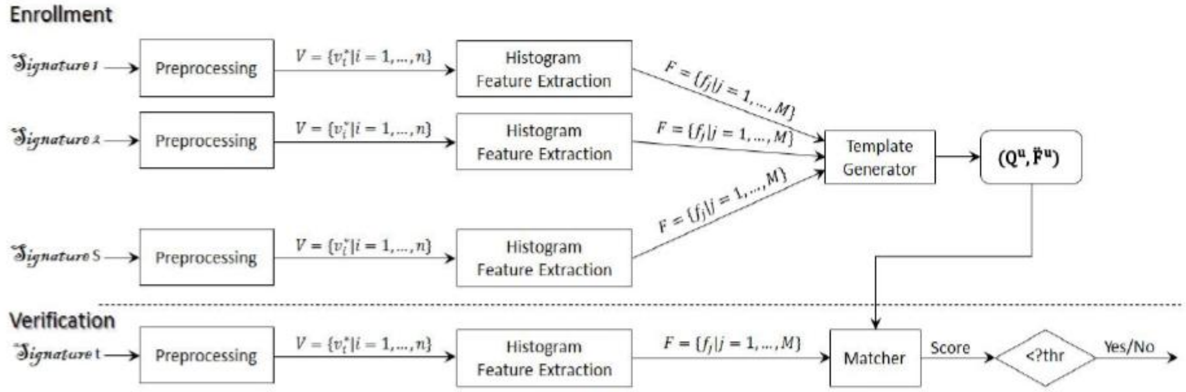

Fig. 7. The proposed online signature verification system.

VI. EXPERIMENTAL RESULTS

The accuracy of the proposed signature verification algorithm was tested on the MCyT database, which includes 100 users and contains 25 genuine signatures and 25 skilled forgeries for each one. The algorithm performance is evaluated by means of the detection error trade off (DET) curve. The false non match

rate (FNMR) and the false match rate (FMR) are used for calculating performance of the system. The best Equal Error Rate (ERR) ,the parameter usually used for determining the quality of a biometric algorithm is 2.74%, which is a good result for most signature verification systems[1].

To prove the speed and the performance of this VFPU, the signature verification algorithm was executed on two additional systems: an ARM Cortex-A8 microprocessor clocked at 720 MHz and the Microblaze microprocessor configured with its own FPU provided by Xilinx. The results obtained with these systems serve as reference pattern to find out the real performance of the proposed VFPU.

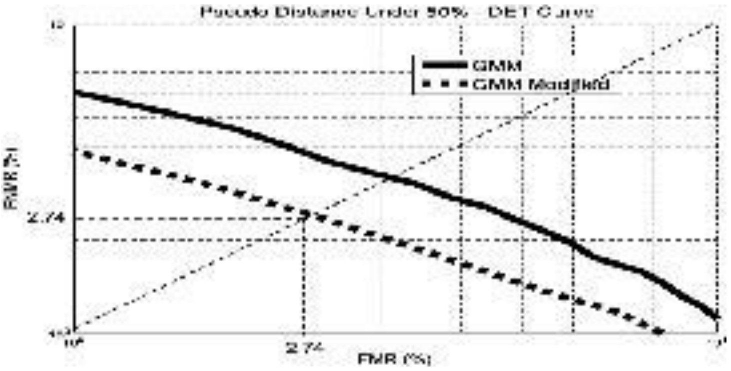

Fig 8 :DET curves obtained using the MCyT database

VII. CONCLUSION

A reliable signature verification system is an important part of law enforcement, security control and in many business processes like for cheques**,** contracts, certificates, etc. The main objective of this work is to present a robust system for on-line signature verification.

This paper describes a complete biometric algorithm for signature verification based on three stages. Signature is normalized by means of a pre-processing. Later, the captured signature is aligned with its template by applying a DTW algorithm. From this aligned signature the most relevant features are extracted and used as input to a GMM model, whose output is used to confirm or deny the user’s identity. This paper also showed the design of an embedded system for implementing this signature

Verification algorithm for online signature in a low-cost FPGA is implemented. The VFPU is accomplished of executing multiple operations in parallel using vectors of any length as operands. Additionally, it reduces the number of accesses to program memory. The performance of the VFPU was compared with those performances offered by the FPU provided by Xilinx and with an ARM Cortex-A8 microprocessor. The verification algorithm was executed on these three systems, indicating that the VFPU offers the best performance. Furthermore online signature verification for the mobile devices are also discussed.

One interesting area for future work is the design of an enrolment protocol that can capture a skilled forgery effectively within a single session. Further investigation includes the use of other biometric key binding approaches, like fuzzy commitment, in order to strengthen security of the system. Finally, 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 authentication performance, particularly for applications where confidentiality of the signature is more.

REFERENCES

Journal Papers:

[1] Mariano López-García, Rafael Ramos-Lara, Oscar Miguel-Hurtado, and Enrique Cantó-Navarro, Embedded System for Biometric Online Signature Verification , IEEE Transactions On Industrial Informatics, Vol. 10, No. 1, February 2014.

[2] Napa Sae-Bae and Nasir Memon,Online Signature Verification on Mobile Devices, IEEE Transactions On Information Forensics And Security, Vol. 9, No. 6, June 2014

[3] Bao ly van, sonia garcia-salicetti, and bernadette dorizzi, On using the viterbi path along with HMM likelihood information for online signature verification, IEEE transactions on systems, man,and cybernetics part b: cybernetics, VOL. 37, no. 5, october 2007

[4] Cheng-lin liu, stefan jaeger, and masaki nakagawa, Online recognition of chinese characters: the state-of-the-art, IEEE Transactions on pattern analysis and machine intelligence, VOL. 26, no. 2, february 2004

[5] D.S. Guru and H.N. Prakash ,Online signature verification and recognition: an approach based on symbolic representation, IEEE transactions on pattern analysis and machine intelligence, VOL. 31, no. 6, june 2009

[6] Musa mailah1 & lim boon Han ,Biometric signature verification using pen position, time, velocity and pressure parameters, Jurnal Teknologi, 48(A) Jun 2008: 35 - 54

[7] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon,,Biometric-rich gestures: A novel approach to authentication on multi-touch devices,in Proc. CHI, 2012, pp. 977–986.