Malaysian Journal of Computer Science, Vol. 9 No. 1, June 1996, pp. 37-41

ENHANCING THE PERSONAL IDENTIFICATION NUMBER INPUT AS A MEANS OF IDENTIFICATION SIGNATURE

Elok Robert Tee
Jabatan Sains Komputer
Universiti Pertanian Malaysia
43400 Serdang
Selangor D. E.
Malaysia
email: ertmakh@pop.jaring.my

N. Selvanathan
Fak. Sains Komputer & Teknologi Maklumat
Universiti Malaya
50603 Kuala Lumpur
Malaysia
email: selva@fsktm.um.edu.my

ABSTRACT

The process of typing the personal identification number (PIN) can be broken down into quantifiable components, such as latency time, keypress force, keypress duration and keypress displacement which can be evaluated and used to verify the identity of a person. The keypress pattern is called the PIN signature. As the PIN signature is like the written signature that differs slightly with every execution, a neural-fuzzy application is devised to verify the PIN signature input against the reference profile.

Keywords: ***PIN, PIN signature, artificial neural networks, fuzzy logic***

1.0 INTRODUCTION

The PIN is a sequence of confidential numbers used by a computer system for verification of identification [1], commonly used for cash- and credit cards over automated teller machines (ATM) or at point-of-sale (POS) terminals. There are few standards governing its proper use in terms of PIN management and security - notably the ANSI/ABA X9.8 and ISO 9564 standards [2, 3] which are adopted by the financial industry in the USA. These standards govern the production, storage, verification and other matters pertaining to the use of the PIN.

The PIN is used for a variety of identification purposes, such as:

- balloting, survey, services and information access via the telephone [4]
- telephone cards [5]
- electronic cash cards such as used by the University of Michigan students *M-Card* [6]
- multipurpose electronic identification card, *Unicard*, from the Unicard Consortium [7]

Adequate security measures are employed to transmit the PIN from the input terminal to the host for validation such as compliance to the Data Encryption Standard (DES) [8, 9]. However, the PIN can be stolen from a user by mere observation of its input and there is no effective way of casting doubt on the transaction, as presently the computer system has no means of verifying the validity of the user of the PIN.

As an enhancement to PIN input, the *PIN signature* is proposed [10]. This paper defines the PIN signature and presents a possible verification mechanism for PIN input using a simple neuro-fuzzy application.

2.0 THE PIN SIGNATURE

The action of typing the PIN sequence constitutes a pattern, which is similar to written signature. This pattern can be broken down into its component parts which can then be used in authentication of the identity of an individual.

The PIN signature is achieved through remembering and typing the PIN sequence as a series of attached and detached digits. For example, a 6 digit PIN *738831* may be memorized as "*seven-three, eight-eight-three-one*" or as "*seven-three-eight, eight-three-one*". The keys are consequently pressed subconsciously in this manner.

Like written signature, the PIN signature pattern is not always consistent and may be slightly different each time it is typed. As such, a method of typing the PIN sequence needs to be devised to ensure minimal measurable deviation.

Consistent input requires the mapping of the fingers with respect to the numeric keypad. This includes consistent placement of the right hand and the limiting of fingers to a specific set of numeric keys.

Table 1: Mapping fingers to the numeric keypad

Finger	Key mapped
Thumb	[0]
1st	[1] [4] [7]
2nd	[2] [5] [8]
3rd	[3] [6] [9]
4th	[Enter]

Table 1 is biased towards those who are right-handed. For the left-handed, the fingers are mapped in reverse order with the thumb on the [Enter] key and the 4th finger kept free. The 1st and 2nd fingers are mapped onto the [0] key. The fingers are restricted to these pre-assigned keys.

In this experiment, artificial neural networks (ANN) and fuzzy logic are utilized for the verification process because of the reliable properties of pattern recognition and non-linear computation, which are highly adaptive to possible variations [11, 12, 13].

Table 2: Alternative mapping of fingers to the numeric keypad.

Finger	Key mapped
Thumb	free
1st	[1] [4] [7] [0]
2nd	[2] [5] [8] [0]
3rd	[3] [6] [9] [Enter]
4th	free

The thumb and little finger are not utilized in this configuration.

3.0 METHODOLOGY

The PIN signature can be broken down into the following components [10]:

- key value
- reaction time - first keypress after the prompt to input is displayed on screen
- latency time - time between keypress
- completion time - total time taken to complete typing the digits
- keypress duration - the duration of time a key is kept held down
- key displacement - the depth the key is pressed down
- keypress force
- rate of keypress release
- rate of keypress force discharge
- average rate of keypress overrun, i.e. touching the adjacent key when typing

For the purpose of this experiment, 4 of the above parameters were selected based on the possibility of obtaining the measurements.

1. *latency time*
2. *keypress force*
3. *keypress duration*
4. *keypress displacement*

A *C* program compiled using Borland C++ was used to measure the latency time using an IBM compatible machine. The latency time is measured from the instance an input prompt appears on the display. The figures for the last 3 parameters were randomly generated as the special hardware needed to measure these parameters were not available. It is envisaged that it is possible to measure these parameters based on the model of touch sensitive keys of electric pianos [14].

Fuzzy rule matrix tables [15, 16] were designed using the chosen parameters to determine if the parameter values are acceptable. The membership function of the 4 selected parameters was set at 10% variance ± from the average values of 20 PIN signature samples.

The fuzzy rule matrix tables are:

1. *Latency-Displacement*
2. *Latency-Duration*
3. *Latency-Force*
4. *Force-Displacement*
5. *Force-Duration*
6. *Displacement-Duration*

Four invalid- and 4 valid input samples were created as determined by the fuzzy rule matrix tables to train the ANN. The invalid samples are used to indicate unacceptable limits of input while the valid samples indicate the acceptable limits of input. A total of 4 user PIN signature profiles were generated and tested on the ANN one at a time. Impostor samples of similar and dissimilar PIN signature patterns were utilised.

3.1 Fuzzy rule matrix tables

Note: The legend used for the description of the fuzzy rule matrices throughout are:

- `N` negative deviation from zero.
- `SN` small negative deviation from zero
- `Z` zero
- `SP` small positive deviation from zero
- `P` positive deviation from zero.
- `No` cause the system to *`Reject`* input
- `Yes` cause the system to *`Accept`* input
- `SoSo` indicates an *`Uncertain`* input

latency time \ keypress displacement	N	SN	Z	SP	P
N	No	No	No	No	No
SN	No	SoSo	**Yes**	SoSo	No
Z	SoSo	**Yes**	**Yes**	**Yes**	SoSo
SP	No	SoSo	**Yes**	SoSo	No
P	No	No	No	No	No

Fig. 1: Latency-Displacement fuzzy rule matrix table

The latency-displacement fuzzy rule matrix permits the system to accept a deviated keypress displacement value because the key displacement is dependent on the distance, condition and strength of the finger, hence, the force applied.

A small deviation (SN or SP) will return Yes while a greater deviation (N or P) will return SoSo which is an *Uncertain* result. A latency time deviation greater than SN or SP will invalidate outright the PIN signature, although the key displacement may be accurate.

latency time \ keypress duration	N	SN	Z	SP	P
N	No	No	No	No	No
SN	No	SoSo	**Yes**	SoSo	No
Z	No	**Yes**	**Yes**	**Yes**	No
SP	No	SoSo	**Yes**	SoSo	No
P	No	No	No	No	No

Fig. 2: Latency-Duration fuzzy rule matrix table

The system will *Accept* a small deviation (SN or SP) with an accurate match (Z) of either parameter (see Fig. 2). A small deviation of both parameters will return the *Uncertain* result. A greater deviation from SN or SP will invalidate the PIN signature.

latency time \ keypress force	N	SN	Z	SP	P
N	No	No	No	No	No
SN	No	SoSo	**Yes**	SoSo	No
Z	No	**Yes**	**Yes**	**Yes**	**SoSo**
SP	No	SoSo	**Yes**	SoSo	No
P	No	No	No	No	No

Fig. 3: Latency-Force fuzzy rule matrix table.

The system will *Accept* a small deviation (SN or SP) with an accurate match (Z) of either parameter. A small deviation of both parameters will return the *Uncertain* result. A greater deviation from SN or SP will invalidate the PIN signature; the exception is a positive increase in keypress force with an accurate match in latency time.

force \ keypress displacement	N	SN	Z	SP	P
N	No	No	No	No	No
SN	No	**SoSo**	**Yes**	No	No
Z	No	**Yes**	**Yes**	**Yes**	No
SP	No	No	**Yes**	**SoSo**	No
P	No	No	No	No	No

Fig. 4: Force-Displacement fuzzy rule matrix table

The system will *Accept* a small deviation (SN or SP) with an accurate match (Z) of either parameter. A small increase or decrease in keypress force will displace the key in a similar direction but not otherwise. The following relationship is not possible:

SP force - SN displacement
SN force - SP displacement

force \ keypress duration	N	SN	Z	SP	P
N	No	No	No	No	No
SN	No	SoSo	**Yes**	SoSo	No
Z	No	**Yes**	**Yes**	**Yes**	No
SP	No	SoSo	**Yes**	SoSo	No
P	No	No	No	No	No

Fig. 5: Force-Duration fuzzy rule matrix table

The system will *Accept* a small deviation (SN or SP) with an accurate match (Z) of either parameter. A small deviation of both parameters will return the *Uncertain* result. A greater deviation from SN or SP will invalidate the PIN signature.

displacement \ keypress duration	N	SN	Z	SP	P
N	No	No	No	No	No
SN	No	SoSo	SoSo	SoSo	No
Z	No	SoSo	**Yes**	**Yes**	No
SP	No	SoSo	**Yes**	**Yes**	No
P	No	No	No	No	No

Fig. 6: Displacement-Duration fuzzy rule matrix table

The system will *Accept* a small positive deviation of either parameter. A small deviation of the remaining matrices of both parameters will return the *Uncertain* result. A greater deviation from SN or SP will invalidate the PIN signature.

3.2 Neuro-fuzzy application model

The ANN application was customised using the HNC Multiple Back Propagation Network (MBPN) package [17]. The application was configured with 24 input nodes for a 6-digit PIN sequence model, a hidden slab size of 12, and 3 output nodes to indicate the verification result:

- 1 - *Accept*
- 0 - *Reject*
- 2 - *Uncertain*.

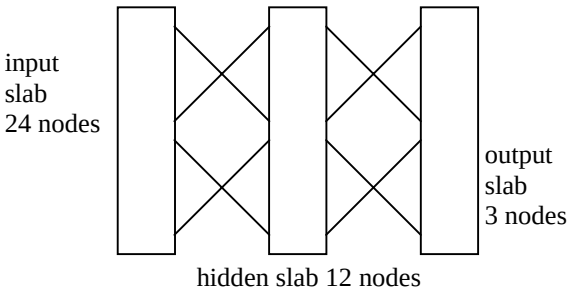

Fig. 7: Schematic of backpropagation neuro-fuzzy model.

4.0 FINDINGS AND LIMITATION

The ANN was trained separately for each user and tested with samples that include impostor samples. A total of 50 samples from each user was tested. A further 10 impostor samples with similar and dissimilar PIN signature patterns were also compared. The acceptance rate are tabulated below:

Table 3: Acceptance rate

	actual	impostor similar pattern	impostor dissimilar pattern
User 1	78.37	20.57	0.00
User 2	71.16	6.42	0.00
User 3	64.67	5.62	0.00
User 4	73.06	10.28	0.00
avg.	71.82	10.72	0.00
var.	5.6568	6.8730	-

The False Rejection Rate (FRR) was 28.18% for authentic users while the False Acceptance Rate (FAR) was 10.72% for impostors with similar pattern. All impostors with dissimilar pattern signatures were identified.

The results are encouraging, however, the simulated values for the keypress force, duration and displacement parameters as well as the different ANN architectures and training algorithms available should warrant further investigation.

5.0 SUMMARY

We have demonstrated that it is possible to implement the PIN signature using a simplified neural-fuzzy model for verification. This approach using neuro-fuzzy differs from the patented Young and Hammon (1989) digraph method of measuring keystrokes for user authentication [18. 19]. The latency time measurement considers only the time taken between each keypress. It does not take into consideration the time of the previous key which was released. The possible measurement of other parameters strengthens the evaluation of the PIN signature pattern.

Like the written signature, the individual has to remember and practise typing the PIN signature to ensure minimal deviation from the usual pattern. This approach of using the keyboard may have limitations for those with physical disabilities.

The proposed PIN signature also requires special keyboard hardware which is touch sensitive yet durable to measure the action of the hand.

The PIN signature offers additional security against theft. A possible implementation of the PIN signature is to incorporate the program in the smart card. The program could cast doubt on an impostor during the instance of input as the system does not have to check the personal dossier for transaction irregularities [7].

REFERENCES

[1] The University of Illinois at Chicago, “Personal Identification Number (PIN)”. *http://www.uic.edu/depts/oar/reg14.htm*, 1995.

[2] ANSI, “ANSI X9.8-1982 (R1991) Personal Identification Number Management and Security”, catalog search: *http://www.ansi.org/cat_c.html*, 1995.

[3] ISO, "ISO 9564-1:1991 Banking -- Personal Identification Number management and security", 2 parts: *http://www.iso.ch/cate/d17309.html, ..d17310.html,* 1995.

[4] MT&T Technologies Inc., "Teledemocracy", *http://www.mtt.ns.ca/info/teledemo.html,* 1995.

[5] A. Cohen, FAQ: rec.collecting.phonecards, 1995.

[6] University of Michigan, "M-CARD An Economic Analysis". *http://www.personal.umich.edu/~ko-vacs/mcard.html,* 1994.

[7] J. Walker, "Unicard". *http://www.formilab.ch/documents/unicard.doc,* 1994.

[8] RSA Laboratories, FAQ: "DES". *http://www.rsa.com/rsalabs/faq/faq_des.html,* 1995.

[9] RSA Laboratories, FAQ: "Key Management". *http://www.rsa.com/rsalabs/faq/faq_km.html,* 1995.

[10] E.R. Tee and Selvanathan N., "PIN Signature: A New Approach to Signature Identification", revised, being reviewed: Journal of Information Technology, 1996.

[11] D. Hammerstrom, "Working with Neural Networks". IEEE Spectrum, July 1993, pp. 46-53.

[12] T. Masters, "Practical Neural Network Recipes in C++". Academic Press, Inc., 1993

[13] L. Prechelt, neural-net-faq: *http://www.ipd.ira.uka.de/prechelt/FAQ/neural-net-faq.html*, 1995.

[14] Yamaha Corporation: Clavinova, Portatone "Action Effect" keyboard technology, brochures and technical papers. 1995.

[15] F.M. McNeill & E. Thro, "Fuzzy Logic A Practical Approach", Academic Press, Inc., 1994, pp. 57-70.

[16] E. Cox, "The Fuzzy Systems Handbook A Practitioner's Guide to Building, Using, and Maintaining Fuzzy Systems". AP Professional, 1994.

[17] HNC Incorporated, "HNC KnowledgeNet Release 2.11" manual, 1991.

[18] J. R. Young and R.W. Hammon, "Method and apparatus for verifying an individual's identity", US Patent Abstract: *http://sunsite.unc.edu/patbin/getabs?PTNO=4805222*, 1995.

[19] J. Rogers, "Neural Network User Authentication". AI Expert, June 1995, pp. 29-33.

BIOGRAPHY

Elok Robert Tee is a Tutor at the Universiti Pertanian Malaysia and is currently writing for his Master in Computer Science at the Universiti Malaya.

Dr. N. Selvanathan is the Deputy Dean of the Faculty of Computer Science and Information Technology, Universiti Malaya.