ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

A Comprehensive Approach on Different Biometric Modalities and Its Applications for Security

Saranya.K.R, Vanitha.S, Selva Priya.G

PG Scholar, Dept of CSE, Dr N.G.P Institute of Technology, Coimbatore, India

Assistant Professor, Dept of CSE, Dr N.G.P Institute of Technology, Coimbatore, India

PG Scholar, Dept of CSE, Dr N.G.P Institute of Technology, Coimbatore, India

ABSTRACT: Biometrics is an automated method of recognizing a person based on a physiological or behavioral appearance. Biometric detection technology relies upon the physical appearance of an individual, such as fingerprints, voiceprint, prototype of the iris of the eye and facial prototype, in identifying an individual, offering positive identification that is difficult to counterfeit. Instances of physiological biometric traits include height, weight, body odour, the aspect of the hand, the prototype of veins, retina or iris, the face and the prototypes on the skin of thumbs or fingers (fingerprints). Instances of behavioral biometrics are voice prototypes, signature and keystroke sequences and gait (the body movement while walking). Biometric identifiers are the distinctive, measurable appearances used to label and describe individuals [1]. Currently, passwords, Personal Identification cards are used for personal detection. However, cards can be stolen, and passwords and numbers can be guessed or forgotten. To solve these problems, biometric verification technology, which identifies people by their unique biological information, is attracting attention [2]. Biometrics is mostly used for authentication purposes to ensure proper safety.

KEYWORDS: counterfeit, detection, gait, iris

I. INTRODUCTION

Biometrics is the identification of humans using intrinsic physiological, biological, or behavioural appearances, traits, or habits [3]. Biometrics have the potential to provide this desired ability — to unambiguously and discretely identify a person’s identity— more accurately and conveniently than other options. Instances of biometric modalities include face, iris, hand, fingerprint, gait, typing, speech, and others. In the past period, advances in computing power have made programmed biometric systems realistic alternatives or supplements to traditional safety systems.

For users, biometric systems can reduce or eliminate the need to retain a key or remember a password, can speed up user throughput, and can be less invasive. For instance, at a border or safety checkpoint, a biometric system could provide a high-confidence identification of a user while they walk through a checkpoint rather than requiring them to stop, produce some identification, and be interviewed by safety personnel. From a system standpoint, biometric systems can check much larger databases than are realistic with traditional safety systems, are more coherent, do not have racial or personal preferences, and can be cheaper to operate. Physiological characteristics are related to the figure of the body.

Instances include, but are not limited to fingerprint, palm veins, face identification, DNA, palm print, hand geometry, iris identification, retina and odour/scent.Behavioural appearances are related to the pattern of activities of a person, including but not limited to typing cadence, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics [4]. More traditional means of access control include token-based verification systems, such as a driver's license or passport, and knowledge-based verification systems, such as a password or personal verification number [1].Since biometric identifiers are unique to individuals, they are more reliable in verifying individuality than token and knowledge-based approaches; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information [1][2].

II. RELATED WORK

Fingerprint identification is one of the most well-known and publicized biometrics. Because of their differentness and coherence over time, fingerprints have been used for recognition for over a century, more recently becoming automated (i.e. a biometric) due to advancements in computing capabilities. Fingerprint recognition is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for gathering, and their established use and collections by law enforcement and immigration [6].Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of mass forms of biometrics used to identify individuals and verify their existence. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print prototype. These include prototypes, which are aggregate appearances of ridges, and minutia points, which are unique features found within the prototypes [5]. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies. For this palm-based or image based algorithm is used and finger-scan technology is used.

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video foundation. One of the ways to do this is by contrasting selected facial features from the image and a facial databank. It is typically used in security schemes and can be compared to other biometrics such as fingerprint or eye iris recognition systems [7]. The human face plays an important role in our social collaboration, conveying people’s uniqueness. Using the human face as a key to security, biometric face detection technology has received significant attention in the past several years due to its potential for a wide variety of applications in both law enforcement and non-law enforcement As compared with other biometrics systems using fingerprint/palm print and iris, face detection has distinct merits because of its non-contact procedure. Face images can be captured from a distance without touching the person being identified, and the recognition does not require interacting with the person. In addition, face detection serves the crime deterrent purpose because face images that have been recorded and archived can later help identify a person. For face recognition PCA and LDA algorithms are used. The Eigen facial recognition technique is suitable for face recognition system.

Iris identification is an automated method of biometric recognition that uses mathematical prototype-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex random prototypes are different, stable, and can be seen from some distance [10]. Retina scanning is different, now obsolete, ocular-based biometric knowledge for which iris recognition is often confused with has been supplanted by iris recognition. Iris recognition uses video camera knowledge with subtle near infrared illumination to acquire images of the detail-rich, intricate shapes of the iris which are noticeable externally. Digital patterns encoded from these patterns by mathematical and statistical algorithms allow the identification of an individual or someone pretending to be that individual [8]. Databases of enrolled prototypes are searched by matcher engines at speeds measured in the millions of templates per second per (single-core) CPU, and with remarkably low false event rates. Several hundred millions of persons in several countries around the world have been enrolled in iris recognition systems for convenience purposes such as passport-free automated border-crossings, and some national ID programs [9].For iris recognition Daugman and tisse algorithms are used.

Voice recognition can raise Speaker recognition, determinant World Health Organization is speaking and Speech recognition, determinant what is being same. The term voice recognition [14] or recognition [15] refers to distinctive the speaker, rather than what they are language. Recognizing the speaker can alter the task of translating speech in systems that area unit trained on a selected person's voice or it should be accustomed proof or verify the identity of a speaker as a district of a security methodology. From the technology perspective, speech recognition has been rummaging several waves of major innovations since over some fifty years past. The foremost recent wave of revolutions since 2009, arguably the foremost very important one that defines the current state of the art in speech recognition accuracy and has been in dominant use since 2013 throughout the speech trade worldwide, depends on deep learning ideas, architectures, methodologies, algorithms, and wise system implementations enabled by vast employment data and by GPU-based vast reckon. Speaker recognition [11] is that the identification of the one that's speaking by characteristics of their voices (voice biometrics), together called voice recognition [12][13].There is a distinction between speaker recognition (recognizing World Health Organization is speaking) and speech recognition (recognizing what is being said). These two terms unit usually confused, and "voice recognition" is also used for every.

to boot, there is a distinction between the act of authentication (commonly ascertained as speaker verification or speaker authentication) and identification. Finally, there is a distinction between speaker recognition (recognizing World Health Organization is speaking) and speaker diarisation (recognizing once the same speaker is speaking). Recognizing the speaker can alter the task of translating speech in systems that area unit trained on specific person's voices or it should be accustomed proof or verify the identity of a speaker as a district of a security method.

Signature recognition could be a behavioral biometric. It may be operated in 2 other ways. Static: during this mode, users write their signature on paper, modify it through associate degree optical scanner or a camera, and therefore the biometric system acknowledges the signature analyzing its form. This cluster is additionally called “off-line”. Dynamic: during this mode, users write their signature during a digitizing pill, that acquires the signature in real time. Dynamic recognition is additionally called “on-line”, spatial coordinate x(t). The progressive in biometric authentication may be found within the last major international competition [16].The most widespread pattern recognition techniques applied for biometric authentication are dynamic time warp, hidden mathematician models and vector quantization. Combos of various techniques additionally exist [17].

Hand pure mathematics could be a biometric that identifies users by the form of their hands. Hand pure mathematics readers live a user's hand on several dimensions and compare those measurements to measurements keep in an exceedingly file. Since hand pure mathematics isn't thought to be as distinctive as fingerprints, palm veins or irises, procedure, palm veins and iris recognition stay the popular technology for high-security applications. Hand pure mathematics is incredibly reliable once combined with alternative varieties of identification, like identification cards or personal identification numbers. In giant populations, hand pure mathematics isn't appropriate for supposed one-to-many applications, within which a user is known from his biometric with none alternative identification [18].

S.no	Modalities	Advantage	Disadvantage	Applications
1	Fingerprint	One huge advantage of fingerprint identification is that it's alright accepted within the community, among enforcement, and also the general public.	Temperature and humidness might have an effect on the standard of the image and during this forgery is incredibly straightforward to try and do.	Physical access organization, Logical access organization, Time and attendance management.
2	Face	One key advantage is that it does not require the cooperation of the test subject to work.	Face recognition is not perfect and struggles to perform under certain conditions.	Access control, Identification systems, Surveillance and pervasive computing.
3	Iris	There is no need to touch any equipment, where a finger has to touch a shell, or retinal scanning, where the eye must be brought very close to an eyepiece (like looking into a microscope).	It is very hard (if not impossible) to prove that the iris is unique. Some medical and surgical procedures that can affect the colour and overall shape of the iris.	National border controls, computer login, cell phone and other wireless-device-based authentication, driving licenses; other personal certificates.
4	Voice	It allows user to operate a computer by speaking to it. It free up cognitive working space and allows dictation of text, commands. It eliminates handwriting and spelling problems.	It requires large amounts of memory to store voice files. It is difficult to use in classroom settings, due to noise interference. It requires each user to train software to identify voice, hard for poor decoders.	Car systems, Health care, Military, Automated phone systems, Google voice, Siri.
5	Signature	It is user friendly and well accepted socially and	High error rates than other traits. It is affected by the	Credit card transactions, To

10.15680/ijircce.2015.0303025

		legally. It is non invasive	physical and emotional state of the user.	validate checks, Financial Institutions, Commercial Organizations
6	Hand Geometry	Most widely used technique for physical access. It is deemed to be one of the easiest to use and administer of all of the biometric technologies that are available today.	It needs large size of hand geometry devices. It is used only for verification.Only single hand is to be allowed. The injuries in hand may affect the quality of the image.	Time and attendance management Used for point of sale applications, Access control, Large Factories
7	Gait	It can also be applied to running or any means of movement on foot. the gait of an individual can be captured at a distance unlike other biometrics such as fingerprint recognition.	A person during pregnancy, after an accident/disease affecting the leg, or after severe weight gain / loss can all affect the movement of an individual. Drugs and alcohol will affect the way in which a person walks.	Medical diagnostics, Biometric identification Systems and dialetics, Comparative biomechanics.
8	Vascular Pattern	It is difficult to forge and it is contact less. It is capable of one to one and one too many matching.	Sometimes it may show the false rates and it leads to many losses. Conventional vascular pattern algorithm is low efficient.	Check the legality of travellers from one country to another, Airports, ATM and Credit cards, Government Workplaces.
9	Retina	Retina recognition captures and analyses the patterns of blood vessels on the thin nerve on the back of the eyeball that processes light entering through the pupil.	The retina is small, internal, and difficult to measure. An individual must position the eye very close to the lens of the retina-scan device, gaze directly into the lens.	Government agencies, Medical applications, Prison.

III. OTHER MODALITIES

A. GAIT RECOGNITION:

Gait recognition is associate rising biometric technology that involves individuals being known strictly through the analysis of the method they walk. Whereas analysis continues to be afoot, it's attracted interest as a technique of identification as a result of it's non-invasive and doesn't need the subject’s cooperation. Gait recognition may even be used from a distance, creating it well-suited to distinguishing perpetrators at against the law scene. However gait recognition technology isn't restricted to security applications – researchers additionally envision medical applications for the technology. as an example, recognizing changes in walking patterns timely will facilitate to spot conditions like Parkinson’s malady and degenerative disorder in their earliest stages. Gait recognition knowledge is, however, still in its developing periods. Gait analysis is that the systematic study of animal locomotion, a lot of specifically the study of human motion, victimization the attention and therefore the brain of observers, increased by instrumentation for measurement body movements, body mechanics, and therefore the activity of the muscles [19].

B. VASCULAR PATTERN RECOGNITION:

Vascular pattern recognition is so the latest during this direction that makes use of vein patterns of human hand to form templates to totally different users. at the side of fingerprint analysis and biometric identification, vein pattern authentication is quick turning into the talk the city. Infrared-like lights square measure won't to penetrate the human skin and capture totally different hand tube-shaped structure patterns of veins gift at the rear of a hand. These distinct patterns square measure coded to organize totally different templates, that square measure recorded within the information of biometric devices. Tube-shaped structure pattern recognition offers higher usability and so, devices like hand tube-shaped structure scanner square measure appropriate each single user within the organization. High accuracy is obtainable by these devices with admirable false acceptance and false rejection rates.

C. RETINA RECOGNITION:

Retina recognition [21][22] is another eye-based biometric, however it uses the structure of the membrane, the liner of the inner surface of the attention, to spot folks. as a result of the membrane is an enclosed structure of the attention, it's not sensible to accumulate noncompliant pictures of the membrane in humans. From a sensible position, acquisition of retinal pictures is often thought of intrusive enough that even for several compliant recognition systems it's not sensible or ideal. To boot, the vein structure of the membrane isn't unshapely with the movement of the attention, and intrinsically retinal vein recognition algorithms aren't applicable for sclerotic coat vein recognition applications [23][24][25].

IV. SIMULATION RESULTS

The Fig.1. Shows the recognition pattern for fingerprint. A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live skim and it is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. Matching innovations are used to compare previously stored templates of fingerprints against candidate fingerprints for confirmation purposes. In order to do this either the original image must be directly compared with the candidate image or certain features must be compared.

The Pattern showed in Fig.2 is the recognition of sclera vein. For the sclera segmentation system, a system is developed that can accurately segment the sclera region using color images and does not require training. The feature extraction and enhancement system uses a bank of Gabor filters to extract the vein pattern from the segmented sclera region. The feature matching system uses a RANSAC-based registration system to register the sclera vein templates to achieve translation-, rotation-, and scaling-invariance. The goal is development of a system that can consistently identify users from their extracted vein pattern descriptors in the presence of noise, unusual vein presentations, and deformations.

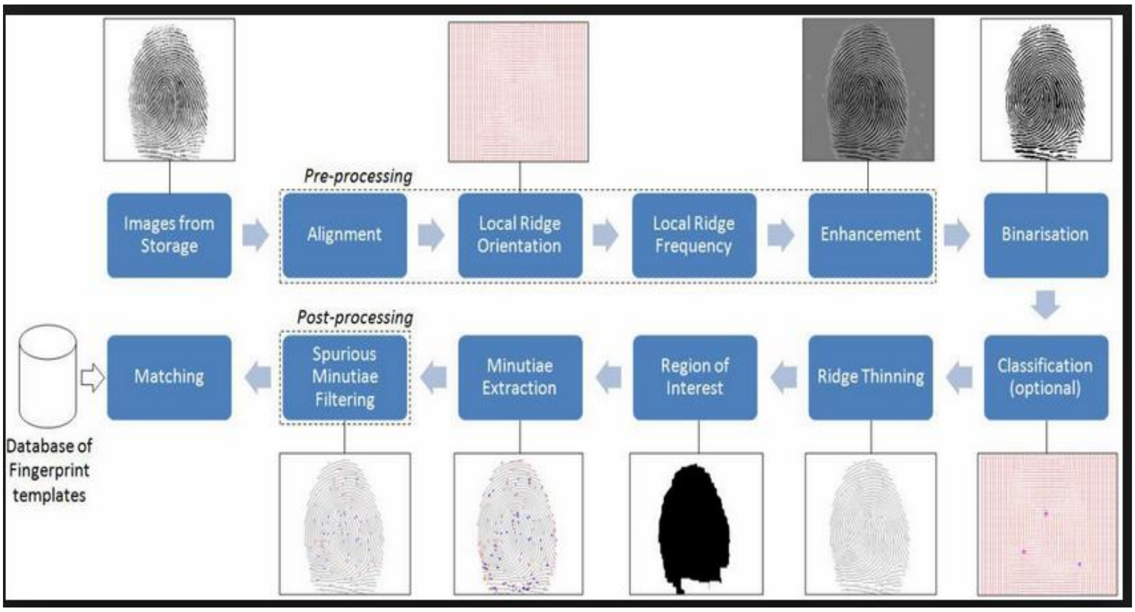

Fig. 1. Recognition Pattern in Fingerprint

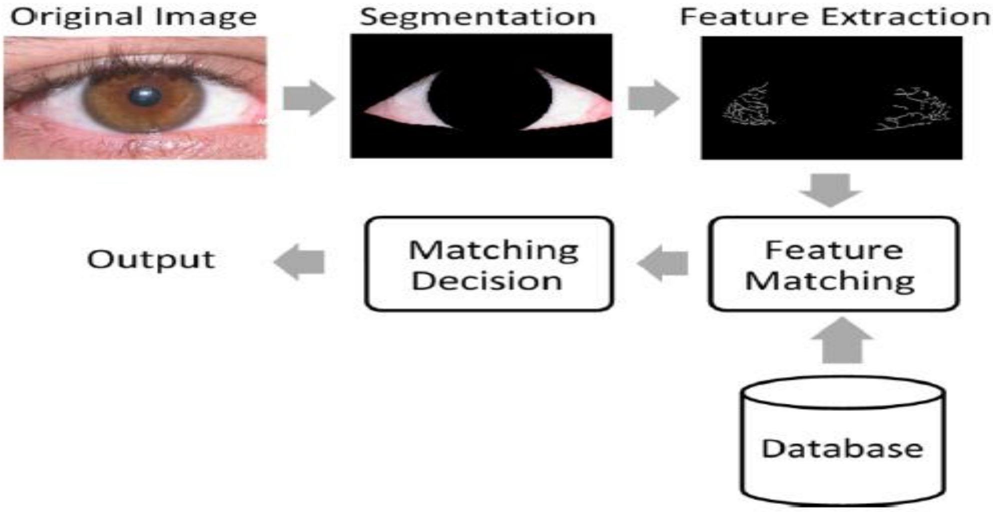

Fig. 2. Recognition of vein Pattern in sclera

V. CONCLUSION AND FUTURE WORK

Biometrics are a security approach that offers great assurance, but also presents users and implementers with a number of practical problems Biometrics offers a valuable approach to extending current security technologies that make it far harder for fraud to take place by preventing ready impersonation of the authorized user. Biometric is the most secure and convenient endorsement tool. It cannot be borrowed, robbed, or forgotten and faking one is practically impossible. Biometric technologies are evolving and emerging towards a large scale of use. Multimodal has several advantages over unimodal. Combining the results obtained by different biometric traits by an effective fusion scheme can significantly improve the overall accuracy of the biometric system. Multimodal system increases the number of individuals that can enroll. It provides resistance against spoofing. Sclera vein recognition is more accurate than any other biometric and it improves the overall accuracy of the system without compromising recognition and it provides more security than any other biometrics. The combination of both Sclera Vein and Finger Vein produce accurate results.

REFERENCES

1. Jain, A., Hong, L., & Pankanti, S. (2000). "Biometric Identification". *Communications of ACM*, 43(2), p. 91-98. DOI 10.1145/328236.328110
2. K. Jain, R. Bolle, and S. Pankanti (Eds) 1999, "*BIOMETRICS: Personal Identification in Networked Society*," Kluwer Academic Publishers
3. A. K. Jain, A. Ross, and S. Prabhakar, 2004, "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, pp. 4-20
4. Weaver, A.C. (2006). "Biometric Authentication", *Computer*, 39 (2), p. 96-97. DOI 10.1109/MC.2006.47
5. Jain, L.C. et al. (Eds.). 1999. *Intelligent Biometric Techniques in Fingerprint and Face Recognition*. Boca Raton, FL: CRC Press.
6. Nalini Ratha and Ruud Bolle, Automatic Fingerprint Recognition Systems (Springer: New York, 2004).
7. R. Brunelli and T. Poggio, "Face Recognition: Features versus Templates", IEEE Trans. on PAMI, 1993, (15)10:1042-1052
8. Zetter, Kim (2012-07-25). "Reverse-Engineered Irises Look So Real, They Fool Eye-Scanners", Wired Magazine. Retrieved 25 July 2012
9. Daugman, J., "High confidence visual recognition of persons by a test of statistical independence", IEEE *Transactions on Pattern Analysis and Machine Intelligence*, 15 (11), pp 1148-1161 (1993)
10. Wildes, Richard P, *Iris Recognition: An Emerging Biometric Technology,* Proceedings of the IEEE. Vol *85,* NO. 9, (1999), pp.1348-1363.
11. Kinnunen, Tomi; Li, Haizhou (1 January 2010). "An overview of text-independent speaker Recognition: From features to supervectors". *Speech Communication* 52 (1): 12–40.Doi:10.1016/j.specom.2009.08.009
12. Jean-Francois Bonastre, Louis-Jean Boe , Joseph P. Campbell , Douglas A. Reynolds , Ivan Magrin-Chagnolleau (September 2003)"Person Authentication by Voice: A Need for Caution"]. *Person Authentication by Voice: A Need for Caution*. 8th European Conference on Speech Communication and Technology. Geneva, Switzerland: isca-speech.org. Retrieved February 21, 2012.
13. Van Lancker and Kreiman "Familiar voice recognition: Patterns and parameters. Part I: Recognition of backward voices". Journal of Phonetics. pp. 19–38. Retrieved February 21, 2012.
14. Reynolds, Douglas; Rose, Richard (January 1995)."Robust text-independent speaker identification Using Gaussian mixture speaker Models", *IEEE Transactions on Speech and Audio Processing* 72–83. doi:10.1109/89.365379. ISSN 1063-6676. OCLC 26108901. Retrieved 21 February 2014
15. Juang, B. H.; Rabiner, Lawrence R. "Automatic speech recognition–a brief history of the technology development". p. 10. Retrieved 17 January 2015.
16. Houmani, Nesmaa; A. Mayoue, S. Garcia-Salicetti, B. Dorizzi, M.I. Khalil, M. Mostafa, H. Abbas, Z.T. Kardkovàcs, D. Muramatsu, B. Yanikoglu, A. Kholmatov, M. Martinez-Diaz, J. Fierrez, J.Ortega- Garcia, J. Roure Alcobé, J. Fabregas, M. Faundez-Zanuy, J. M. Pascual-Gaspar, V. Cardeñoso-Payo, C. Vivaracho-Pascual (March 2012). "BioSecure signature evaluation campaign (BSEC'2009): Evaluating online signature algorithms depending on the quality of signatures". *Pattern Recognition* 45 (3): 993–1003. doi: 10.1016/j.patcog.2011.08.008.
17. Faundez-Zanuy, Marcos (2007). "On-line signature recognition based on VQ-DTW". *Pattern recognition* 40 (3): 981–992. doi:10.1016/j.patcog.2006.06.007.
18. Miroslav Bača; Petra Grd and Tomislav Fotak "Basic Principles and Trends in Hand Geometry and Hand Shape Biometrics". New Trends and Developments in Biometrics. InTech. Retrieved 1 December 2013.
19. Levine DF, Richards J, Whittle M. (2012). Whittle's Gait Analysis Whittle's Gait Analysis Elsevier Health Sciences. ISBN 978-0702042652
20. Piérard, S.; Azrour, S.; Phan-Ba, R.; Van Droogenbroeck, M. (October 2013). "GAIMS: A reliable Non-intrusive gait measuring System". *ERCIM News* 95: 26–27.
21. N. A. Rahman, A. S. Mohamed, and M. E. Rasmy, "Retinal Identification," in *Cairo International Biomedical Engineering Conference*, 2008, pp. 1-4.
22. H. Borgen, P. Bours, and S. D. Wolthusen, "Visible-Spectrum Biometric Retina Recognition," in *Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing*: IEEE Computer Society, 2008.
23. E. Martinez-Perez, A. D. Hughes, A. V. Stanton, S. A. Thom, A. A. Bharath, and K. H. Parker, "Segmentation of retinal blood Vessels based on the second directional derivative and region growing," *Proceedings of International Conference on Image Processing*, 1999, pp. 173-176.vol. 2.
24. H. Narasimha-Iyer, J. M. Beach, B. Khoobehi, and B. Roysam, "Automatic Identification of Retinal Arteries and Veins From Dual-Wavelength Images Using Structural and Functional Features," *IEEE Transactions on Biomedical Engineering*, vol. 54, pp. 1427-1435, 2007.
25. Ostaff, Courtney. "Retinal Scans Do More Than Let You In The Door." Retrieved on 2007-04-02.