VERIFYING ON-LINE HANDWRITTEN SIGNATURE USING NEURAL NETWORKS APPROACH

Fadzilah Siraj, Azizi Zakaria, Wan Hussain Wan Ishak
Sekolah Teknologi Maklumat

ABSTRACT : Signatures are used everyday to authorize the transfer of funds for bank cheques, credit cards, legal documents and others. Forgeries on banking and business transactions amount to a large sum of money every year. Although the cashier sometimes can spot the forgeries, it is not cost effective to check the forgeries manually. Hence, if automated verification is available, this will certainly benefit the customers and promote Electronic Commerce. Thus handwritten signature verification system can play an important role in future reading system (Bartneck, 1996). It is a worthy and challenging area of further investigation (Cote et. al, 1998). This paper discusses the neural network models and thus identifies suitable model for on-line Handwritten Signature Verification. Such a model is implemented and the performance of the neural network model is evaluated.

Keywords: *Digital signature, On-line handwriting signature, On-line signature verification, Electronic signature, Electronic authentication, Neural networks.*

1.0 Introduction

As transaction through Internet such as electronic commerce became a new way of doing business, the electronic authentication has been used to improve security for banking and business transactions (Kuner and Miedbrodt, 1999). The used of credit card or plastic money was introduced since the cash payment is not suitable for transaction through Internet. However, as the transaction is done on-line the security has become the major issue to be considered. One of the most common way to overcome the problem is by introducing the digital signature. The digital signature is defined as a string of bits that uniquely represents another string of bits that is formed using a combination of software techniques and cryptography based on a secret value known only to the signer (Kang, 1998). In conjunction with this approach, there are several security concerns regarding the secrecy of digital signature namely, the human error, storage and backup as well as the possibility of someone breaking the codes. Since the security is an important issue in digital signatures, a new technology

should be explored to increase security in electronic transactions. Kang (1998) suggested that handwritten signature can be replaced or combined with digital signature to promote security. To this end, the electronic signature is defined as the string of bits that digitally represents a handwritten signature captured by computer system when human applies it on an electronic pen pad connected to the system. In this paper, the electronic signature is referred to as the handwritten signature.

The differences between the handwritten and digital signatures are presented in Table 1 (Fillingham, 1997).

Table 1: Differences between handwritten signature and digital signature

Handwritten signature	Digital signature
Biologically related with an individual.	Bind signatures to individuals through technical and procedural mechanisms.
Controlled by that individual.	Applied by a computer commanded by the signer.
Forgeries detection done by the expert.	Detected by the computer.
Data integrity is week.	Data integrity is much stronger.
Can be witnessed.	Can be notarized.
Can be used for verification as long as it is in good condition.	Limited to certain time or the evolution of cryptographic technique.
Secure against repudiation.	Required third party time-stamping to augment their non-repudiation security service.
Suitable for any level of security.	Vary widely in the strength of the security they offer.
Simple and easy to understand.	Complex and hard to understand.

Three main factors that governed the security of digital signature namely, the secrecy of the secret value, the integrity of the public value, and the cryptographic strength of the digital signature algorithm (Kang, 1998). These factors influence the security of on-line services that uses the digital signature. The secrecy of the secret value depends on several other factors such as its composition, the rightful owner and the system used. There always a case where the rightful owner given away their numbers to their trusted friend. This trusted one uses the signature without acknowledging the real owner. When the owner realizes, the transaction has been done and he or she has to take the responsibility for the transaction. In the second factor, the public value is digitally representing the identity of the signer. If the value is compromised by the perpetrator then the integrity of the signed message becomes questionable.

The digital signature algorithm is used to generate the unique digital signature from the given input. The cryptographic strength of the digital signature algorithm helps to avoid the perpetrator or hackers from interfering the signed document. If something went wrong with any factor mention above, the digital signature would not be reliable to secure the transactions. A new method or approach needs to be explored to overcome the weaknesses of digital signature. One possible approach is to combine a digital signature with handwritten signature in order to minimize or at least overcome the shortcoming of both techniques. Handwritten signature is a name of an individual, written in script by that individual (U.S. Department of Health and Human Services, 1992). In conjunction with the combined methods, a high assurance document integrity system can be achieved. As a human signature is a behavioural attribute of a person, the imitation of signature is a very difficult process (see Figure 1). This paper discuses the use of artificial neural network models for verifying on-line handwritten signature verification system. Several models will be chosen and the model that obtains the highest generalization performance, lower false

acceptance rate and false rejection rate will be recommended to be incorporated in the verification system.

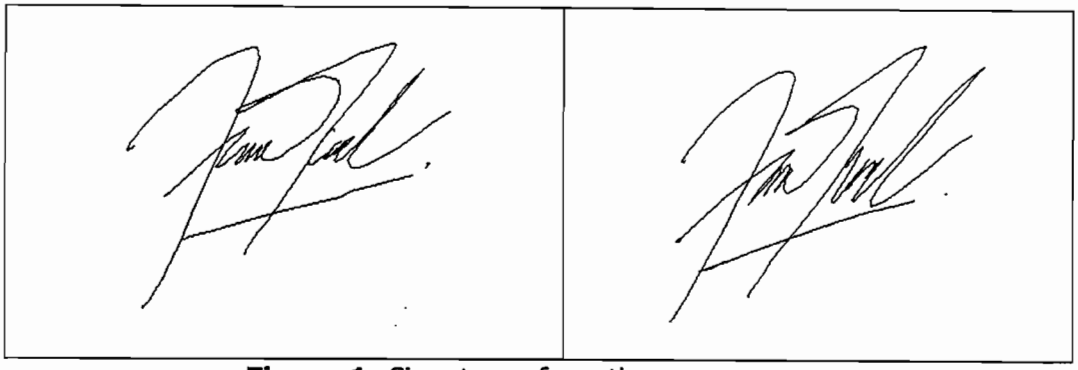

Figure 1: Signatures from the same person

2.0 Neural Networks In Handwritten And Handwritten Signature Verification Systems

Handwritten signatures that is signed on a piece of paper has been used as an authentication tool. The uses of signature have been recorded in the Talmud (fourth century), complete with security procedures to prevent the alteration of documents after they are signed (see (Fillingham, 1997)). To date, with advances in computer and hardware technology, handwritten signature can be recorded electronically (Lecrerc and Plamondon, 1994). One of the recent techniques implemented in handwriting and handwritten signature verification system is using neural networks.

Schomaker *et al.* (1994) used automatic detection of generic handwriting style to counteract the problem. The data was pre-processed and in this case, the neural network model known as a Kohonen Feature Map is used to obtain a finite list of prototypical strokes. In the next processing level, the strokes codes are classified as letters by probabilistic stroke transition network. In other studies, a Time Delay Neural Network (TDNN) improves the generalization of

character recognition problem (Matic *et al.,* 1994 and Cardot *et al.,* 1994). An extension of TDNN known as A Multi State Time Delay Neural Network (MS-TDNN) was employed in on-line cursive handwriting recognition (Manke and Bodenhausen, 1994, and Manke *et al.,* 1995). The network combines the high accuracy character recognition of a TDNN with non-linear time alignment procedure. The study shows that MS-TDNN is capable to learn and finding stroke and character boundaries in handwritten words and perform the classification with high recognition performance. On-line handwriting recognition could also be performed during the data entry (Grob, 1997). In addition, a TDNN was combined with Hidden Markov Models (HMM) to handle variety of writing styles including cursive script (Tay and Khalid, 1999) and hand-print (Schenkel *et al.*, 1995). This neural network model was also used to estimate a *posteriori* probabilities for characters in word (Cardot *et al.,* 1994). The word were segmented and optimized by HMM using the dictionary. On the other hand, HMM could also be combined with other neural networks model such as Radial Basis Function to improve the performance of the networks (Lemarie *et al.,* 1996).

Another neural network model called feedforward network with backpropagation learning algorithm was utilized in off-line handwritten signature verification (Mighell *et al.,* 1989). The study indicates 2% rejection of genuine signatures with 2% acceptance of forgeries. In another study, multilayer perceptron and Kohonen Map were integrated to perform the cooperation tasks in the recognition systems for signature verification on cheques (Cardot *et al.,* 1994). Guyon *et al.* (1995) developed Penacée (system for recognizing on-line handwriting) with a multi-modular architecture by incorporating Time Delay Neural Networks (TDNN). This system outperforms the existing commercial system with 80% of forgeries correctly detected and 5% rejecting the genuine signature. The neural networks models that have been implemented in handwritten signature verification are summarized in Table 2.

Table 2: Summary neural network models usage in handwriting and handwritten signature verification

Model	Research
Feedforward network with backpropagation	Mighell *et al.*, 1989
Time Delay Neural Network (TDNN)	Seni, 1995; Guyon *et al.*, 1995; Cardot *et al.*, 1994
Multi State Time Delay Neural Network (MS-TDNN)	Manke and Bodenhausen, 1994; Manke *et al.*, 1995
Recurrent Neural Networks (RNN)	Senior, 1994
Kohonen Map	Schomaker *et al.*, 1993; Schomaker *et al.*, 1994; Cardot *et al.*, 1994
Multilayer Perceptron (MLP)	Cardot *et al.*, 1994
Adaptive Resonance Theory (ART)	Dimauro *et al.*, 1997

3.0 Methodology

The handwritten signature verification system consists of three main modules: the data acquisition, preprocessing and neural recognizer modules. The data acquisition module involves the capturing of digital signatures and the handwritten signatures. The digital signature is used as a verification phase prior to capturing the handwritten signatures. The first tasks of handwritten signature verification system involves obtaining raw data. Data could be divided into two categories depending on how the data was collected whether, on-line data or off-line data (Seiler, 1994). On-line data usually collected using the digitizer (Figure 2). On-line data is preferable as the temporal information about the handwritten signature is still available (Manke and Bodenhausen, 1994). Off-line data usually captured using the digital camera or the scanner (Figure 3). In this case, the dynamic information of the signature is not available. However, there exists techniques to retrace the handwritten

signature and collect the dynamic information. The tracing involves hierarchical decision making for stroke identification and ordering based on the heuristic rules (Lee and Pan, 1992). In some cases, the signature is mixed with the background patterns particularly the signature on the cheque. This problem could be solved using the technique proposed by (Yoshimura and Yoshimura, 1994).

Figure 2: Digitizer used to captured the signature

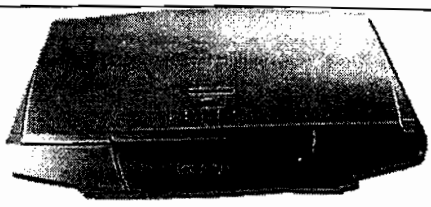

Figure 3: Scanner used for off-line data

In this study, on-line data was collected using the digitizer (see Figure 2) and presented as a string of coordinates (*x,y*). The coordinates were then preprocessed to eliminate noise ((Musa *et al.*,, 1990) and (Maudal, 1996)) that could reduce the data quality and reduce recognition performance (Plamondon, 1994). The smoothing was performed to reduce the noise caused by the erratic hand motion and inaccuracies of the digitizer (Seni, 1995). The smoothed data was further preprocessed to select the attributes that represents the signature (see Figure 4). A previous survey in the fields of on-line signature verification has shown that most system can be classified in two principal methods: those using function as features and those dealing with parameters. In the first method, the complete signals (for example positions, velocity, acceleration, etc.) are considered as, or are represented by, mathematical time function whose value directly constitute the features sets. In the second method, the parameters are referred as features that are computed from the

measured signals (Plamondon, 1994). The system in this study adopted the first method as suggested by (Nelson *et al.,* 1994).

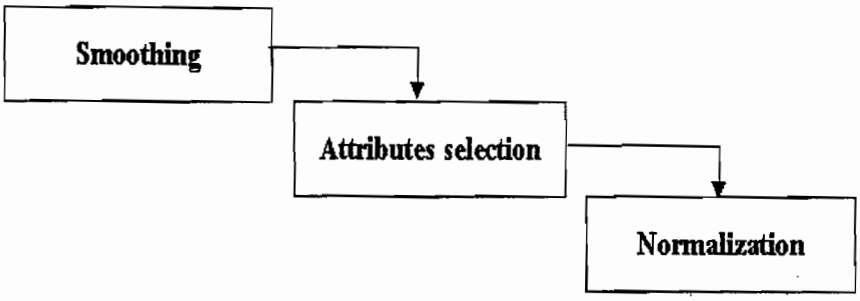

Figure 4: Preprocessing stages

It was reported in the literature that many kind of relevance attributes could be selected from the signature (Gupta and McCabe, 1997). For the purpose of this study, only nine attributes will be used (Dullink *et al.,* 1995) viz.:

- Total time
- Number of zero crossings in x-velocity
- Number of zero crossings in y-velocity
- Number of zero crossings in x-acceleration
- Number of zero crossings in y-acceleration
- Number of zero values in x-acceleration
- Number of zero values in y-acceleration
- The overall pen-up time
- Overall path length

The attributes are then normalized, so that all the attribute value is in the range 0 and 1. Each signature is normalized simply by dividing each parameter by the parameter that has the largest value for a particular pattern (Bigus, 1996). Several characteristics are identified to distinguish between the true signature

and the forged ones. The forged signatures can be identified by a few factors such as ((Fillingham, 1997) and (Anderson, 1994)):

- Written slower then the genuine signatures.
- Frequent change of the grasp of pencil or pen.
- Blunt line endings and beginnings.
- Retracing and patching.
- Stops in places where writing should be free.

In order to train the neural networks models, the forgeries data need to be included in the learning and test sets ((Mighell *et al.,* 1989) and (Anderson, 1994)). The forgeries are created by obtaining forged signatures, which resemble the genuine signature, written freehand to produce what is known as a "simulated forgeries". The forged signatures were also obtained from forged "signatures of fictitious person". Other forgeries were collected from forged signatures where no attempt has been made to make a copy of the genuine signature of the person purporting to sign the document. The complete architecture for the handwritten signature verification system is illustrated in Figure 5. Once the digital signature is verified, the handwritten signature is captured using the digitizer. The signatures will be pre-processed before they are stored in the database. The data will be divided into three sets, namely the training, validation and test sets. Once the signatures are trained using the neural recognizer, the neural network models will be evaluated using the test set. The generalization performance, the false acceptance rate (FAR) and false rejection rate (FRR) will be calculated to assess the performance of the networks (Cardot *et al.,* 1994).

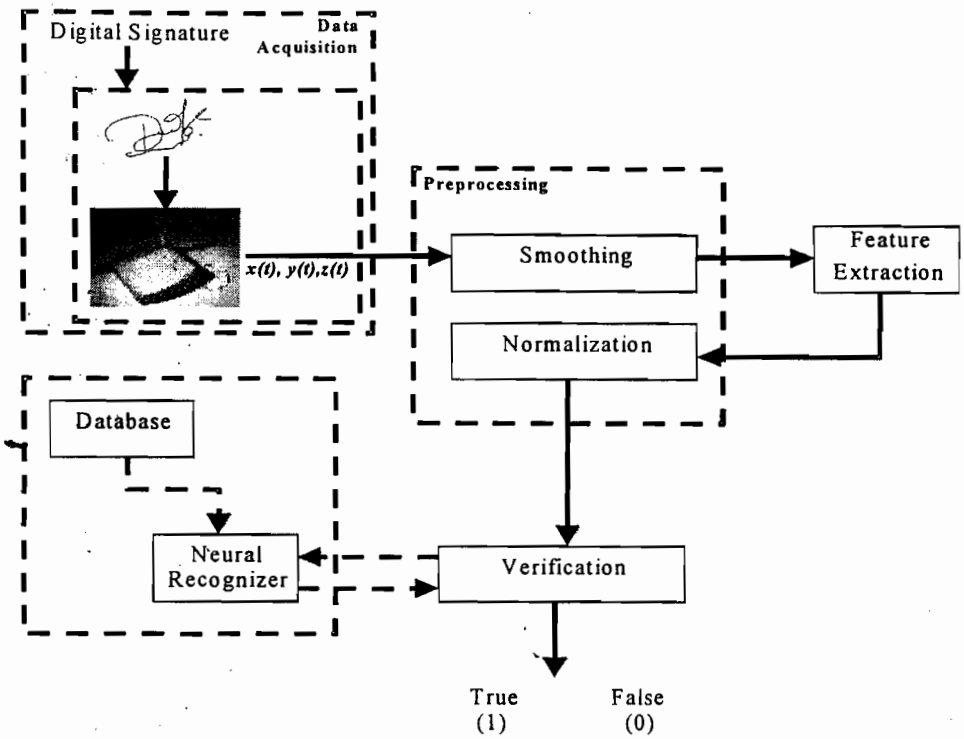

Figure 5: System Architecture

4.0 Results

The evaluation of the performance of the handwritten signature verification is a difficult task. The result depends to a great extends on the characteristic of genuine signature used for training and also on the quality of forgeries used for the test. To evaluate the performances of a verification system, two rates generally computed: the false rejection rate (FRR) and the false acceptance rate (FAR) (see (Mighell *et al.,* 1989), (Cardot *et al.,* 1994), (McCabe, 1997), and (Gupta and Joyce, 1997)). For general acceptance, FRR should be no more than 0.5% and no more than 20% FAR on forgeries (Nelson *et al.,* 1994).

Cardot *et al.* (1994) suggested that the FRR or FAR must be below a desired rate, for instance FAR must lower than 1%.

Several neural networks models and a statistical model were utilized in the experiments. The results are presented in Table 3. Two neural networks models achieved 100% generalization performances. Comparing the Multilayer Perceptron (single hidden layer) with the Radial Basis Functions, the first model need to be trained only up to 96.3% to achieve 100% generalization. However, Radial Basis Function networks are faster to train than Multilayer perceptron (Bigus, 1996). On the other hand RBF network are not suitable to be used for larger applications ((Bigus, 1996) and (Lemarie *et al.,* 1996)). Therefore, in this case Multilayer Perceptron is preferable to Radial Basis Function networks. The results presented in Table 3 also indicate that for the individual signatures (30 genuine out of 90 signatures) yield at most 5.88% FRR. The results also imply that all models do not produce any FAR. In verification system, it is important to produce low FAR because this will ensure that the system will not allow the unauthorized users to have access into the system.

Table 3: The generalization performance of neural network and a statistical model on handwritten signature.

Model	**Training (%)**	**Testing (%)**	**FAR**	**FRR**
Multilayer Perceptron (MLP) (9-20-1, learning rate = 0.8, momentum = 0.1)	96.3	100	0	0
Radial Basis Function (RBF) (9-20-1, Euclidean, Spline Functions)	100	100	0	0

Model	Training (%)	Testing (%)	FAR	FRR
Bayesian Network (3-5 hidden units)	98.15	94.44	0	5.88
Regression	96.3	94.44	0	5.88

5.0 Conclusion

On-line signature verification has several advantages when compared with other verification system such as face recognition, fingerprint recognition and retina and iris scanning. Some of the advantages of on-line signature verification are listed as follows:

- The verification system can only be applied when human is conscious.
- It is a natural evolution from handwritten signature on paper to electronic digitizer tablet.
- Forging and electronic signature is more difficult then a fingerprint.

The advantages of neural networks are that they can be trained to recognize signatures and their characteristics are such that they could be used to classify signatures as genuine or forged as a function of time through a retraining process based on recent signatures. Their primary disadvantage is often the large number of specimens required to ensure that the networks does in fact learn.

The detection of handwritten signature forgery depends on the skill of the examiner. Many handwritten forgery attempts will not be detected until after action is taken on the basis of the suspect signature (e.g., after the cheque is cashed). Due to the cryptographic nature of digital private signature key has

been compromised, or control of the signing mechanism has been seized. In these cases, distinguishing between a valid and invalid digital signature may be impossible, even for a computer forensics specialist. Handwritten signatures are inherently secured against repudiation (again, to the extent of the skill of the document examiner), whereas digital signatures require third party time-stamping to augment their non-repudiation security service.

At all times, handwritten signatures can be verified, whereas digital signatures will likely become unverifiable after ten years or so due to data processing equipment and cryptographic standards obsolescence, certificate expiration, and other factors. Digital signatures vary widely in the strength of the security services they offer, depending on the certificate policy associated with the signer. Although digital signature technology and handwritten signature have both emerged from two separate technological fields, they are now starting to converge to meet the common objectives of assuring information integrity and authenticity (Kang, 1998). It seems unlikely that handwritten signature will fully replace digital signatures in the foreseeable future. To this end, the combination between handwritten and digital signature will inevitably improve the security for on-line transactions.

The experiment conducted in this study reveals that neural networks approaches to handwritten signature verification system achieved better results than statistical approach. Although, different types of signatures forgeries have been incorporated in the training and test data, the generalization obtained reaches 100%. This indicates that neural networks approach is one of the most promising techniques to be used in conjunction with digital signature for handwritten signature verification system.

References

Anderson, C. (1994). Document Examination, *NSW Law Society Journal.* http://www.docexam.com.au/ download.htm#Document

Bartneck, N. (1996). The role of handwriting recognition in future reading systems, *In: Proc. Of the Fifth International Workshop on Frontiers in Handwriting Recognition*, University of Essex, England, 147-176.

Bigus, J. P. (1996). *Data Mining with Neural Networks*, New York, Mc-Graw Hill.

Cardot, H., Revenu, M., Victorri, B., and Revillet, M. (1994). A Static Signature Verification System Based on a Cooperating Neural Networks Architecture, *International Journal of Pattern Recognition and Artificial Intelligence,* Vol. 8, No. 3, 679-692.

Cote, M., Lecolinet, E., Cheriet, M., and Suen, C. Y. (1998). Automatic Reading of Cursive Scripts Using a Reading Model and Perceptual Concepts.

Dimauro, G., Impedovo, S., Pirlo, G., and Salzo, A. (1997). A Multi-Expert Signature Verification System for Bankcheck Processing. *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 11, No. 5, 827-844.

Dullink, H., Daalen, B. V., Hijhuis, J., Spaanenburg, L., and Zuidhof, H. (1995). Implementation a DSP Kernel for Online Dynamic Handwritten Signature Verification Using the TMS320 DSP Family, *Technical Report*, Texas Instrument.

Fillingham, D. (1997). A Comparison of Digital and Handwritten Signatures, *MIT 6.805/STS085: Ethics and Law on the Electronic Frontier*, URL: http://www-swiss.ai.mit.edu/6095/student-papers/fall97-papers/fillingham-sig.html

Grob, R. (1997). Run-on recognition in an on-line handwriting recognition system, *Technical Report,* University of Karlsruhe, Germany.

Gupta, G. K., and Joyce, R. C. (1997). A Study of Shape in Dynamic Handwritten signature Verification, *Technical Report 97/04*, Computer Science Department, James Cook University of North Queensland.

Gupta, G. K., and McCabe, A. (1997). A review of Dynamic handwritten signature verification, *Technical Report*, James Cook University.

Guyon, I., Bromley, J., Matic, N., Schenkel, M., and Weissman, H. (1995). Penacée: A Neural Net System for Recognizing On-line Handwriting, *In E. Domany, J. L. van Hemmen, & K. Schulten, (Eds.), Models of Neural Networks,* Vol. 3, 255-279. Springer.

Kang, Meng-Chow. (1998). Dynamic Handwritten Signature Verification System Can Electronic Signature Replace Digital Signature?, URL: http://home1.pacific.net.sg/~mckang/RNsign.html

Kuner, C., and Miedbrodt, A. (1999). Written Signature Requirements and Electronic Authentication: A Comparative Perspective, URL: http://www.kuner.com/data/sig/signature_perspective.html

Lecrerc, F., and Plamondon, R. (1994). Automatic Signature Verification: The State of the Art 1989-1993, *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 8, No. 3, 643-660.

Lee, S., and Pan, J. C. (1992). Offline Tracing and representation of Signature, *IEEE Transaction on Systems, Man and Cybernatics*, Vol. 22, No. 4, 755-771.

Lemarié, B., Gilloux, M., and Leroux, M. (1996). Handwritten Word Recognition using contextual Hybrid Radial Basis Function Network/Hidden Markov Models, *Advances in Neural Information Processing Systems 8*, 764-770.

Manke, S., and Bodenhausen, U. (1994). A Connectionist Recognizer For On-Line Cursive Handwriting Recognition. *Proceedings of the International Conference on Acoustics, Speech and Signal Processing (ICASSP 94),* 633-636, Adelaide: South Australia

Manke, S., Finke, M., and Waibel, A. (1995). The Use of Dynamic Writing Information in a Connectionist On-line Cursive Handwriting Recognition System, *In Tesauro, et. al., (Eds.), Advances in Neural Information Processing Systems 7,* 991-1006.

Matic, N., Guyon, I., Denker, J., and Vapnik, V. (1993). Writer adaptation for on-line handwritten character recognition, *Second International Conference on Pattern Recognition and Document Analysis*, 87-191, Tsukuba: Japan.

Maudal, O. (1996). Preprocessing Data for Neural Network Based Classifiers: Rough Sets vs Principal Component Analysis, *M.Sc Thesis*, University of Edinburgh.

McCabe, A. (1997). Implementation and Analysis of a Handwritten Signature Verification Technique. *B.Sc Thesis,* James Cook University.

Mighell, D. A., Wilkinson, T. S., and Goodman, J. W. (1989). Backpropagation and its Application to handwritten Signature Verification, *Advances in Neural Information Processing Systems 1*, 340-347.

Musa Md. Lazim, Mohd. Noor Md. Sap and Dzulkifli Mohamad (1990). Pengecaman Tulisan Tangan: Keperluan Sistem dan Satu Pendekatan Terhadap Penyelesaian Deterministik, *Jurnal Teknologi Maklumat*, Vol. 1, No. 1, 44-53.

Nelson, W., Turin, W., and Hastie, T. (1994). Statistical Methods for On-line Signature Verification, *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 8, No. 3, 749-770.

Plamondon, R. (1994). The Design of an On-line Signature Verification System: From Theory to Practice, *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 8, No. 3, 795-811.

Schenkel, M., Guyon, I., and Henderson, D. (1995). On-line cursive script recognition using time delay neural networks and hidden Markov models, *Machine Vision and Applications*, 215-223.

Schomaker, L., Abbink, G., and Selen, S. (1994). Writer and Writing-Style Classification in the Recognition of Online Handwriting, *Proceedings of the European Workshop on Handwriting Analysis and Recognition: A European Perspective*, 12-13, London: The Institution of Electrical Engineers.

Seiler, R., Schenkel, M., and Eggiman, F. (1994). Off-line Cursive Handwriting Recognition Compared with On-line Recognition, *Technical Report*, Swiss Federal Institute of Technology: Zurich

Seni, G. (1995). Large Vocabulary Recognition of On-line Handwritten Cursive Words, *Ph.D. Dissertation*, State University.

Senior, A. W. (1994). Off-line Cursive Handwriting Recognition Using Recurrent Neural Networks, *Ph.D. Dissertation*, Cambridge University.

Tay, Y. H., and Khalid, M. (1999). Two-cost stroke segment grouping mechanism for off-line cursive hand-written word recognition, *In Proceedings the first national conferences on Artificial Intelligence applications in industry,* Kuala Lumpur, SIRIM Berhad, 36-46.

U.S. Department of Health and Human Services (1992). *Progress Report-February 24, 1992,* U.S: Food and Drug Administration.

Yoshimura, I., and Yoshimura, M. (1994). Off-line Verification of Japanese Signatures After Elimination of Background Patterns, *International Journal of Pattern Recognition and Artificial Intelligence,* Vol. 8, No. 3, 692-708