where $\bar{S}$ is the sample feature vector of components Si (i=1 to f) and Ti is the true (reference) feature mean value of variance Vi.

This distance measure requires only five to ten true signatures to establish initial values for user behaviour statistics at enrolment.
The 'best' feature set selected as standard by the above method contained features: 1, 2, 3, 6, 11, 12, 13, 14, 16, 20, 22, 25, 26, 27, 28, 29, 30, 32, 33, 40, 41, 42, 43 and 44. 24 features in all.

REFERENCES

[1] Masuyama, H. (1985) 'Properties of personal identification systems using question–answer techniques' *Trans Int Electronics and Communications Engineering* J69D/4, 613–620.
[2] Kniessler, H. (1985) *Identification of individuals with computer graphics* SRI Report, SRI International Inc.
[3] Harmon, L. D., Khan, M. K., Lasch, R. and Ramig, P. F. (1981) 'Machine identification of human faces' *Pattern Recognition* **13**(2) 97–110.
[4] Siemens, A. G. (1982) *Fingerprint personal identification system* DE 3036 912. 13 May 1982.
[5] Asai Koh (1980) *Device for extracting a density as one of a number of pattern features extracted for each feature point* ... GB 2050026. 31 Dec 1980. *Nippon Electric Co Ltd.*
[6] Sparrow, M. K. and Sparrow, P. J. (1985) *A Topological approach to the Matching of Single Fingerprints* US Dept of Commerce, NBS. Oct. 1985.
[7] Isenor, D. K. and Zaky, S. G. (1986) 'Fingerprint identification using graph matching' *Pattern Recognition* **19**(2) 113–122.
[8] Sibany Mfg. Corp. (1966) *Recognising fingerprints* GB 1150511. 29 April 1966.
[9] Stellar Systems Inc. (1983) *Personnel identification system using characteristic data* US Au8335163. 31 March 1983.
[10] Fowler, R. C., Ruby, K., Sartor, F. F. and Sartor, T. F. (1985) *Fingerprint Imaging Apparatus* US 4537484. 27 Aug 1985. Identix Inc, Palo Alto, Ca.
[11] Fingermatrix Inc. (1984) *Fast action fingerprint check for access control* US EP125–532. 21 Nov 1984.
[12] IBM Corp. (1979) *Palm print identifier* GB 1535467.
[13] Palmguard Inc. (1982) *Image recognition system for recognising human palm.* US 4186378. 20 Jan 1982.
[14] Stellar Systems Inc. (1984) *Personnel Identification Devices Using Hand Measurement Techniques* April, 1984.
[15] Mitsubishi Denki K. K. (1985) *Individual identification apparatus based on finger length comparison* JP EP132665A. 13 Feb 1985.
[16] Zuccarelli, H. (1983) 'Ears hear by making sounds' *New Scientist* **100** BPC.
[17] EYE-D Developments II Ltd (1984) *Ocular fundus reflectivity pattern identification apparatus* US EP126549A. 28 Nov 1984.
[18] Rice, J. (1986) *Method of, and Apparatus for the Identification of Individuals* UK 8509389 86.

[19] Abberton, E. and Fourcin, A. J. (1978) 'Intonation and speaker identification' *Language & Speech* **21**(4) 305.
[20] Bolt, R. H., Cooper, F. S., David Jr, E. E. and Denes, P. B. (1973) 'Speaker identification by speech spectrograms: some further observations' *JASA* **54**(2) 531–537. Acoustic Society of America.
[21] Holden, A. D. C. and Cheung, J. Y. (1977) The role of idiosyncracies in linguistic stress cues, and accurate formant analysis, in Speaker Identification *Carnahan Conference 1977*, University of Kentucky, 33–37.
[22] McGlone, R. E. and Hollien, H. (1976) 'Partial analysis of acoustic signal of stressed and unstressed speech' *Carnahan Conference*, University of Kentucky, 19
[23] Davis, R. L., Sinnamon, J. T. and Cox, D. L. (1982) *Voice verification upgrade*. Report Texas Instruments Inc.
[24] Rosenberg, A. E. (1976) 'Automatic speaker verification: a review' *Proc IEEE* **64**(4) 475–487.
[25] DeGeorge, M. (1981) 'Experiments in automatic speaker verification' *Carnahan Conference 1981*, University of Kentucky, 103–110.
[26] Bunge, E., Hofker, U., Hohne, H. D. and Kriener, B. (1977) 'Report about speaker-recognition investigations with the AUROS system' *Frequenz* **31**(12) 382.
[27] Kuhn, M. H. and Geppert, R. (1980) 'A low cost speaker verification device' *Carnahan Conf 1980*, University of Kentucky, 57–61.
[28] Ney, H. and Gierloff, R. (1982) 'Speaker recognition using a weighting technique' *IEEE Int. Conf. on Acoustics, Speech and Signal Processing* 1645–1648
[29] IBM Corp. (1967) *Speech recognition* GB 1179029. 19 April 1967.
[30] Perkin Elmer Corp. (1970) *Speech recognition* GB 1289202. 21 April 1970.
[31] NCR Corp (1977) *Verification* GB 1532944. 21 Feb 1977.
[32] Kashyap, R. L. 'Speaker recognition from an unknown utterance and speaker-speech interaction' *Tr Acou. Speech & Signal Processing ASSP* **24**(6) 451.
[33] Tokyo Shibaura Denki (1983) *Individual verification apparatus based on speech recognition* JP EP-86–064. 27 Jan 1983.
[34] Reitboeck, H. J. (1977). 'Speaker identification over telephone transmission channels' *Carnahan 1977*, University of Kentucky, 237–238.
[35] Shridhar, M., Baraniecki, M. and Mohankrishnan, N. (1982) 'A unified approach to speaker verification with noisy speech input' *Speech Communication* 103–112.
[36] Kiyohiro, S. (1985) *Text-Independent Speaker Recognition Experiments using Codebook* Computer Science Dept C-M U, 9 April 1985.
[37] Moore, R. K. 'Systems for isolated and connected word recognition' *NATO ASI* **16** 74–143 Springer-Verlag.
[38] Nagel, R. N. and Rosenfeld, A. (1977) 'Computer detection of freehand forgeries' *Trans on Computers* **C 26**(9) 895.
[39] Rediffusion Computers Ltd (1983) 'Rediffusion introduces low-cost signature verifier' *Financial Times* 24 Feb 1983, 19.
[40] Chainer, T. J., Scranton, R. A. and Worthington T. K. (1985) *Data input pen for signature verification* US 4513437. 23 April 1985.
[41] Crane, H. D. and Ostrem, J. S. (1983) 'Automatic signature verification

using a three-axis force-sensitive pen' *Trans on Sys., Man & Cybernet* **SMC-13**(3) 329–337.

[42] Quest Automation Ltd (1979) *Transducer pad for electrographics* GB 1539755.

[43] Greenaway, D. L. (1978) *Apparatus and Method for Producing an Electrical Signal Responsive to Handwriting Characteristics* US 4122435. 24 Oct 1978.

[44] Darringer, J. A., Denil, N. J. and Evangelisti, C. J. (1975) 'Speed pen' *IBM Tech Disclosure Bulletin* **18**(7) 2374–5.

[45] Radice, P. F. (1980) *Personal Verification Device* US 4234868. 18 Nov 1980.

[46] Worthington, T. K., Chainer T. J., Williford, J. D. and Gundersen, S. C. (1985) 'IBM dynamic signature verification' *Computer Security*, Elsevier Science Publishers BV, 129–54.

[47] Zimmermann, K. P. and Varady, M. J. 'Handwriter, identification from one-bit quantized pressure patterns' *Pattern Recognition* **18**[1] 63–72.

[48] Hale, W. J. and Paganini, B. J. (1980) 'An automatic personal verification system based on signature writing habits' *Carnahan Conf. on Crime Counter*, University of Kentucky, 121–125.

[49] Stuckert, P. E. (1979) 'Magnetic pen and tablet' *IBM Technical Disclosure Bul* **22**(3) 1245–1251.

[50] de Bruyne, P. (1984) 'An ultrasonic radar graphic input tablet' *Scienta Electrica* 1–26.

[51] Lew, J. S. (1980). 'Optimal accelerometer layouts for data recovery in signature verification' *IBM Journal of R & D* **24**(4) 496–511.

[52] Herbst, N. M. and Liu, C. N. (1977) 'Automatic signature verification based on accelerometry' *IBM Jour of R & D* 245.

[53] Liu, C. N., Herbst, N. M. and Anthony, N. J. (1979) 'Automatic signature verification: system description and field test results' *TR Sys., Man & Cybernetics* **SNC 9**(1) 35.

[54] de Bruyne, P. (1977) 'Developments in signature verification' *Int Conf on Crime Countermeasure*, Oxford Univ.

[55] Watson, R. S. and Pobgee, P. J. (1980) 'A computer to check signatures' *Visible Language* **13**(3).

[56] Fox, P. F. (1982) 'A practical method of personal identification by signature validation' *IACSS Conference*, Zurich, Switzerland.

[57] Umphress, D. and Williams, G. (1985) 'Identity verification through keyboard characteristics' *Int J Man-Machine Studies* 263–273.

[58] Haberman, W. and Fejfar, A. (1976) 'Automatic identification of personnel through, speaker and signature verification – system design and testing' *Carnahan Conference 1976*, University of Kentucky, 23–30.

Chapter 8

Cryptography and the Smart Card

D. W. DAVIES

(Data Security Consultant)

Cryptology is the key technology for secure systems.

8.1 Introduction

The close relationship between smart card and cryptographic techniques can be looked at from two directions. The smart card can be used as a component of a cryptographic system to improve its convenience or level of security. From the other viewpoint, the smart card itself is the main component of the system and cryptography is called upon to help it with its task. In this chapter we shall mainly adopt the second viewpoint, which is centred on smart card applications but first let us look at the smart card as an adjunct to cryptography.

The confidentiality of data on a communication line can be protected by enciphering it. Encipherment is a transformation which makes the transformed data seem meaningless to an outsider, yet which allows an inverse transformation, for those authorised to receive the information, which turns it back into its clear text. To separate the authorised readers from others, the authorised readers hold a secret value called a *cryptographic key* without which decipherment is impossible. In the usual form of cryptography, this secret key is used as a parameter for both the encipherment and the decipherment functions.

When cryptography is used to protect data travelling some distance, before it can go into operation a secret key must be established at both the sending and the receiving end. Conveying the key from one place to the other entails a risk of losing it to an opponent. A smart card can be used to store a key for secure transport. The use of this key can be authorised by means of a password, known only to authorised users, and the smart card itself can take part in the complex process of key management. Some of the techniques are described later in the chapter.

Sometimes, cryptography is used to encipher information not for communications purposes but to protect it while it is stored locally. It might be difficult to protect the local store from illicit access or information stored on a removable medium might be stolen or copied. When cryptography is used for stored data, the keys are not transported but their security is very important because they can unlock all the protection provided. Most computers are physically insecure, so a smart card can be used to hold the keys and the card taken away by its owner and stored in a safe place. Here also, a password can be used to unlock the secret key from the card.

A related problem of cryptography is the protection of the cryptographic mechanism itself. Not only must the key be protected but also the place where the cryptographic transformations take place. Smart cards can help in this problem by becoming, themselves, the 'cryptographic engine' of the system. If they have enough processing power for the purpose, they can hold all the protective mechanism of a secure system, particularly at the terminal end where the processing demands are less severe. The computer itself, which might be an intelligent terminal, is physically insecure and any part of its store or process is open to tapping or 'bugging'. To counter this, cryptographic methods are used and the keys, together with the cryptographic transformations, are contained entirely in smart cards. When these are removed, the system is locked up and the information it contains is safe against illegal access.

These are examples of the close relationship between smart cards and cryptography, seen from the side of the cryptographer who regards the smart card as an additional tool. Our viewpoint in the rest of this chapter is to think of the smart card as a main component of the system and see how cryptographic techniques are used for its purpose.

8.2 PROTECTION FROM PASSIVE AND ACTIVE ATTACKS

Cryptographic techniques can be used in a large number of ways and for many different purposes. The basic purpose is to protect a system against misuse by impostors or unauthorised people. The first stage in protecting a system is to analyse the threats to the system and the risks they entail. We shall consider only those threats that are amenable to cryptographic protection and, as a first step we divide these into *passive* and *active* attacks.

A passive attack attempts to read information without changing it. Examples are the tapping of a telephone line, stealing or copying a diskette, observing a password by looking at the keyboard while it is entered or picking up stray electromagnetic radiation from which a meaningful signal can be reconstructed. Generally speaking, these attacks are not difficult to carry out and in a widespread communication network it is impossible to prevent them. The tapping or bugging of voice conversations is a highly developed art which can be applied (with a few

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.