Recognition of Dynamic Signatures for People Verification

Shern Yau and Dinesh Kant Kumar

School of Electrical and Computer Engineering,RMIT University Melbourne, Australia

Abstract. Machine based identity validation has applications such as authentication of documents, for financial transactions, and for entry into restricted space and database. The ineffectiveness of password and personal identification numbers has been demonstrated by recent explosion of frauds. This paper proposes the use of unpenned dynamic signature to validate the authentic user and related transactional instruments. A comparison of the ability of various classifiers for classifying the multi-dimensional features of the dynamic signatures is reported. The technique has been tested for single user and multi user and also when the forger is actively attempting to cheat the system. The system is able to perfectly determine the authentic user from other users when the user's signature trace is secret. The system is also able to perfectly reject forgers who may have access to the user's signature, with a 10% of the authentic user signature being classified as 'unknown'.

1 Introduction

Our society is extremely conscious of security with an urgent need for securing building space, data, and transactions. It is important to verify the identity and authenticate an individual and related instruments of communication such as emails and e-documents. There are three underlying principles for verifying the identity of an individual- what they have (identity card), what they know (password) or what they are (biometrics).

Penned signature is by far the most common person validation technique. This combines the 'what they know' with 'who they are' and makes it a very effective tool for person verification. Time immemorial, signatures have been used to validate identity of people or authenticate documents and other such instruments. For less sensitive applications such as validation of the signature is routinely conducted by lay people such as people on the retail outlet check-out counter or teller of a bank or the sentry of the building. Often the signatures are verified based on the visual comparison with the sample of the authentic signature that is either kept on the back of the card (credit card) or other similar instrument.

While the use of penned signatures in the traditional banks was not free from frauds, the number of frauds was few because the bank executives were trained to be able to spot forgery. But with the explosion of the use of credit cards there has been an explosion of frauds. The database of the authentic signature are available at the back of the card itself, and the check-out cashier are not trained to spot forgeries.

Yau S. and Kant Kumar D. (2007).
Recognition of Dynamic Signatures for People Verification.
In *Proceedings of the 7th International Workshop on Pattern Recognition in Information Systems*, pages 189-198
DOI: 10.5220/0002417601890198

While graphic-analysis experts are able to spot the differences between authentic signatures and frauds, a lay person at the counter of a departmental store is unable to see such subtleties.

Use of Personal Identification Number (PIN) and password have evolved over the past 3 decades to provide means of authentication of people for accessing funds, database or buildings. These are being used at banks and ATM, for telephonic access to financial and data, for accessing computers and database, and as a digital signature to authenticate an electronic document. While this technique has the advantage that it is easy to be automated, there are several shortcomings. Authentic users may forget their PIN, and it has been demonstrated repeatedly that it is possible to deduce the PIN from other seemingly unrelated information of the user.

In the recent past, biometrics techniques have been developed for machine based verification of the identity of a person. Biometric authentication is based on using some physiological or behavioural characteristic of a subject to authenticate that particular subject [12]. Verification is defined as comparing an entity provided by the user to a biometric template stored in the database.

Biometrics based verification techniques such as the use of DNA are suitable for very high level of confidence, these techniques are not feasible for routine applications such as logging into the computer, or accessing funds or paying at the grocery store. Biometrics based techniques that are exceedingly being used include the use of fingerprints, hand geometry and iris scan.

Even though the use of the anatomical measurements of the individual has often been considered to be extremely robust for identifying an individual, these have their own limitation. All traditional biometrics measures have certain limitations associated to them [12]. DNA cannot be used in certain applications due to issues of contamination, sensitivity, cumbersomeness and privacy; ear-shape as a biometric measure has a problem of non unique features; facial biometrics have problems with aging, face disguise and variable imaging conditions; hand and finger geometry can be easily copied. Although fingerprints are very unique but they also have the problem of fake fingers, storage and imaging conditions problems. Iris biometrics is intrusive and has issues of unreliability. Speech biometrics has the limitation of mechanical variance due to the microphone and dependence on subjects' health [12]. The other major concern with the anatomical based biometrics is that these can be copied by the impostor using deceit or force, and once copied, the authentic user would be faced with life-long loss of identity.

To overcome some of the above mentioned shortcomings, researchers have attempted to develop non-anatomical 'biometrics'. Biometrics such as keystroke and gait analysis are based on the behaviour of the individual [12] but the reliability is highly questionable. The other shortcoming in each of these is that these do not give the user any control.

This paper describes a machine based verification of identity that overcomes the above mentioned difficulties. The system is based on the use of traditional signatures, but without the user leaving a visual trace of the signature. The system does not require any photograph, or any other physical or visual trace of the signature. The unpenned signature verifier (USV) – captures the dynamics of the drawing of the signature, which is much more difficult to copy even by an expert forger [10]. The other advantage of this technique is that the data required to authenticate the USV is small enough to be stored within an electronic document or on a smart-card.

The features of the authentic user are a small vector (typical 30 bytes) and may be stored on a database, a smart-card or a computer. The system has been designed such that the user can configure the USV for his/ her signature, without requiring the system administrator.

2 Theory

It is important [3] to seek identity verification modality which provides high degree in performance and yet is still acceptable by a majority of users. Handwritten signatures offer high degree in performance and are "yet a known and established legal status, acceptability by the public, the elimination of common concerns about unwelcome connotations or health factors associated with some other modalities, and the convenience in execution afforded to users". Handwritten signatures also offer the biometrics measures as these are dependent on the user biometrics, while allowing the users to change their signatures for suitable applications.

A signature can be authenticated either through static or dynamic verification. These are discussed below:

Static: In this mode, the signature is written, either on a piece of paper and then scanned or directly on the computer using devices such as the digital pad. The shape of the signature is then compared with the authentic signature. This mode is also known as "off-line" [4]. The difficulty with such a technique is that a good forger will be able to copy the shape of the signature.

Dynamic: In this mode, the user writes his or her signature. This may happen in front of a person, on camera or on a digitized tablet which acquires the signature in real-time. By using this set of dynamic data, further information such as acceleration, velocity, and instantaneous trajectory angels and displacements can be incurred [4].

To dynamically authenticate a signature, features are extracted from a temporal domain scan of the user's signature. These features form a template which is later matched to the user's enrolled signature template. A representative of the user's enrolled signature template needs to be available for the purpose of comparison in the smart card [10] or encrypted with the document or message.

Some of the signature features currently used to determine the authenticity are [1, 4, 13]:

- Azimuth and Altitude.
- Initial and final points.
- Writing speed -X & Y axis.
- Pen pressure.
- Pen-up and pen-down.
- Critical points.
- Pen position.
- Pen-tilt angle.
- Direction and pen movement.

This paper reports the use of the following features:

- Time of pen-up and pen-down.
- Maximum Speed of pen movement.
- Total time to sign.
- Length of the signature.
- Maximum height of the signature.
- Maximum width of the signature.

3 Classification for Verification

Classification involves assigning of new inputs to one of a number of predefined discrete classes. The complexity of a classification task is dependent on the variability of the feature values of the observations of the same class relative to the difference between feature values of the observations of different classes. The variability of the feature values for inputs in the same class may be due to the underlying model of the features or noise[2]. In a signature validation system, the noise associated with classification of visual speech features is due to device, while the variation in the signature of the authentic user is the underlying model variation. It is impossible for classifiers to yield perfect performance and there is always an error rate due to the misclassification of input patterns into wrong classes. However, it is desirable to keep this error rate as low as possible to ensure the robustness of the applications.

Classification is performed via the partitioning of the multi-dimensional feature space using statistical techniques or iterative learning algorithms. If the features can be accurately classified by partitioning the feature space with hyperplanes (or straight lines) are linearly separable. However, most of the real-world pattern recognition applications involve non-linear partitioning of the feature space where the surfaces dividing the feature space in the different class regions are nonlinear[14]. Hence, such tasks would require the use of nonlinear classifiers. Examples of linear and nonlinear classification techniques are Hidden Markov Models (HMM), Artificial Neural Networks (ANN), Bayesian classifier, Support Vector Machines (SVM) and cluster analysis.

These classification techniques can be further categorized into supervised and unsupervised classifiers depending on the availability of training data. Supervised classifiers are provided with training patterns with known class labels and exploit the a-priori information of the training data. The unsupervised classifiers are not given any training data with class labels. For such classifiers, the classification algorithms attempt to find the underlying ‘similarities’ and group the ‘similar’ feature vectors in one class. This paper reports the development of signature validation technique that is user reconfigurable and hence requires a supervised classification system where the targets are determined by the user.

There are number of possible classifiers that are available for classifying the different inputs. The selection of the suitable classifier is very important to ensure the success of the system. Some of the important classifiers are:

A. Bayesian Classifier: Bayesian classifier is a statistical classification technique based on the Bayesian decision theory. The Bayesian classifier quantifies the different classification decisions using probability and costs associated with such decisions.

The Bayesian classifier assigns a feature vector to the 'most probable' class for the feature vector. Such classifier relies on the assumption that the underlying probability values of the input data are known [14]. It may be possible to determine the probability function if the error of misclassification was random, but when attempting to identify a fraud who is attempting to forge the signature, it is not possible to estimate this probability and hence such classifiers are not suitable.

B. Hidden Markov Models (HMM): Hidden Markov Models (HMM) are one of most commonly used classifiers for applications where the pattern is related to the temporal variations. HMM can be applied to both discrete and continuous input signals. Example of HMM-based classifiers are speech recognizers [11]. The main advantage of using HMM classifiers for this applications is the ability of HMM in modelling the temporal variation of non-stationary signals which could be important for classifying the sequence of frames.

HMM models the sketching of the signature by characterizing only the statistical properties of the signal. HMM technique assumes that the input signals can be well characterized as a parametric random process known as Markov processes. The difficulty with this approach is the complexity of the sketch and large number of variables leading to a level of HMM that would be computationally impossible.

C. Artificial Neural Network: Artificial Neural Network (ANN) is an iterative learning technique from the field of Artificial Intelligence (AI) that emulates the way human's biological nervous systems, such as the brain, processes information. ANNs learn by examples provided to the network during training. An ANN can be configured for data classification applications through a learning process. The major advantage of using ANN is the non parametric nature of the network and also the ability of ANN to classify data by without assumptions on the underlying statistical distribution of the data. ANN can be made to generalize very well with sufficiently large training sets. The parallel processing capabilities further encourage the use of ANN in speech and image recognition where high computation rates are required and the current systems are far from equalling human performance[8]. The ability of a lay person to train the ANN to adapt and learn is important when designing a reconfigurable system.

ANN models consist of a number of simple and highly interconnected processing units known as neurons or nodes, which are analogous to the biological neurons in the brain. The ANN model is composed of many nodes operating in parallel and interconnected via numerical weights. The weights are iteratively changed during training such that the ANN learns the features of the given input classes. The nodes of ANN sum the weighted inputs and pass the results through a nonlinear transfer function. The nodes of ANN can be characterized based on the internal threshold and the type of transfer function used. Three common types of transfer function used are; hard limiters, threshold logic elements (linear) and sigmoidal nonlinearities. The architecture of an ANN can be varied and may consist of a single or multiple layers of neurons.

Number of training algorithms have been developed for different applications and ANN design. The training of ANN may be supervised or unsupervised. Unsupervised ANN classifiers are self-learning and involve the partitioning of the data in the feature space into subgroups where input and target pairs are not provided

during training. Unsupervised ANN classifiers are related to clustering techniques. Supervised ANN classifiers require training with suitable examples (input and target pairs) to learn the patterns of each class[7].

4 Measure of Performance

The criterion for performance of the system is measured by the ability of the system to identify the authentic user and reject the impostor. As with any security system, given that the subject is, or is not a true instance of the enrolled subject, there are four possible outcomes of the errors [2]. The accuracy of any biometric method may be judged by four measures of error:

- Acceptance of Authentic Enrolled Subject (AA) or Genuine Accept Rate (GAR)
- Acceptance of Impostor Subject (IA) or False Accept Rate (FAR)
- Rejection of Authentic Subject (RA) or False Reject Rate (FRR)
- Rejection of Impostor Subject (RI) or Genuine Impostor Rejection (GRR)

The biometric system accuracy requirements depend greatly on the application. In forensic applications, such as criminal identification, FRR rate (and not FAR) is the critical design issue, because we do not want to miss a criminal even at the risk of manually examining a large number of potentially incorrect matches that the biometric system identifies. In some cases the FAR might be one of the most important factors in a highly secure access-control application, where the primary objective is prevent impostors (e.g., at airports). Many civilian applications such as digital signatures require the performance requirements to lie between these two extreme limits of both FAR and FRR. The first (GAR) and the fourth (GRR) identification rates are the main goals to test the efficacy of the method.

The application of the current system is to ensure that the impostor is rejected, while minimising the rejection of the authentic user. It is thus desirable to have FAR as close to zero as it is possible.

5 Method

This paper reports experimental verification of the unpenned signature verifier for two applications. The first requires the system to identify the individual based on the unpenned signature from the database. The second requires the system to determine the authentic user when there are number of people attempting to forge the signature of the authentic user. The experiments have been conducted using a digital tablet and stylus (make ADC).

The method of person identification is divided into two separate modules: an enrolment (or training) module and a recognition (or testing) module. The enrolment module is responsible for enrolling new individuals in the system database. During the enrolment phase, the individual supplies a number of samples of his/ her signature. A model (developed iteratively) of the individual is built based on the features extracted from the signature. During the recognition (test) phase, the

individual repeats the signature. A measure of similarity is computed between the features of the test signature with the signatures during enrolment. A multilayer perceptron (MLP) of with 50 hidden and 1 output neurone was used for this purpose. The size was determined iteratively. The efficacy of the technique is determined by computing the Accuracy of Accepting an Enrolled Subject AAES (%) and Accuracy of Rejecting the Impostor (ARI%).

5.1 Experimental Settings

This paper reports two sets of experiments; (i) identifying if a non-authentic user could be classified as the user, when the signatures of the user are not known and (ii) identifying the ability of the system to detect a forgery, when the fraud attempts to copy the signature of the user. The experiments were conducted on 17 subjects. The two set of experiments are described below:

Experiment 1. The first experiment required the subjects to sign on a digital tablet and repeat the signature 30 times. The start of the signature was determined by the pen-down instant, while the end of the signature was manually segmented. Each subject was the 'authentic user' and against were the other people who also were asked to record their signatures. Each sample of the signature were parameterised. The parameters were then used to train the MLP that had the size of 90*50*1 neurones. After the training was completed, the user was made to repeat the signature 10 times. Other people were also asked to repeat their signatures own respective signatures 10 times. These signatures were then used to test the system. The correct classification of the authentic user and the 'others' was tabulated and used to determine the performance of the system.

Experiment 2. In the second experiment the data of 60 signature samples were considered. 30 of them were signed by one person – the authentic user, and the other 30 are signed by 5 other people (selected randomly) who were asked to copy the signature of the first person. These 5 people were shown the signatures of the authentic user, were given a trace of the signature and were requested to learn to copy the authentic signature. 20 out of the 30 signatures were signed with the help of a guide to help them sign as close as the reference signature as they could. The rest of the signatures were signed by the 'forger' signers after they had practiced the authentic signature. Lay people were unable to identify the difference from the trace.

From the pool of 30 samples belonging to each class, 20 out of 30 genuine and forged signatures were chosen at random to be used as training data for the neural network classifier. The balance 10 signatures of each of the class were used as test samples.

The MLP output was given a threshold of 0.4 and 0.8, such that if the output was less than 0.4 was classified as 0 and output greater than 0.8 as 1. An output greater than 0.4 and less than 0.8 was classified as 'unknown'.

For checking the efficacy of the approach Accuracy of Accepting an Enrolled Subject AAES (%) and Accuracy of Rejecting an Impostor ARI (%) is calculated and tabulated.

6 Results and Discussion

The results of the experiments have been tabulated in tables 1, 2 and 3. Table 1 is shows the output when the tests signatures were used on the trained neural networks.

Table 1. Results of Experiment 1- authentic user and other user.

	ANN Output	
Sample no.	**genuine**	**Other**
1 to17	100%	100%

From this table, it is observed that the genuine acceptance rate for the system when the other users are not attempting to forge gives perfect results (100%). This demonstrates that the ability of the system for low level security applications.

Table 2. Results of Experiment 2- Authentic user and Forger- 10 examples.

	ANN Output		**Classification accuracy, threshold = 0.4, 0.8**	
sample no.	**genuine**	**forgery**	**genuine**	**forgery**
1	0.941	0.0029	√	√
2	0.829	0.004	√	√
3	0.936	0.0029	√	√
4	0.574	0.119	Unknown	√
5	0.975	0.787	√	Unknown
6	0.5337	0.0729	Unknown	√
7	0.9917	0.3322	√	√
8	0.89	0.7943	√	Unknown
9	0.9585	0.0849	√	√
10	0.9505	0.0099	√	√

Table 3. Table of Genuine Acceptance Rate, False Acceptance Rate, False Reject Rate and Genuine Reject Rate for Experiment 2.

Type	**percentage**
GAR	90%
FAR	0%
FRR	0%
GRR	90%

From the table 2, it is observed that the system is robust and no forger is classified as the authentic user. The robustness of the system is also demonstrated

because it does not classify any authentic user as a forger. However the system does classify 2 forgers and 2 authentic user signatures as Unknown. The False Acceptance Rate and False Rejection rate is perfect (0%), the Genuine Acceptance Rate and Genuine Rejection Rate is at 90%.

The results of the second experiment demonstrate that the system is suitable for high level security applications where it is essential that FAR and FRR is 0, while the GAR and GRR are 'reasonable'.

7 Conclusion

The experiments results validate the use of unpenned dynamic signatures based system for digital verification of the identity of the authentic user. The size of the data required for the verification of a user is small and may easily be applied for validating the author of related instruments of communication such as emails and e-documents.

Experiments were conducted to determine the ability of the system to (i) recognise the signature from a database of signatures and (ii) determine the authentic signature against forged signatures. The results indicate that the system is able to recognise the authentic user with perfect accuracy from a small database of about 20 signatures. The system also demonstrates robustness when the other users actively attempt to forge the authentic user's signatures, even with the help of tracing guides. The system has perfect False Acceptance Rate and False Reject Rate, suggesting its suitability of being used for high security applications.

The system has used easy to obtain digital tablets, and utilises a simple neural network that allows the user or user defined reconfiguration. The system provides the user the ability to change their signature, and does not require a physical trace of the signature, making it extremely secure.

Unlike some biometrics systems that are based on the anatomical measures of the users, this system is user defined and controllable, and overcomes the shortcomings of the biometrics techniques. It is based on time tested and accepted penned signature and is expected to be acceptable across different national and cultural boundaries, while providing similar level of reliability. It does not suffer from other biometrics shortcomings such as the permanent loss of identity of an authentic user as it empowers the user with the choice of the signature.

References

1. Dimauro, G., Impedovo, S., Lucchese, M.G., Modugno, R. and Pirlo, G., "Recent Advancements in Automatic Signature Verification," Frontiers in Handwriting Recognition, 2004. IWFHR-9 2004. Ninth International Workshop, pp. 179 – 184, 2004.
2. Duda, R.O., Hart, P.E., and Stork, D.G., Pattern Classification: John Wiley & Sons Inc, 2001.
3. Fairhurst, M.C. and Kaplani, E., "Perceptual analysis of handwritten signatures for biometric authentication", Vision, Image and Signal Processing, IEE Proceedings, vol. 150, no. 6, pp. 389 – 394, 2003.

4. Faundez-Zanuy, M., “Signature Recognition State-of-the-art,” Aerospace and Electronic Systems Magazine, IEEE, vol. 20, no. 7, pp.28 - 32, 2005.
5. George Panotopoulos, D.P., "Hand Gesture Biometrics", Caltech Centre for Neuromorphic Systems Engineering, 2001.
6. Jain, A. Griess F, and Connell D, "On-line signature verification," Pattern Recognit., vol.35, no.12, pp.2963–2972, Dec. 2002.
7. Kulkarni, A.D., Artificial Neural Networks for Image Understanding. New York: Van Nostrand Reinhold, 1994.
8. Lippmann, R.P., “An Introduction to Computing with Neural Nets,” in IEEE ASSP Magazine, 1987.
9. Nixon, M.S., et al., "Automatic Gait Recogntion", Biometrics: Personal Identification in Networked society, pp. 231-250, 1999.
10. Plamondon, R., “The handwritten signature as a biometric identifier: psychophysical model and system design,” Security and Detection 1995. European Convention, pp. 23 – 27, 1995.
11. Potamianos, G., Neti, C., Gravier, G., Garg, A., and Senior, A.W., “Recent Advances in the Automatic Recognition of Audiovisual Speech,” Proceedings of the IEEE, vol. 91, pp.1306-1324, 2003.
12. Prabhakar, S., Sharathpankanti. and A.K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security and Privacy, 2003.
13. Schmidt, C. and Kraiss, K.F., “Establishment of Personalized Templates for Automatic Signature Verification,” Document Analysis and Recognition, 1997. Proceedings of the Fourth International Conference, vol. 1, pp. 263 – 267, 1997.
14. Theodoridis, S., and Koutroumbas, K., Pattern Recognition: Academic Press, 1999.