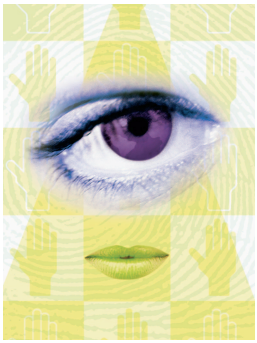
Qinghan Xiao
Defense Research and Development, CANADA

Technology Review

Biometrics—Technology, Application, Challenge, and Computational Intelligence Solutions

I. Introduction

Since the September 11th terrorist attacks, there has been an increased focus on biometrics as the solution to a wide range of problems. An increasing number of countries have decided to adopt biometric systems for national security and identity theft prevention. This trend makes biometrics an important component in security-related applications such as: logical and physical access control, forensic investigation, IT security, identity fraud protection, and terrorist prevention or detection.


© EYEWIRE

Biometrics is the science of the measurement of unique human characteristics, both physical and behavioral. Various biometric technologies are available for identifying or verifying an individual by measuring fingerprint, hand, face, signature, voice, or a combination of these traits. New biometric algorithms and technologies are proposed, tested, reviewed, and implemented every year.

Because a biometric trait cannot be captured in precisely the same way twice, biometric matching is never exact. The matching is always a "fuzzy comparison". This feature makes computational intelligence (CI), primarily based on artificial intelligence, neural networks, fuzzy logic, evolutionary computing, etc., an ideal approach for solving different biometric problems. In recent years, use of CI techniques has increased in biometric authentication and identification. In particular, CI approaches that perform face detection and recognition, iris processing, speech verification, speaker recognition, handwriting and signature recognition, and odor source localization were presented at the 2006 IEEE World Congress on Computational Intelligence (WCCI).

This paper aims to assist readers as they consider biometric solutions by examining common biometric technologies, introducing different biometric applications, and reviewing recent CI solutions presented at the 2006 IEEE WCCI. The remainder of the paper is organized in the following manner: Section II provides a general overview of biometrics and biometric systems. It also illustrates the difference between authentication and identification. Section III shows the broad array of biometric applications in a variety of areas ranging from enhancing national security to countering identity fraud. Section IV provides two approaches for dealing with technical and legal challenges: anti-spoofing technology and two-way authentication strategy. Section V discusses the cost issues involved in implementation of biometric technology. The CI-based biometrics solutions presented at the 2006 IEEE WCCI are reviewed in Section VI. Finally, Section VII sets out the conclusions.

II. Biometrics and Biometric Systems

The word biometrics is a combination of the Greek words *bio* and *metric*. When combined, it means "life measurement." Biometric technology refers to any technique that reliably uses measurable physiological or behavioral characteristics to distinguish one person from another. Common physiological biometric traits include: fingerprints, hand geometry, retina, iris, and facial images. Whereas, common behavioral biometric traits include: signature, voice recordings, and keystroke rhythms. It should be noted that behavioral biometrics generally include a physiological component as well.

Practically, all biometric systems work in the same manner. The first process is called enrollment in which each new user is registered into a database. Information about a certain characteristic of the person is captured. This information is usually passed through an algorithm that turns the information into a template that the database stores. Note that it is the template that is maintained in the system, but not the original biometric measurement as many people may suspect. Compared with the original measurement of the biometric trait, the template has a very small amount of information; it is no more than a collection of numbers with little meaning except to the biometric system that produced them. When a person needs to be recognized, the system will take the appropriate measurement, translate this information into a template

1556-603X/07/$25.00©2007IEEE

using the same algorithm that the original template was computed with, and then compare the new template with the database to determine if there is a match, and hence, either an authentication or identification (Figure 1).

An important distinction between biometric authentication and identification lies in that authentication is a one-to-one comparison, while identification is a one-to-many search in a database. They perform different functions since authentication is used to confirm one's identity and identification is used to find one's identity.

III. Biometric Applications

With increasing security requirements, improving system performance, and decreasing costs, we are seeing more and more biometric applications and systems used across broad sectors of society, such as the military, government, education, and business, for both physical and logical security.

A. Military

The US Department of Defence (DoD) is moving forward with its biometrics initiative. It is exploring whether commercial security products and services are the answer to DoD biometrics needs. The DoD has established its Biometrics Management Office (BMO) to ensure the availability of biometric technologies within the Department. In addition, the DoD has set up its first biometric testing laboratory, the Biometrics Fusion Center (BFC), which will scientifically test, evaluate, and formulate recommendations for hundreds of commercial biometrics products. On 23 September 2004, the BMO awarded Lockheed Martin a five-year contract to design, build, and maintain a new Automated Biometric Identification System (ABIS). This electronic database with its associated set of software applications will consolidate, store, and search fingerprint data collected from persons of interest with respect to national security. Over time, ABIS will support the storage, query, and retrieval of additional biometric modalities such as facial image, iris image, voiceprint and DNA information [1], [2].

B. Biometric Passport

After the terrorist attacks of 11 September 2001, security concerns played an even more important role in border protection, passport fraud, and forgery for many nations. One way to enhance passport security is to include biometrics—the International Civil Aviation Organization has proposed using the face as the primary biometric with fingerprint or iris as an optional secondary measurement [3]. Designs for the new biometric passport (sometimes known as BioPass or ePassport) commonly include an embedded Radio Frequency Identification (RFID) chip carrying the same data that is printed on the data page as well as the passport holder's biometric identifiers. While these applications should be tamper-resistant, Lukas Grunwald, a consultant with a German security company, recently demonstrated the cloning of a biometric passport [4]. He was successful in his demonstrations as the security details of the ePassport system documented in the ICAO standards are publicly available. The ePassport, as a type of RFID, was found to be vulnerable to skimming and eavesdropping.

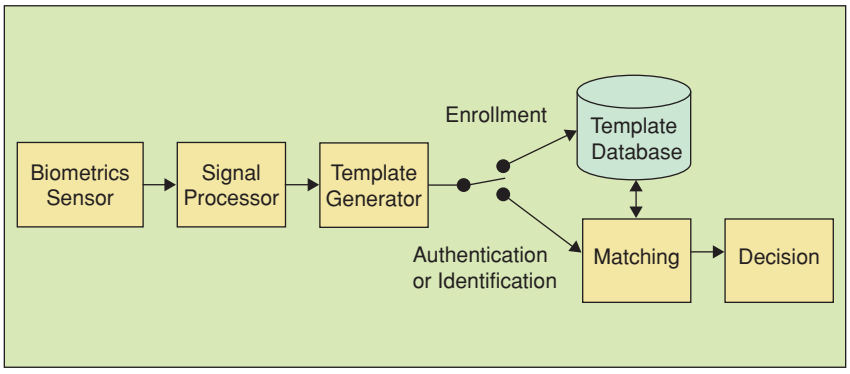


FIGURE 1 A generic biometric system.

C. Airport Security

A further example of the successful implementation of biometrics is the Ben Gurion International Airport in Tel Aviv, Israel, one of the world's busiest air terminals. A hand geometry system, which is included in 21 automatic inspection kiosks throughout the airport, is being used to identify travellers [5]. All passengers at Ben Gurion now go through these kiosks. During enrollment, the system captures biographic information and hand geometry data. When they arrive or depart, passengers use an ID card for initial identification, and the system verifies their identity with the hand geometry template. If verified, the system prints a receipt to allow travellers to proceed. Otherwise, they are referred to an inspector.

D. Financial Transactions

A growing number of banks and retail stores are strongly considering using biometric technology as a more efficient and secure method to combat fraud and identity theft. Bank United was the first bank in the United States to implement iris recognition at Automated Teller Machines (ATMs) in 1999. Thousands of consumers were able to withdraw cash from their accounts at the ATM just by looking at it. At the ATM, the customer's iris can be captured even through glasses, contact lenses, and most sunglasses.

The Japanese banking industry has been a pioneer in deploying biometric systems for security, privacy and customer service. The Big Four banks in Japan have adopted biometrics as a solution to the growing problem of ATM card forgery and ID theft in the wake of a recent scandal. Two of these banks have chosen a "palm vein" authentication technology, while the other two have elected to use a "finger vein" system. The rate of biometric technology adoption has grown extensively in Japan.

As of December 2005, fifteen financial institutions had announced the introduction of biometric bank cards [6].

IV. Challenges

A. Spoofing

Biometric systems are vulnerable to attacks and can be compromised at various stages (Figure 2) as other information systems. Biometric systems are susceptible to some common attacks such as: denial of service, spoofing, and man in the middle. While most IT systems are vulnerable to these attacks in general, biometric systems are especially vulnerable to spoofing.

Spoofing is an attack where a malicious individual pretends to be someone else. In biometrics, spoofing is a process that defeats a biometric system by providing a forged biometric copy of a legitimate user. Although spoofing techniques are different for each biometric technology, one thing common to all is that fake biometric samples are presented to the sensor [7]. Spoofing of physiological biometric technologies includes three stages: first, capturing the biometric sample belonging to the enrolled user; then, creating a copy of the captured sample by means of an artifact; and finally, using the artifact to attack the sensor. Mimicry is the most common method used to spoof behavioral biometric technologies.

B. Anti-Spoofing

Trying to overcome the spoofing vulnerability of biometric systems, several anti-spoofing techniques have recently been proposed and tested in both hardware and software. One method for anti-spoofing is called "liveness detection." It aims to add the ability to detect whether a biometric sample is being provided by a live human being or by a copy from an artifact. Liveness checks can be achieved through detecting physical properties of the live biometric, e.g. electrical measurement, thermal measurement, moisture, reflection or absorbance of light or other radiation; the presence of a natural spontaneous signal such as pulse; or the response to an external stimulus e.g. contraction of the pupil in response to light, muscular contraction in response to electrical signal etc.

Another major anti-spoofing approach is multi-modal biometric fusion, which combines several mono-modal biometric subsystems into one biometric system. In general, fusion can be performed at various levels, such as at the sensor level, matching score level, or decision level. It has been presented that fusion at the sensor level performs better than fusion at the other two levels [8]. The reason is obvious—the earlier the fusion is performed, the richer the information obtained. From an anti-spoofing point of view, a multi-modal biometric system increases the difficulty of spoofing because an impostor would have to break several biometric systems simultaneously for the spoof to succeed.

C. Privacy Protection

In April 2006, Unisys Corporation conducted a global survey that stated, "...many headlines today seem to question biometric adoption because of legitimate privacy concerns" [9]. It is clear that in order to make a biometric application successful, it is important to consider user resistance, such as fear of unfamiliar technology, invasion of privacy, etc. The major privacy concern is about the potential for mislaid biometric information and the danger of user profiles being used by government or other organizations for other purposes. Because user cooperation can have a great impact on accuracy, the attitude of users towards the intended biometric solution can make or break the implementation of a biometric system.

It has been reported that phishing attacks can pop up a login prompt imitating a trusted site on the victim's terminal. If the user does not recognize this as a fake prompt and inputs his or her login information, then his or her user name and password will be captured and no longer remain a secret. The same attack on a biometric authentication process has the possibility of capturing the user's biometric traits.

In order to solve this problem, a two-way authentication strategy is presented [10]. The user must not only be authenticated by the system, but a function must be developed to allow the user in turn to authenticate the system. The function works in the following manner. During the enrollment, the user is asked to select both password and personal "secret" greeting phrase. This secret phase will be encrypted with Public Key Infrastructure (PKI) encryption. When performing the user authentication, after the user's password is verified but before his or her biometric trait is inputted, the corresponding personal greeting will be displayed so that the user knows that he or she will be submitting the biometrics to the correct system. Not only does this solution increase the security level of the system, but also it makes the users feel confident that their biometrics are being collected by a system that they can trust.

V. Benefits and Costs

Cost is always an important issue when implementing a new technology. While

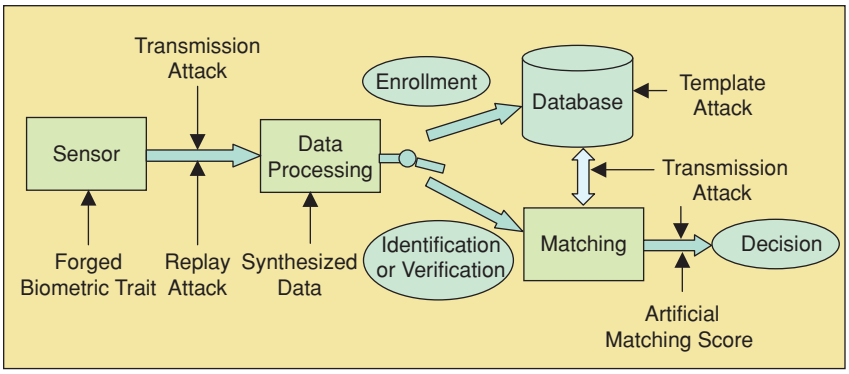


FIGURE 2 Attacks on biometric system.

examining the cost of a biometric application, people often focus uniquely on the cost of sensor hardware and associated software. However, the actual cost of implementing any biometric technology goes far beyond these basic elements. There are also costs associated with installation, integration, administration, user education, data collection, and system maintenance.

Another important consideration is to avoid falling into a trap because the vendors tend to tell one part of the story— the positive part, although in many respects, that is quite legitimate. Instead of positive news, a user needs to consider that

- A system sometimes needs modification to work
- An annual maintenance fee may have to be paid to keep the system in working order
- The system may be susceptible to the "patch and pray" problem

If possible, procurement should be based on the advice from an independent third party with credible expertise, such as a government biometrics laboratory, but avoid buying a biometric system on the basis of the vendor's product literature alone.

When doing the cost-benefit analysis for any proposed system, it should be noted that the cost-benefit analysis for a security-related project, such as biometrics, is different from that of a non-security-related project. A new component needs to be considered: the risk of attack. It can be defined as

$$\text{Risk}_{\text{Attack}} = \text{P}_{\text{Attack}} \times \text{Loss}_{\text{in attack}} \quad (1)$$

where P_{Attack} is the probability of attack and $\text{Loss}_{\text{in attack}}$ is the estimated loss in the attack represented by dollars.

In this way, we can calculate a value if the risk can be reduced when implementing a new technology.

$$\text{Reduced Risk} = (\text{P}_{\text{Attack old}} - \text{P}_{\text{Attacknew}}) \times \text{Loss}_{\text{in attack}} \quad (2)$$

Since the new and old technologies may not bring us the same benefits, the benefits can be expressed in terms of dollars as:

$$\text{Benefit} = \text{B}_{\text{Original}} + (\text{B}_{\text{Added}} - \text{B}_{\text{Lost}}) \quad (3)$$

The cost-benefit analysis will be evaluated by the following formula:

$$\textit{If } \text{Cost} \ll \text{Reduced Risk} + \text{Benefit}, \textit{ then } \text{implement} \quad (4)$$

In general, biometric technology, if implemented correctly, will enhance the system security level and significantly reduce the probability of a system being successfully breached.

VI. Recent CI-based Biometric Technology

Computational intelligence is a fast-moving research field with approaches primarily based on neural networks, machine learning, fuzzy logic, genetic algorithms and evolutionary computing. Computational intelligence methods have been applied to solve real-world complex problems including biometric authentication and identification. Recently, at the 2006 IEEE WCCI conference, various CI-based approaches, such as neural networks, fuzzy logic, particle swarm optimization (PSO), evolutionary algorithm (EA), boosting, and self organizing maps (SOMs), were presented in the areas of face detection, facial recognition, speech recognition, speaker verification, iris processing, handwriting and signature recognition, all of which will be described in this section.

A. Face Detection and Facial Recognition

Facial images are probably the most natural biometric measurement used by humans to make a personal identification. Face detection is the fundamental first step in any facial recognition system. It is the process of identifying human faces and eliminating background pixels in a captured image. The performance of the face detection algorithm will heavily affect the speed and accuracy of a facial recognition system. In general, face detection can be treated as a two-class pattern recognition problem with a "face" class and a "non-face" class. Since it is an established method for the optimization of the topology of neural networks, evolutionary algorithm has been proposed as an efficient tool for face detection [11]. Jang and Kim presented a fast face detection system using AdaBoost and a cascade structure as a basic framework [12].

Boosting refers to a general method of combining weak classifiers into highly accurate classifiers to improve the classification performance. The AdaBoost algorithm, introduced in 1995 by Freund and Schapire [13], has strong practical advantages over previous boosting algorithms in the speed of learning. In [12], an evolutionary pruning method was proposed to find the set of classifiers, which resulted in an even lower number of classifiers than what was provided by AdaBoost learning. The authors claimed that using evolutionary pruning not only reduced the number of classifiers and provides faster computation times, but also the cascade structure of the classifiers could be optimized to achieve increased detection accuracy.

Unlike face detection in which there are only two classes, a facial recognition algorithm needs to authenticate or identify one or more persons in a captured image using a stored database of faces. The 2002 Face Recognition Vendor Test (FRVT 2002) showed that "the best 2002 face recognition probability of verification was 90 percent using a single face image with controlled illumination" [14]. To improve the accuracy, Nakamura and Miyamoto presented a rotation and size spreading associative neural network (RS-SAN net) that was based on space and 3-D shape recognition systems in the brain [15]. Further research efforts were presented at the 2006 WCCI conference by Nakamura and Takano [16]. They studied the recognition characteristics of the RS-SAN net through different facial images of the same subject, varying the orientation, size, and shape characteristics. An experiment of user authentication using

minimum distance criterion was carried out, which showed that the false acceptance and false rejection rates were 0% when the decision threshold was set at 0.04 ~ 0.06.

B. Speech Recognition and Speaker Verification

The terms speech recognition and speaker verification are often used interchangeably but actually refer to different technologies. Speech recognition is used to recognize what is being said while speaker verification is used to determine who said it. In other words, speech recognition recognizes words, while speaker verification verifies identities. Despite recent improvements in speech recognition, it is still a very difficult task in some applications. One of the hardest tasks has been the attempts to improve the performance of a connected Mandarin digit recognizer. Mandarin is especially difficult to deal with because it is a monosyllabic language [17]. In [18], the authors used a chaotic neural network mimicking the olfactory system, the KIII network, as a pattern classifier for Mandarin digital speech recognition. The KIII network is based on biological neural studies and has been successfully used on such problems as the classification of EEG waveforms. The algorithm was tested on the pronunciation of 0~9 digits in Mandarin. The performance of the KIII network was compared with the other neural network algorithms such as Back Propagation (BP) and Radial Basis Function (RBF) networks. The experimental results showed that the KIII model outperforms the other general neural networks on Mandarin digital speech.

RBF networks were introduced in neural network literature by Broomhead et al. in the late 1980s [19]. Not only can they be used in speech recognition, but also RBF networks can be applied to speaker verification. At the 2006 IEEE WCCI conference, Ham et al. presented a speaker verification system based on a bank of RBF neural modules (BRBFNM) to verify a speaker's identity [20]. Since the classic 2-dimensional receiver operating characteristic (ROC) curves only plot true-positive and false-positive measurements, a 3-dimensional ROC curve was developed to represent the mis-verification measurement. The simulation results, based on 10 different key words each repeated 12 times by 4 speakers, showed that when using 2-dimensional ROC curves the correct verification rate (CVR) was 86.5%, while using 3-dimensional ROC curves the CVR increased to 90.5%.

C. Handwriting and Signature Recognition

Using handwriting characteristics for user authentication has been of interest to researchers since the 1960s. The approaches to signature verification can be divided into two categories: online and offline. It should be pointed out that "online signature verification is more reliable than offline signature verification" [21]. Heinen and Osório presented an online signature authentication system prototype that used principal component analysis (PCA) to reduce the input space dimensionality and artificial neural networks to perform signature authentication. The neural network used in their prototype contained 117 neurons in the input layer and one neuron in the output layer. The experimental results showed that neural networks are very suitable for signature authentication tasks [22].

An online signature verification system usually includes a special pen and pressure-sensitive tablet. Self-organizing maps (SOMs) provide a powerful and prominent technique for data visualization, which can be used to map a multi-dimensional dataset onto a two-dimensional surface. Dozono et al. presented a method for PDA authentication by analyzing the pen pressure pattern of a user [23]. Instead of inputting a signature, the user was asked to trace the displayed symbols. A major concern was that it might be easier to trace the symbols with steady pressure than sign signatures consistently on PDA touch panel. The authors used PCA method and batch-type SOM for pen pressure analysis. The result showed that 70% of the users could be correctly authenticated with the proposed method. However, it was observed that the authentication rates varied widely among the users.

Unlike the online methods, offline signature verification can only take a 2-D image of the signature as the input without dynamic characteristics. Based on their previous research using the Modified Direction Feature (MDF), which generated encouraging results [24], Armand et al. presented an offline signature verification method that combined a number of structural features, such as surface area, length, and skew, with MDF [25]. Two neural network classifiers, the resilient back-propagation (RBP) neural network and radial basis function (RBF) network, were used to compare the signature verification accuracy. Tested on a publicly available database of 2106 signatures (936 genuine and 1170 forgeries), the RBF classifier showed a better verification rate (91.21%) than that of the RBP (88.0%).

VII. Conclusions

Increasing interest in biometrics has led to rapid improvements in biometric technologies with better performance, faster transaction speeds, and lower costs. The advantages of using biometrics to enhance security have been widely reported. There are various biometric projects underway around the world to strengthen security. Because a biometric sensor will never capture the exact same data twice, the matching of biometric features is a fuzzy comparison. Computational intelligence approaches are most suitable with such a situation. In recent years, various CI techniques, such as neural networks, fuzzy logic, and the evolutionary algorithm, have been applied more and more to solve complex biometric authentication and identification problems. With increasing security requirements, improvements in technology, and falling prices, we are likely to see many more biometric applications in the near future.

(continues on page 25)

TABLE 6 Obtaining values for hypothesis testing.

X1	X2	d = X1−X2
84.07	82.42	1.65
86.45	86.08	0.37
87.36	87.55	−0.18
87.00	87.00	0.00
87.73	86.81	0.92
90.29	89.01	1.28
91.94	88.46	3.48
89.74	86.81	2.93
88.10	87.91	0.18
91.58	91.21	0.37
92.86	90.11	2.75
92.67	89.56	3.11
88.83	87.91	0.92
92.31	90.48	1.83
91.94	89.74	2.20
91.76	90.29	1.47

5. Conclusions

The principal objective of this paper was to investigate the efficiency of the enhanced version of the MDF feature extractor for signature verification. Investigations adding new feature values to MDF were performed, assessing the impact on the verification rate of the signatures, using six-fold cross validation. Two different neural classifiers were used and two methodologies for verification were applied. The experiments conducted, whereby MDF was merged with the new features, provided very encouraging results.

Using RBP, MDF reached an 86.08% v. r., and MDF-CTLF reached 88% v. r. The RBF classifier provided better results than the RBP classifier overall with a single network configuration. The best v. r. obtained reached 91.21% with MDF-CTLFS, the combination of all the features described in this paper. However, with the multi-network configuration, RBP outperformed RBF with an error rate of 1.16%.

In future research, investigations will be conducted to enhance the feature extraction process. These include further combinations and investigations of the features. In addition, a larger signature database will be collected, including multilingual signatures, to investigate the techniques proposed in this paper. Additional classifiers, including Support Vector Machines (SVMs), will also be investigated for verifying the signatures.

References

[1] S. Chen and S. Srihari, "Use of exterior contour and shape features in off-line signature verification," *8th International Conference on Document Analysis and Recognition (ICDAR '05)*, pp. 1280–1284, 2005.

[2] M.A. Ferrer, J.B. Alonso, C.M. Travieso, "Offline geometric parameters for automatic Signature Verification using fixed-point arithmetic," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 27, no. 6, pp. 993-997, 2005.

[3] K. Han and I.K. Sethi, "Handwritten Signature Retrieval and Identification," *Pattern Recognition,* vol. 17, pp. 83–90, 1996.

[4] M. Hanmandlu, M.H.M. Yusof, and V.K. Madasu, "Off-line Signature Verification using Fuzzy Modeling," *Pattern Recognition,* vol. 38, pp. 341–356, 2005.

[5] K. Huang, and H. Yan, "Off-Line Signature Verification Based on Geometric Feature Extraction and Neural Network Classification," *Pattern Recognition,* vol. 30, no. 1, pp. 9–17, 1997.

[6] E.J.R. Justino, F. Bortolozzi, and R. Sabourin. "A comparison of SVM and HMM classifiers in the off-line signature verification," *Pattern Recognition Letters,* vol. 26, pp. 1377–1385, 2005.

[7] M.K. Kalera, S. Srihari, and A. Xu, "Off-line signature verification and identification using distance statistics," *International Journal of Pattern Recognition and Artificial Intelligence,* vol. 18, no. 7, pp. 1339–1360, 2004.

[8] A. Kholmatov, and B. Yanikoglu, "Identity Authentication using improved online Signature Verification method," *Pattern Recognition Letters*, in press, 2005.

[9] X.Y. Liu and M. Blumenstein, "Experimental Analysis of the Modified Direction Feature for Cursive Character Recognition," *International Workshop on the Frontiers of Handwriting Recognition (IWFHR-9)*, Japan, pp. 353–358, 2004.

[10] H. Lv, W. Wang, C. Wang and Q. Zhuo, "Off-line Chinese Signature Verification based on Support Vector Machines," *Pattern Recognition Letters,* vol. 26, pp. 2390–2399, 2005.

[11] L.E. Martinez, C.M. Travieso, J.B. Alonso, and M. Ferrer, "Parametrization of a forgery Handwritten Signature Verification using SVM," *IEEE 38th Annual 2004 International Carnahan Conference on Security Technology*, pp. 193–196, 2004.

[12] H. Srinisvasan, M.J. Beal and S.N. Srihari, "Machine Learning approaches for Person Identification and Verification," *SPIE Conference on Homeland Security*, pp. 574–586, 2005.

Technology Review *(continued from page 9)*

References

[1] T. Morgan "The DoD automated biometric identification system (ABIS)", *Biometrics Task Force*, [Online]. http://www.biometrics.dod.mil/documents/BRIEFS/DoD%20ABIS_Morgan_final.pdf#search=%22abis%20voice%20dna%22.

[2] J. Woodward, Jr., "Using biometrics to achieve identity dominance in the global war on terrorism", in *Military Review*, pp. 30–34, Sep.–Oct. 2005.

[3] "Biometrics deployment of machine readable travel documents," *ICAO TAG MRTD/NTWG*, Technical Report, Version 2.0, May 2004.

[4] J. Lettice, (2006, Aug. 4) "How to clone the copy-friendly biometric passport," *The Register* [Online]. http://www.theregister.co.uk/2006/08/04/cloning_epassports/.

[5] C. Handley, "Will airports look at biometrics?" *A Namitech Magazine,* vol. 1, pp. 13–14, 2002.

[6] Report Published by *Celent*, (2006, March 29) "Biometric ATMs in Japan: fighting fraud with vein pattern authentication", [Online]. http://www.celent.com/PressReleases/20060329(2)/BiometricsJapan.htm

[7] D. Kingsley, (2002, June 20) "Fingerprint security easy to fool," *News in Science* [Online]. Available: http://www.abc.net.au/science/news/stories/s585792.htm.

[8] K. Delac and M. Grgic, "A survey of biometric recognition methods," *Proceedings of the 46th International Symposium Electronics in Marine, ELMAR-2004*, pp. 184–193, Zadar, Croatia, 16–18 June 2004.

[9] Report Published by *Unisys*, (Apr. 26, 2006) "Consumers worldwide overwhelmingly support biometrics for identity verification, Says Unisys Study," [Online]. Available: http://www.unisys.com/about__unisys/news_a_events/04268651.htm.

[10] Q. Xiao, "Biometric user authentication for heightened information security," *The 1st International Conference on Biometric Authentication*, Lecture Notes in Computer Science, LNCS3072, pp. 708–715, Springer-Verlag, July 2004.

[11] J. Jang, K. Han and J. Kim, "Evolutionary algorithm-based face verification," *Pattern Recognition letters,* vol. 25, pp. 1857–1865, 2004.

[12] J. Jang and J. Kim, "Evolutionary pruning for fast and robust face detection", in *Proc. 2006 International Joint Conference on Neural Networks*, pp. 4436–4442, Vancouver, 16–21 July 2006.

[13] Y. Freund and R. Schapire, "A decision-theoretic generalization of on-line learning and an application to boosting." In *Proc. Second European Conference on Computational Learning Theory,* Springer-Verlag, pp. 23–37, Mar. 1995.

[14] M. Herman, "Ensuring the security of America's borders through the use of biometric passports and other identity documents", June 22, 2005, http://hsc.house.gov/files/ TestimonyHerman.pdf#search=%22frvt%202002%20improvement%22.

[15] K. Nakamura and S. Miyamoto, "Rotation, size and shape recognition by a spreading associative neural network," *IEICE Trance. on Information and Systems*, vol. E-84-D, no. 8, pp. 1075–1084, 2001.

[16] K. Nakamura and H. Takano, "Rotation and size independent face recognition by the spreading associative neural network", in *Proc. 2006 International Joint Conference on Neural Networks*, pp. 8213–8219, Vancouver, 16–21 July 2006.

[17] F. Zhao, P. Raghavan, and S. Gupta, "Automatic speech recognition in mandarin for embedded platforms," in *Proc. Of ICSLP'2000,* vol. 2, pp. 815–818.

[18] J. Zhang, G. Li, and W. Freeman, "Application of novel chaotic neural networks to Mandarin digital speech recognition", in *Proc. 2006 International Joint Conference on Neural Networks*, pp. 1380–1385, Vancouver, 16–21 July 2006.

[19] M. Broomhead and D. Lowe, "Multivariable functional interpolation and adaptive networks". *Complex Systems*, vol. 2, pp. 321–355, 1988.

[20] F. Ham, R. Acharyya, and Y. Lee, "Speaker verification using 3-D ROC curves for increasing impostor rejections", in *Proc. 2006 International Joint Conference on Neural Networks*, pp. 4868–4872, Vancouver, 16–21 July 2006.

[21] A. Kholmatov and B. Yanikoglu, *Biometric authentication using online signatures*, Lecture Notes in Computer Science-ISCIS 2004, Oct. 2004, vol: 3280, pp. 373–380.

[22] M.R. Heinen and F.S. Osório, "Handwritten signature authentication using artificial neural networks", in *Proc. 2006 International Joint Conference on Neural Networks*, pp. 10111–10118, Vancouver, 16–21 July 2006.

[23] H. Dozono, M. Nakakuni, H. Sanada, and Y. Noguchi, "The analysis of pen inputs of handwritten symbols using self organizing maps and its application to user authentication", in *Proc. 2006 International Joint Conference on Neural Networks*, pp. 4884–4889, Vancouver, 16–21 July 2006.

[24] M. Blumenstein, X.Y. Liu, and B. Verma, "A modified direction feature for cursive character recognition", *International Joint Conference on Neural Networks (IJCNN '04)*, pp. 2983–2987, 2004.

[25] S. Armand, M. Blumenstein, and V. Muthukkumarasamy, "Off-line signature verification using the enhanced modified direction feature and neural-based classification", in *Proc. 2006 International Joint Conference on Neural Networks*, pp. 1663–1670, Vancouver, 16–21 July 2006.