A Novel Signature Verification Based Automatic Teller Machine

Akash choubey, Amarjot Singh, Srikrishna Karanam, Devinder Kumar, and Ketan Bacchuwar

***Abstract*—Biometric identification is the need of hour and automatic recognition systems are such biometric techniques to look upon. Accurate automatic recognition systems are important for a wide range of applications such as banks, restricted areas, government classified areas etc. As traditional identity recognition methods such as pins, passwords etc suffer from some fattle flaws and are unable to satisfy the security requirements. The paper introduces a novel system, a combination of behavioral traits as well as traditional methods for identity recognition. The system uses signature verification as the behavioral trait along with an unique identity number (referred as UIN in rest of paper) for the recognition. Signature verification is an important domain for confirming a person's identity. The system is applied of an ATM (Automatic Teller Machine) to decrease the risk of theft from an individual's account. It can be effectively employed to reduce the risk of forgery by releasing the trouble of carrying ATM cards by the users, by employing a signature verification system fused with an unique identity number. The paper further presents a comparison of three extremely efficient methods CDTW (Continuous Dynamic Time Warping), DTW (Dynamic Time Wraping) and HMM (Hidden Markov Model) employed for signature verification and the best method was stated.**

***Index Terms*—Continuous dynamic time wraping, dynamic time wraping, hidden markov model, automatic teller machine, unique identity number.**

I. Introduction

Biometrics is the need of the hour as it is heavily required for security in many critical scenario's like banks, ATM's, credit card transactions etc. ATM has become very popular among people all around the world. This is due to its easy to carry part, usage as plastic money and any time operational which is not in case of banks. Recent advancements in the field of biometrics have outreached human's performance in knowing an individual's identity. Biometrics is mainly divided into two groups: physiological and behavioral biometrics.

Physiological traits are related to the shape of the body like face, finger print etc while behavioral are related to the behavior of the person. Many methods have been applied for physiological model like speech recognition, face detection but major flaws have been observed in the methodologies along with a lot of computational cost.

ATM's high popularity is justifiable due to these ease and mobility to avail mobile money. But still in this modern world of sophistication, a person finds it difficult to take care of such a plastic card which may get damaged in one or the other way. Even its magnetic strip may get damaged easily making ATM useless. So the aim of this paper is to create an environment free from carrying ATM. The system has a double security level which makes it very difficult to breach. Firstly, the UIN provided to the user is confidential and secondly, the signature verification which increases its security level to a very high grade. Thus this system stands over the current ATM system in two major ways- firstly the user is relaxed from carrying and taking care of his ATM card. Thus this is user friendly system. Secondly, it increases the security level by a much higher level due to double layer security counter.

In order to overcome these disadvantages, signature verification as behavioral models has been used. Signatures are composed of special characters and flourishes therefore most of the time they can be unreadable. Also intrapersonal variations and interpersonal differences make it necessary to analyze them as complete images and not as letters and words put together [1]. As signatures are the primary mechanism both for authentication and authorization in legal transactions, the need for research in efficient auto-mated solutions for signature recognition and verification has increased in recent years.

Signature verification can be further classified into online and offline signature verification. In online signature verification, a computer tablet with a pressure pen, stores the dynamic information which can be further used for identification while offline signature verification deals with static image of signature which is scanned and can be further used for verification.

A number of pattern recognition methods in past have been used for signature verification like SVM, vector quantization, neural network, HMM, DTW etc. It has been observed that most of the methods perform well in their domain. This paper compares the capabilities of DTW with CDTW and further with HMM's. DTW has been previously used for on-line signature verification. In this method, the user's signature is sampled at time interval with respect to the edge points and stored. Then, a distance matrix is created with which stores the data of distance between template signature's points and points of the signature done on-line. Then minimum distance between two curves is calculated and signatures can be compared while another famous method CDTW (Continuous Dynamic time warping) uses a little bit different approach from DTW but has far better results. This method samples not only at edge points but also at intermediate points giving more accurate results than DTW. Further, the paper computes

Manuscript received April 25, 2012; revised June 1, 2012.

Akash Choubey, Amarjot Singh, Devinder Kumar, Ketan Bacchuwar are with the Electrical Department of National Institute of Technology, Warangal, India (e-mail: amarjotsingh@ieee.org).

Srikrishna Karanam, is with the Electronics and Communication Department of National Institute of Technology, Warangal, India.

the results for hidden markov model which computes the result on models working on observation sequences.

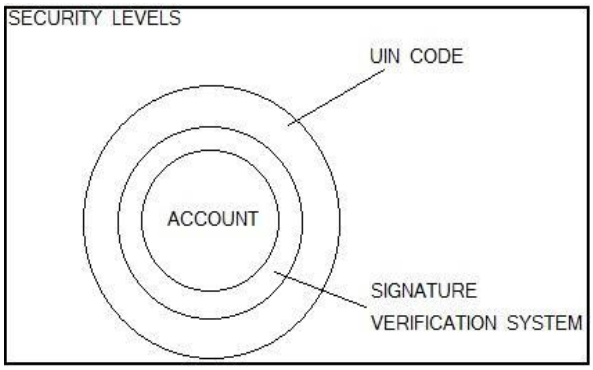


Fig. 1. Proposed ATM model.

DIVISION IN AAAAA,			
AAAAA	TRANSVERSAL IS ROW WISE (if previous level is cleared)		
	Numerical Code 1	Signature verification of 1	ACCOUNT 1
	Numerical Code 2	Signature verification of 2	ACCOUNT 2
	Numerical Code 3	Signature verification of 3	ACCOUNT 3

Fig. 2. Database structure showing numeric code, signature verification and finally access to account.

The paper is further divided into following sections. Next section explains the related work on the identification methodologies specified to signatures. Third section explains our modified automatic teller machine while section four explains the methodologies used in the paper for signature verification. Finally section five and six elaborates the result and conclusion for the simulations.

II. Related Work

In order to achieve successful signature verification, the problem of combining disparate forms of signature information, including both continuous and discrete features, and parametric and signal-based methods of signature representation [2] must be addressed [3]. The combination of different sources of information about a signature, in the form of different feature sets and classification methods, provides an opportunity to develop an improved level of verification compared to the use of a single set of descriptors[4], [5]. Online signature verification methods vary in classification methods, preprocessing and feature selection. A number of classification methods have been discussed in [6]. The methods focus on differentiation of sine and cosine angle values with respect to consecutive points in *x* and *y* plane followed by grey values in adjoining pixels. Focusing on the classification methodology, different approaches can be found to measure the similarity between test signature and signer model. Dynamic time warping [6] and hidden Markov model (HMM) [2] are widely used for signature verification. Vector quantization (VQ) [3] pattern recognition algorithm has also been tested [3] in this field. Dynamic time warping [1], [7] and hidden Markov model(HMM)[2] are two of the most widely used approaches followed by Vector quantization(VQ) In the Signature Verification Competition 2004 (SVC04), DTW and HMM based systems were shown to be the most competitive algorithms.

III. Proposed Automatic Teller Machine

The proposed system is a combination of a number of security levels which needs to be traversed in order to access the account as shown in Fig. 1. In order to access the account the user is supposed to enter the unique identity number given by the bank to the user. Once the number is identified, the user enters into security level one. In order to traverse the second level and access the account, the user has to get identified by the signature verification security layer. Once the signature has been verified the account can be accessed. The system is elaborated in detail below:

A. UIN (Unique Identity Number)

The unique identity number or UNI is a combination of 5 letters and 5 numbers, making it a ten digit code. Both of the letter and numerical part have their equal importance. The first part of the code is the first five alphabets of user's name or last five letters of his name, provided by the bank to the user. It will be decided by the bank to use first five letters of first name or last name depending on the criteria so that data base is equally divided and is not burdened over the same place. Thus the database will be arranged on letters making it easy to handle and retrieve data from the data base. The benefit of this system is that the user won't forget his user name as it's a part of his name and that it makes the information retrieval much easier. The data base will be arranged in order of A to Z. This algorithm arranges the user name in as similar way to that of DICTIONARY. All accounts are arranges in ascending order of alphabets for easy retrieval of data.

The second part of the code is a five digit combination. These digits will be provided by the bank to the users. These will be randomly generated digits similar to the PIN (Personal Identification Number) provided presently. These digits will be known only to the user and will be used for accessing his account.

B. Signature Verification Layer

The signature verification layer is the innermost layer of the system. Once the person successfully enters the outer UNI layer, the person has to traverse the inner layer utilizing a novel signature verification system. Once the signatures of the user are matched with the signature present in the database corresponding to the UNI, the user is given access to the account as shown in Fig. 2.

IV. Algorithms

The paper mainly discusses three algorithms employed to discuss and compare their performance. The algorithms mainly are DTW, CDTW and HMM. The algorithms are explained in detail below.

```
n ← |X|
m ← |Y|
d[] ← new[n × m]
d(0,0) ← 0
for i=1;i ≤ n;j++ do
    d(i,1) ← d(i-1,1)+c(i,1)
end for
for j=1;j ≤ m;j++ do
d(1,j) ← d(1,j-1)+c(1,j)
end for
for i=1;i ≤ n;j++ do
   for j=1;j ≤ m;j++ do
       d(i,j) ← s(i,j)+min{d(i-1,j);d(i,j-1);d(i-1,j-1)}
    end for
```

Fig. 3. Code DTW and CDTW.

Fig. 4. Signature acquisition system.

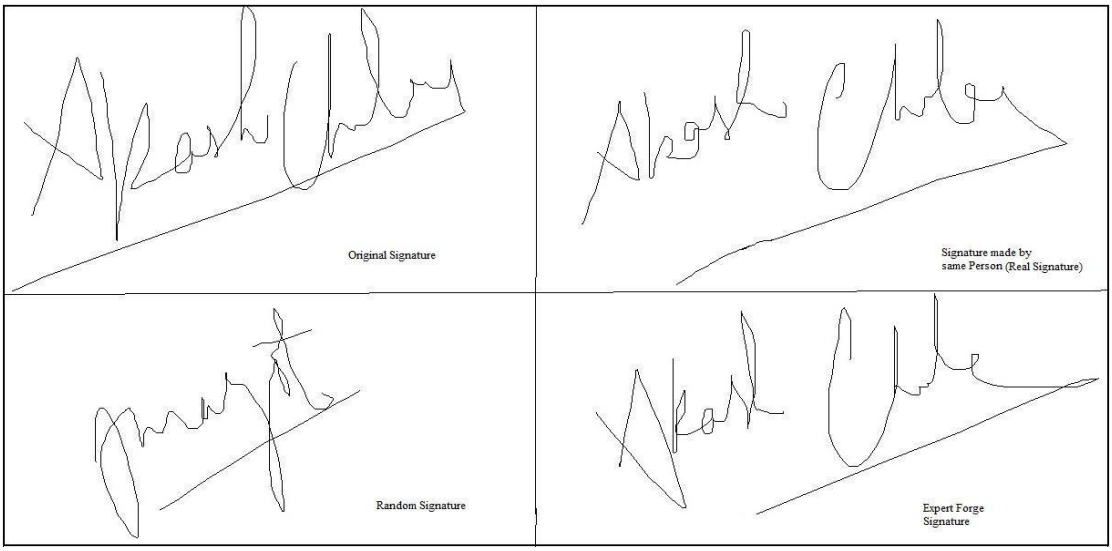


Fig. 5. (a) original signature (b) Signature by same person (c) Random signature (d) Signature by expert forger.

A. DTW and CDTW

In order to understand DTW and CDTW, we prefer to explain the concept of frechet distance. It is defined as the minimum length of leash required to connect a man and his dog. Also recognized as dog man measure, it is a measure of finding similarity between two curves. Consider a situation in which a man is moving, holding his dog with a leash. Then the minimum distance of leash at any point of time required to join both man and dog is called as Frechet distance. The Frechet distance itself is minimum (over all trajectories) of the maximum leash length for the fixed trajectory. But the condition for both man and dog is that both can neither back track their path although they can change their direction and even can stop but can't back track.

Let *X* and *Y* be two continuous curves being defined in a metric space *C*. Both are continuous map from the unit interval into *C*, so that $X:[0,1]\to[0,1]$ (same for *Y*). Consider a reparametrization '*a*' is a continuous, non-decreasing surjection such that $a:[0,1]\to[0,1]$ (same for *b*). Therefore '*a*' and '*b*' are mapping from the unit interval to the unit interval.

Frechet distance is defined as the minimum distance over all reparametrizations a and b of [0, 1] of the maximum over all $t\in[0,1]$ of the distance in C between $Y(b(t))$ and $X(a(t))$;

$$F(X,Y)=\inf_{a,b}\max_{t\in[0,1]}\{d(X(a(t)),Y(b(t)))\} \quad (1)$$

The above mathematical equation cab be explained as the situation where $X(a(t))$ is the position of man at any time t with $a(0)=0$ and $a(1)=1$. Similarly $Y(b(t))$ is motion defined by dog in time *t*. Thus the minimum summation of maximum leash length required to join the two paths over the time interval t is Frechet distance.

DTW (or Discrete Dynamic time warping) is a method which measures the similarity between curves based on a time distortion function. It aligns the curves in best possible way and measures the distance between them by sampling the curves. Sampling has high influence on its results. For each sample in a curve it finds the sample that can be best aligned in its way using a predefined metric. It has been applied in many fields of protein structure matching, computer vision and data mining. But it suffers drawback as it is defined over discrete edge points. The part where sampling is sparse affects the output as the part is not properly resolved. Solutions like spline interpolation are available but it will

over burden the computational cost. Continuous Dynamic Time warping overcomes these drawbacks of DTW since it is defined over continuous terrain rather than discrete point.

Let A and B be 2 curves defined over time $T=(t_1,t_2,...t_n)$. Let x_i and y_i be defined on the path at t_i so that $x_i = X(t_i)$ and $y_i = Y(t_i)$. Let them be the vertices of curve. The dynamic time warping measure d is defined as the distance obtained by the function-

$$D_{dtw}(X,Y)=\min_{\beta}\sum_{\beta_a=(i.j)\in\beta}^{n}\left\|y_j-x_i\right\| \tag{2}$$

where $\beta=(\beta_1,\beta_2,.....,\beta_m),\beta_i\in[1....n]^2$ is satisfying continuity for $\beta_i=(a_i,b_i),\beta_{i+1}=(a_{i+1},b_{i+1}),$ we have $a_{i+1}-a_i\le 1, b_{i+1}-b_i\le 1$. Monotonicity for all $(x_1,y_1),(x_2,y_2)\in\beta$ where $x_1\le x_2$ we have $y_1\le y_2$.

A translation variant kind of D is defined with $z_a=y_j-x_i$ is

$$D_{dtw}(X,Y)=\min_{\beta}\sum_{\beta_a\in\beta}\left\|z_a\right\| \tag{3}$$

The measure $\tilde{D}_{dtw}(X,Y)$, denoting translation invariant DTW will be defined as

$$\tilde{D}_{dtw}(X,Y)=\min_{\beta}\sum_{0\le a<m}^{n}\left\|z_{a+1}-z_a\right\| \tag{4}$$

The above mathematical expression works on the simple principle of firstly finding the distance between all points in two curves and then it finds the minimum distance between two curves by minimizing the total sum of distances between points in two curves over its length. The code for DTW is presented in fig. 3 which can be modified for CDTW.

B. Hidden Markov Models (HMM)

Hidden Markov Model is a stochastic process with an underlying finite state structure satisfying the model topology, output distribution parameters and transition parameters [2]. Hidden markov model follows a number of states to predict the final result. Each of these states is associated with a random function. The signal to be estimated possesses some measurable and distinct properties within a state. Within a discrete period of time, the process is assumed to be in a specific state while an observation is generated by the random function related to the state. Depending upon a set of possibilities associated with each state, the system transits from one state to another. Another important parameter which can be continuous or may be quantized is the physical output of system. Deciding the number of states N is also an important task. Other parameters in the HMM which need to be managed are the Initial State Probability, the state transition probability and the observation system probability.

The HMM model is summarized as follows. The observation sequence is provided to find the probability of observation sequence. The observation sequence is further used to choose the corresponding state sequence. Given the model, the work is to adjust its parameters to maximize the probability of the observation sequence.

V. Results

The results obtained enable us to investigate the capabilities of our system applied to real signature datasets. The paper proposes a novel ATM machine which can be can be effectively used to limit forgery attempts. The system consists of a unique identity number followed by signature verification. The paper uses and compares three different techniques for signature verification mainly DTW, CDTW and HMM.

The section elaborates and compares the results obtained for all three methodologies tested on a Pentium core 2 duo 1.83 Ghz machine. The algorithms are compared on the basis of runtime analysis and the accuracy of signature verified, compared across a common ground truth. This section further emphasizes on the factors affecting the performance of the algorithms, followed by their advantages as well as disadvantages.

The inputs given to the system using the signature acquisition system shown in Fig. 4 is the original curve which the writer is asked to inscribe while the secondary curve can be the signature rewritten by the writer, the signature inscribed by an expert forger or the forger signature done by an armature writer as shown in Fig. 5. The results obtained in case of signatures helps to identify if the sign is by the authorized person or if it's a forge. The results obtained for all three methods DTW, CDTW and HMM are applied to real data are shown in Fig. 8. All the algorithms are one by one applied to both the inputs resulting into the confusion matrix shown in fig6 and Fig. 7 for DTW and CDTW respectively while the overall acceptance rate for all three algorithms is shown in Fig. 8. CDTW takes 3 seconds to compute, DTW takes 2.4 while HMM performs in 4 seconds. The results demonstrates that CDTW is more effective than HMM or DTW in recognizing the signature. CDTW has the highest success rate followed by HMM while DTW standing at the last. The ability of CDTW is also explained from its confusion matrix shown in Fig. 7. The large increase in distance as we move from original signature to forge signature helps in differentiating the signatures efficiently. Overall CDTW is the most capable method among the methods experimented above.

	Original (base)	Real signature	Expert forge	Random signature
Original (base)	0	41	164	383
Real signature	413	0	108	455
Expert forge	164	108	0	489
Random signature	383	455	489	0

Fig. 6. Confusion matrix by DTW applied to different signatures.

	Original (base)	Real signature	Expert forge	Random signature
Original (base)	0	55	201	473
Real signature	523	0	156	574
Expert forge	164	108	0	601
Random signature	473	574	601	0

Fig. 7. Confusion matrix by CDTW applied to different signatures.

METHOD	DTW	HMM	CDTW
Successful Acceptance Rate(%)	90.3	92.7	94.6

Fig. 8. Acceptance rate for DTW, CDTW and HMM applied to different signatures.

VI. Conclusion

The results obtained from real time simulation by CDTW, DTW and HMM applied on real time data are presented in the paper. The following presents a concise summary with the conclusions related to the performance of algorithms. CDTW performs much better than DTW and HMM with the highest accuracy. CDTW gives minimum distance between two curves to a much higher precision as compared to DTW while it performs much better than HMM. The value given by CDTW is higher than DTW and HMM signifying that it can measure to much higher accuracy, leading to a very less false acceptation ratio as compared to the other method. In the process of CDTW, along with the points used in DTW process, some more intermediate points are introduced making the distance between the curves function somewhat more continuous. Theses intermediate points an extra edge over the DTW and HMM method. The CDTW distance calculated between the curves helps in analyzing the originality of data. CDTW is observed to be more accurate as compared to DTW as DTW works only on end points while CDTW computes the similarity on end as well as intermediate points. The distance matrix clearly demonstrates the capabilities of the system to differentiate forge signatures effectively from the original signature by a large margin. Overall CDTW is a much better option to choose as compared to other methods.

CDTW find application in many real time applications. They are used for stock analysis, protein structure matching, speech recognition, in database, in computer vision, in time series clustering and data mining. It has been also used for sub pixel contour matching. It is for the first time that an alternate to ATM card through signature verification is proposed.

References

[1] M. E. Munich and P. Perona, "Continuous Dynamic Time Warping for translation invariant curve alignment with applications to signature verification," in *Proc. of the 7th International Conference on Computer Vision (ICCV'99)*, Korfu, Greece, September 1999.

[2] D. Muramatsu and T. Matsumoto, " An HMM on-line signature verifier Incorporating signature trajectories," in *INCDAR*, pp. 438-442, 2003

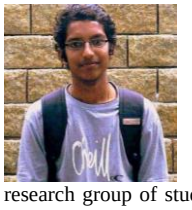
[3] M. Faunddez-Zauny, "On-line signature recognition based on VQ-DTW," *Pattern Recognition* vol. 40, no. 3, pp. 981-992, 2007

[4] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," *Pattern recognition* vol. 35, pp.2963-2972,2002

[5] C. Tappert, C. Suen, and T. Wakahara, "The state of the art in on-line handwriting recognition," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 12, pp. 787–808, 1990.

[6] A. Kholmatov and B. Yanikoglu, "Identity authentication using improved online signature verification method," *Pattern Recognition Letters* vol. 26, no. 15, pp.2400-2408, 2005

[7] A. Efrat, Q. Fan, and S.Venkatasubramnianan, "Curve Matching, Time Warping, and Light Fields: New Algorithms for Computing Similarity between Curves," *Journal of Mathematical Imaging and Vision*, vol. 27, no. 3, pp. 203-216, DOI: 10.1007/s10851-006-0647-0.



Srikrishna Karanam (srikrishna@ieee.org) is currently pursuing his Bachelor's degree in Electronics and Communication Engineering at the National Institute of Technology Warangal, India. His research interests include Robotics and Computer Vision. He is the co-founder of the illuminati@nitw (illuminatiatnitw.weebly.com), a research group of students well known across many countries in Asia and Europe. In the past, he has received third place in the IEEE Region 10 student paper contest. He was also a finalist in the 2011 IEEE Presidents' Change the World Competition. His study is partially supported by the Institute Merit Scholarship Fund of NIT Warangal and the Central Board of Secondary Education, Government of India. He is a student member of the IEEE.