ISSN:2348-2079

SEP-2014

International Journal of Intellectual Advancements and Research in Engineering Computations

A SURVEY ON MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEM IN CLOUD COMPUTING

[*1]Ms.V.Karunya, [*2]Mrs.P.Sarala, [*3]Dr.N.Shanthi

ABSTRACT

Authenticating the user based on behaviour based biometrics is more reliable than the more traditional means of password authentication. Biometric systems for today's high security applications must meet stringent performance requirements. The fusion of multiple biometrics helps to minimize the system error rates. Fusion methods include processing biometric modalities sequentially until an acceptable match is obtained. As security is the main concern in using cloud computing fused biometric authentication technique which can be used as single sign on so that the services can be more secure and reliable ,and that biometric authentication is provided as a service by a cloud provider.

Index terms: Multimodal, Biometric, Fusion, Single Sign On.

I INTRODUCTION

Today a growing number of companies have to process huge amounts of data in a cost-efficient manner. Classic representatives for these companies are operators of Internet search engines, like Google, Yahoo, or Microsoft. The vast amount of data they have to deal with every day has made traditional database solutions prohibitively expensive. Thus the cloud is best suitable for above requirements.[1]. To provide security in cloud biometric authentication system is used.

The word "biometrics" comes from the Greek language and is derived from the words bio (life) and metric (to measure).Biometrics (or biometric authentication) refers to the identification of humans by their characteristics or traits. In [3]Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Hence, single biometric may not be able to achieve the desired performance requirement in real world applications. One of the methods to overcome these problems is to make use of multimodal biometric authentication systems, which combine information from multiple modalities to arrive at a decision.

Studies have demonstrated that multimodal biometric systems can achieve better performance compared with unimodal systems. This paper presents the review of multimodal biometrics. This includes applications, challenges and areas of research in multimodal biometrics. The different fusion techniques of multimodal biometrics have been discussed.

Author for Correspondence:

[*1]Ms.V.Karunya, Department of CSE, Nandha Engineering College, Erode, Tamilnadu, India.
E-mail:Karunyavel07@gmail.com.

[*2]Mrs.P.Sarala, Asst. Professor, Department of CSE, Nandha Engineering College, Erode, Tamilnadu, India.
E-mail:sarala.p@nandhaengg.org.

[*3]Dr.N.Shanthi, Professor & Dean, Department of CSE, Nandha Engineering College, Erode, Tamilnadu, India.
E-mail:deancse@nandhaengg.org.

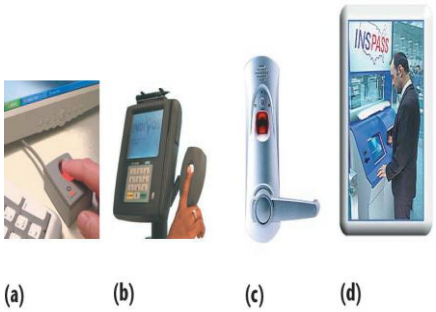

Figure: Design of Biometric authentication

II PROBLEM AND ANALYSIS

The well-known buzzword, say Cloud Computing, attracts the attention from both academy and industry across the world, because of its potential in achieving the long-held dream, say Utility Computing and opens a new era for new services. To prevent data from cloud service provider, data is encrypted while saving it on the cloud using Confidentiality, Integrity, Availability (CIA) values which will categorize data in three rings[1].

Fingerprint Verification Competition FVC2004 was organized by the authors of this work for the purpose of assessing the state-of-the-art in this challenging pattern recognition application and making available a new common benchmark for an unambiguous comparison of fingerprint-based biometric systems.FVC2004 is an independent, strongly supervised evaluation performed at the evaluators' site on evaluators' hardware[2].

To achieve more reliable verification or identification we should use something that really characterizes the given person. Biometrics offer automated methods of identity verification or identification on the principle of measurable physiological or behavioral characteristics such as a fingerprint or a voice sample. These characteristics are unique and slow intrusive[3].

This paper reviews a line of research carried out over the last decade in speech recognition assisted by discriminatively trained, feed forward networks. The particular focus is on the use of multiple layers of processing preceding the hidden Markov model based decoding of word sequences[4].

A biometric authentication system based on measurements of the user's three-dimensional (3-D) hand geometry is proposed. By exploiting 3-D information we are able to limit the constraints usually posed on the environment and the placement of the hand, and this greatly contributes to the unobtrusiveness of the system[6].

Isolated word/sentence recognition was performed using cepstral feature extraction by linear predictive coding, as well as Hidden Markov Models (HMM) for pattern training and classification using the Al-Alaoui Algorithm[7].

In traditional methods for noise robust automatic speech recognition, the acoustic models are typically trained using clean speech or using multi-condition data that is processed by the same feature enhancement algorithm expected to be used in decoding a noise adaptive training (NAT) algorithm that can be applied to all training data that normalizes the environmental distortion as part of the model training[8]. Effective human and automatic processing of speech requires recovery of more than just the words by a metadata detection system that combines information from different types of textual knowledge sources with information from a prosodic classifier[9]. Biometric authentication techniques, which try to validate the identity of an user based on his/her physiological or behavioral traits, are already quite widely used for local authentication purposes (for private use), while their use on the Internet is still relatively modest. The main reason for this setting is open issues pertaining mainly to the accessibility and scalability of existing biometric technology[11].

A wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. By using biometrics it is possible to confirm or establish an individual's identity[12].

Greater adoption of biometric payment system will drive down the cost of biometric readers and thus making it more affordable to small business owners. We really need alternate payment systems. This "perpetual toll" to credit card companies has to stop[13]. It provides reliable means of biometric authentication due to its features Universality, Distinctiveness, Permanence and Accuracy. It is the

method of identifying an individual and it can be used in various application, such as, medical records, criminal investigation, cloud computing communication etc[15].

Fingerprints possess two main types of features that are used for automatic fingerprint identification and verification: (i) Ridge and furrow structure that forms a special pattern in the central region of the fingerprint and (ii) Minutiae details associated with the local ridge and furrow structure[17].

"Cloud computing may be the only way to handle vast, unstable query loads—differentiated data in any number of formats and with any number of relationships," Data Security is considered as major aspect in cloud environment while using an application. This Data security can be implemented with respect to user authentication and authorization using cryptography system[19].

The fusion of multiple biometrics helps to minimize the system error rates. Fusion methods include processing biometric modalities sequentially until an acceptable match is obtained. More sophisticated methods combine scores from separate classifiers for each modality[20].

PASSWORD HACKING AND DATA INTRUSION IN CLOUD

One of the Security risks in cloud computing according to Garfunkel [11] is hacked passwords or data intrusion. If someone hacks a password they get control over the resources. They can manipulate the information or disable the services. Furthermore, there is a possibility for the user's email (Amazon user name) to be hacked (see [10] for a discussion of the potential risks of email), and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password [19].

BIOMETRICS METHOD

TYPES OF BIOMETRICS

Two classes of biometric methods are:

Physical Biometrics:

Physiological biometrics is based on measurements and data derived from direct measurement of a part of the human body. Fingerprint, iris-scan, retina-scan, hand geometry, and facial recognition are leading physiological biometrics.

Behavioral characteristics:

Behavioral characteristics are based on an action taken by a person. Behavioral biometrics, in turn, are based on measurements and data derived from an action, and indirectly measure characteristics of the human body. Voice recognition, keystroke-scan, and signature-scan are leading behavioral biometric technologies. One of the defining characteristics of a behavioral biometric is the incorporation of time as a metric – the measured behaviour has a beginning, middle and end [3]. A number of biometric methods have been introduced over the years, but few have gained wide acceptance.

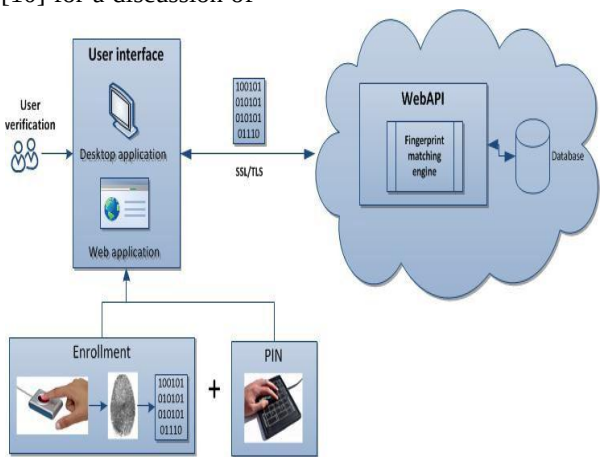

Figure: Working model of biometric system

FACTORS OF EVALUATION

False Accept Rate (FAR) and False Match Rate (MAR):

The probability that the system incorrectly declares a successful match between the input pattern and a non matching pattern in the database. It measures the percent of invalid matches. These systems are critical since they are commonly used to forbid certain actions by disallowed people.

False Reject Rate (FRR) or False Non-Match Rate (FNMR):

The probability that the system incorrectly declares failure of match between the input pattern and the matching template in the database. It measures the percent of valid inputs being rejected.

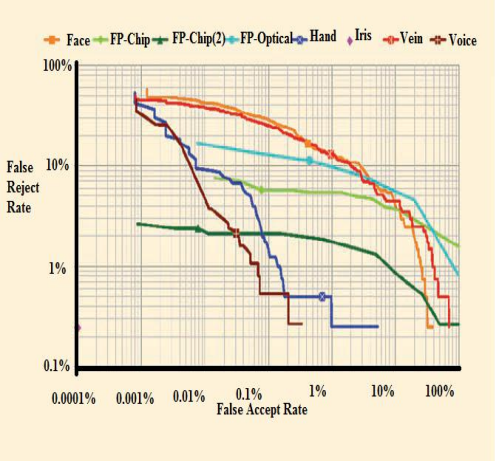

Figure 3: FRR & FAR comparison

Relative Operating Characteristic (ROC):

In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). In biometric systems the FAR and FRR can typically be traded off against each other by changing those parameters. The ROC plot is obtained by graphing the values of FAR and FRR, changing the variables implicitly. A common variation is the Detection Error Trade off (DET), which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

Equal Error Rate (EER):

The rates at which both accept and reject errors are equal. ROC or DET plotting is used because how FAR and FRR can be changed, is shown clearly. When quick comparison of two systems is required, the ERR is commonly used. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered 0to be.

Failure to Enroll Rate (FTE or FER):

The percentage of data input is considered invalid and fails to input into the system. Failure to enroll happens when the data obtained by the sensor are considered invalid or of poor quality.

Failure to Capture Rate (FTC):

Within automatic systems, the probability that the system fails to detect a biometric characteristic when presented correctly is generally treated as FTC.

Template Capacity:

It is defined as the maximum number of sets of data which can be input in to the system.

PROS AND CONS OF DIFFERENT BIOMETRIC METHODS

Theoretically biometrics is a great way of authenticating a user.

Finger prints: It's impossible to lose your finger prints, no chance of forgetting them. However in practice according to the problem that has been pointed out by Guy Churchward, CEO of LogLogic uniqueness the thing that makes using biometric data an inherently flawed choice for a primary method of authentication."Once you have your fingerprint scanned it will give a unique data sequence which if compromised is not exactly something you can change," he says. "Imagine having an option of only one password 'ever'. One loss and you are screwed"[4].The above problem can be solved by

using biometric and password together for authentication.

	FVC2000	FVC2002	FVC2004
Call for participation	November, 1999	October, 2001	April, 2003
Registration deadline	March 1st, 2000	January 10th, 2002	October 15th, 2003
Submission deadline	June 1st, 2000	March 1st, 2002	November 30th, 2003
Evaluation period	July–August, 2000	April–July, 2002	January–February 2004
Anonymous participation	Not allowed	Allowed	
Categories	-		*Open* and *Light*
Registered participants	25 (15 withdrew)	48 (19 withdrew)	110 (64 withdrew)
Algorithms evaluated	11	31	*Open Category*: 41 *Light Category*: 26
Presentation of the results	15th ICPR Barcelona, September 2000	16th ICPR Quebec, August 2002 [18]	1st ICBA Hong Kong, July 2004 [19]
Databases	Four new databases, each one containing: set A (100x8) and set B (10x8)		
DB1	Optical (KeyTronic)	Optical (Identix)	Optical (CrossMatch)
DB2	Capacitive (ST Microelectr.)	Optical (Biometrika)	Optical (Digital Persona)
DB3	Optical (Identicator Tech.)	Capacitive (Precise Biometrics)	Thermal-sweeping (Atmel)
DB4	Synthetic (SFinGe v2.0)	Synthetic (SFinGe v2.51)	Synthetic (SFinGe v3.0)
Databases availability	DVD accompanying "Handbook of Fingerprint Recognition" [20]		Not available yet
Website	http://bias.csr.unibo.it/fvc2000	http://bias.csr.unibo.it/fvc2002	http://bias.csr.unibo.it/fvc2004
HW/SW used for running the evaluation	Pentium III (450 MHz) Windows NT FVC Test suite v1.0	Pentium III (933 MHz) Windows 2000 FVC Test suite v1.2	Athlon 1600+ (1,41 GHz) Windows XP FVC Test suite v2.0

Figure 4: Comparison table for different biometric types

Hand scans: Hand scans requires low data storage but may not be unique to every user.

Retina Scans: Retina scans are highly accurate and require low storage space but they need expensive hardware and user identification frequency is less.

Iris scans: Iris scans are low intrusive and they are more accurate and needs less storage space.

Voice authentication: Voice authentication is unique and non intrusive method and also the hardware requirements required for this type of authentication are cheap and are available readily. Microphones can be used for this purpose. However the back ground noise must be controlled, high storage is required for this kind of authentication. This type of authentication can also be extraneously influenced by once sore throat and cold.[6]

Facial scans: One major advantage is that facial-scan technology is the only biometric capable of identification at a distance without subject complicity or awareness. Another advantage of facial-scan technology is the fact that static images can be used to enroll a subject[7].

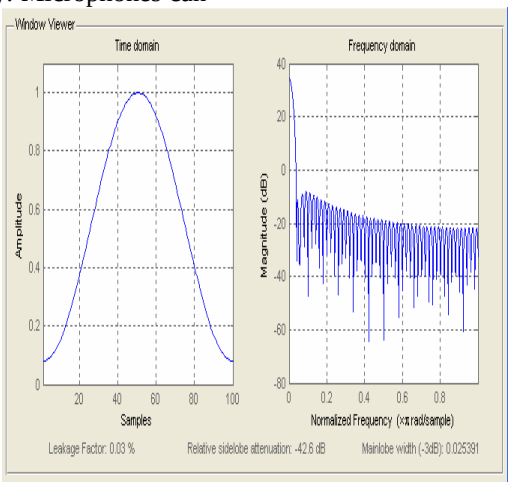

Figure 5: Graph for facial scan to measure time and frequency domain

Disadvantages include acquisition environment and facial characteristic changes that effect matching accuracy and the potential for privacy abuse. Images are most accurate when taken facing the acquisition camera and not sharp angles. The users face must be lit evenly, preferably from the front [7].

III MECHANISM AND SOLUTION

BIOMETRICS AUTHENTICATION SYSTEM WORKING

The authentication service provider maintains the biometric data base .The data has to be stored in encrypted format using cryptography on biometric for the security reasons. In this paper it site a blind protocol technique which is given by Upamanyu.M, the protocol is blind in the sense that it reveals only the identity, and no additional information about the user or the biometric to the authenticating server or vice-versa. As the protocol is based on asymmetric encryption of the biometric data, it captures the advantages of biometric authentication as well as the security of public key cryptography [12].

Registration process:

The user initially enrolls with the biometric system which is provided by a cloud, once the identity is registered his/her biometric authentication details are stored in cloud service provider database. The authorization details are also entered at the registration time which is also encrypted. Whenever the user wants to use any cloud service user first uses the biometric authentication service rather than a traditional password mechanism. Once authenticated, the user is redirected to the actual cloud service for which he is authorized to use.

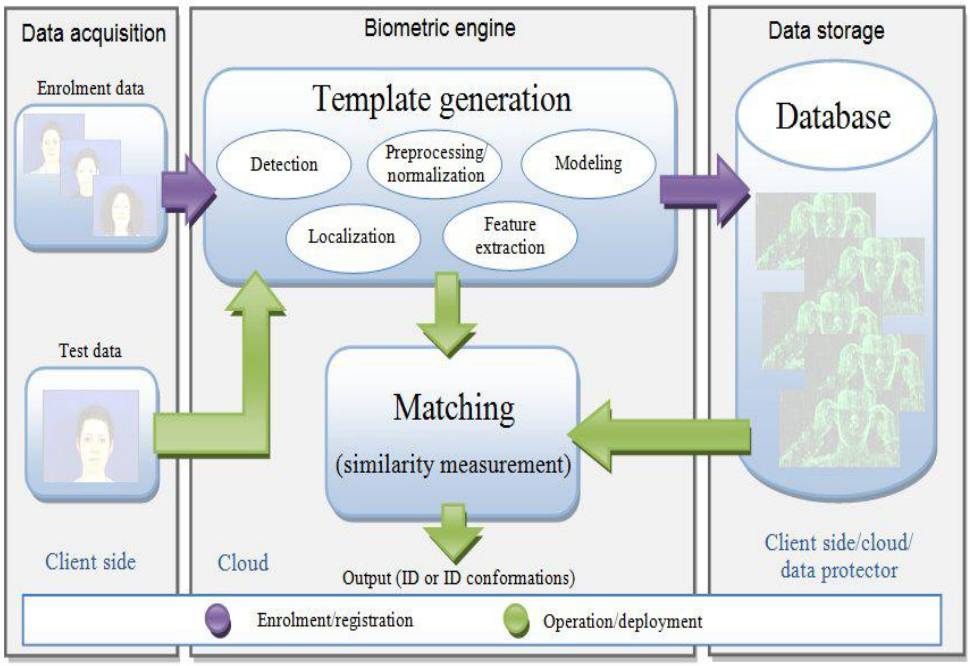

Figure 6: Working model of authentication system

MULTIMODAL-BIOMETRIC METHOD

The term "multimodal" is used to combine two or more different biometric sources of a person (like face and fingerprint) sensed by different sensors. Two different properties (like infrared and reflected light of the same biometric source, 3D shape and reflected light of the same source sensed by the same sensor) of the same biometric can also be combined. In orthogonal multimodal biometrics, different biometrics (like face and fingerprint) are

involved with little or no interaction between the individual biometric whereas independent multimodal biometrics processes individual biometric independently. Orthogonal biometrics are processed independently by necessity but when the biometric source is the same and different properties are sensed, then the processing may be independent, but there is at least the potential for gains in performance through

collaborative processing. In collaborative multimodal biometrics the processing of one biometric is influenced by the result of another biometric.

NEED OF MULTIMODAL BIOMETRIC

Most of the biometric systems deployed in real world applications are unimodal which rely on the evidence of single source of information for authentication (e.g. fingerprint, face, voice etc.). These systems are vulnerable to variety of problems such as noisy data, intra-class variations, inter-class similarities, non-universality and spoofing. It leads to considerably high false acceptance rate (FAR) and false rejection rate (FRR), limited discrimination capability, upper bound in performance and lack of permanence [8]. Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. These systems allow the integration of two or more types of biometric systems known as multimodal biometric systems. These systems are more reliable due to the presence of multiple, independent biometrics [9]. These systems are able to meet the stringent performance requirements imposed by various applications. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge – response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a 'live' user is indeed present at the point of data acquisition.

COMPARSION OF SEVERAL BIOMETRIC TECHNOLOGIES

Biometric	EER	FAR	FRR	Comments
Face	NA	1%	10%	varied light, indoor /outdoor
finger print	2%	2%	2%	rotation and exaggerated skin distortion
hand geometry	1%	2%	2%	with rings and improper placement
Iris	.01%	.94%	.99%	indoor environment
Keystrokes	1.8%	7%	.1%	during 6 months period
Voice	6%	2%	10%	text dependent and multilingual

IV CONCLUSION

This paper presents the various issues related to multimodal biometric systems. By combining multiple sources of information, the improvement in the performance of biometric system is attained. Various fusion levels and scenarios of multimodal systems are discussed. Fusion at the match score level is the most popular due to the ease in accessing and consolidating matching scores. Performance gain is pronounced when uncorrelated traits are used in a multimodal system. The challenges faced by multimodal biometric system and possible research areas are also discussed in the paper.

REFERENCES

[1]. Karthik Nandakumar, Student Member, IEEE, Anil K. Jain, Fellow, IEEE, and Sharath Pankanti, Senior Member, IEEE, "Fingerprint-Based Fuzzy Vault:Implementation and Performance", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 2, NO. 4, DECEMBER 2007.

[2]. R.Cappelli, "Synthetic Fingerprint Generation," Handbook of Fingerprint Recognition,Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, eds. New York: Springer, 2003.

[3]. K.H.Davis,R.Biddulph,and S. Balashek, "Automatic recognition of spoken digits," J.

Acoust. Soc. Amer., vol. 24, no. 6, pp. 627–642, 1952.

[4]. Dahl, M. Ranzato, A. Mohamed, and G. E. Hinton, "Phone recognition with the mean-covariance restricted Boltzmann machine," in Advances in Neural Information Processing 23. Cambridge, MA: MIT Press, 2010.

[5]. M. Bazen and S.H. Gerez, "Systematic methods for the computation of the directional fields and singular points of fingerprints," IEEE Trans. Pattern Anal. Machine Intell., vol. 24, no. 7, pp. 905–919, July 2002.

[6]. N. Otsu, "A threshold selection method from gray-level histograms," IEEE Trans. Syst., Man. Cybern., vol. SMC-9, pp. 62–66, 1979.

[7]. [7] M. Al-Alaoui, "A new weighted generalized inverse algorithm for pattern recognition", IEEE Transactions on Computers, vol. C-26, no. 10, October 1977.

[8]. V. Digalakis, D. Rtischev, L. Neumeyer, and E. Sa, "Speaker adaptation using constrained estimation of Gaussian mixtures," IEEE Trans. Speech Audio Process., vol. 3, no. 5, pp. 357–366, Sep. 1995.

[9]. McCallum, "Mallet: A machine learning for language toolkit," 2002, http://mallet.cs.umass.edu. A. Jules and M. Sudan, "A Fuzzy Vault Scheme," Proc. IEEE Int'l Symp. Information Theory, IEEE Press, 2002, p. 408.

[10]. D. Balfanz et al., "The future of authentication",IEEE Security & Privacy, vol. 10, pp. 22-27, 2012.

[11]. Phillips, A. Martin, C. Wilson, and M. Przybocki, "An introduction to evaluating biometric systems", IEEE Computer Society., Volume 33, No. 2, Feb. 2000, pp. 56–63.

[12]. Anil K. Jain, Arun Ross and Salil Prabhakar: "An Introduction to Biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[13]. Jucheng Yang, Naixue Xiong, "A Fingerprint Recognition Scheme Based on Assembling Invariant Moments for Cloud Computing Communications." Jiangxi University of Finance and Economics, IEEE systems journal, vol. 5, no. 4, December 2011.

[14]. A.Georghiades, P. Belhumeur, and D. Kriegman. From few to many: Illumination cone models for face recognition under variable lighting and pose. IEEE Transactions on Pattern Analysis and Machine Intelligence, 23(6):643–660, 2001. B. Miller, "Vital signs of identity," IEEE Spectrum, vol. 31, pp. 22–30, Feb. 1994.

[15]. J. E. Siedlarz, "Iris: More detailed than a fingerprint," IEEE Spectrum, vol. 31, p. 27, Feb.1994.