A Survey of Automated Biometric Authentication Techniques

Atul N. Kataria, Dipak M. Adhyaru (Member IEEE), Ankit K. Sharma, Tanish H. Zaveri

Abstract--**Biometric authentication refers to the automatic identification of a person by analyzing their physiological and/or behavioral characteristics or traits. Since many physiological and behavioral characteristics are unique to an individual, biometrics provides a more reliable system of authentication than ID cards, keys, passwords, or other traditional systems. A wide variety of organizations are using automated person authentication systems to improve customer satisfaction, operating efficiency as well as to secure critical resources. Now a day an increasing number of countries including India have decided to adopt biometric systems for national security and identity theft prevention, which 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. Various biometric authentication techniques are available for identifying 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. This paper aims to give a brief overview of the field of biometrics and summarize various biometric authentication techniques including its strengths and limitations.**

Index Terms - **Biometrics, Identification, Verification, Universal Identification program.**

I. INTRODUCTION

A biometric authentication system is basically a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological and/or behavioral characteristic possessed by the user. Physiological characteristics are related to the shape of the body, such as hand geometry, Palm print, face recognition, fingerprint, DNA, iris recognition, retina and odor. Behavioral characteristics are related to the behavior of a person, such as typing rhythm, gait, and voice. The method of identification based on biometric characteristics is preferred over traditional passwords and PIN based methods for various reasons such as: The person to be identified is required to be physically present at the time of identification and identification based on biometric techniques obviates the need to remember a password or carry a token. Since, today, a wide variety of applications require reliable verification schemes to confirm the identity of an individual, recognizing humans based on their body characteristics became more and more interesting in emerging technology applications.

The selection of a particular biometric for use in a specific application involves a weighting of several factors. Seven such factors to be used when assessing the suitability of any trait for use in biometric authentication: Universality, Uniqueness, Permanence, Measurability, Performance, Acceptability and Circumvention [1]. Universality means that every person using a system should possess the trait. Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another. Permanence relates to the manner in which a trait varies over time. Measurability or collectability relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets. Performance relates to the accuracy, speed, and robustness of technology used. Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed. Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute.

Examples of physiological and behavioral characteristics which are currently in use for automatic personal authentication include fingerprints, voice, iris, retina, hand geometry, face, handwriting, keystroke, and finger shape. But this is only a partial list as new measures such as gait, ear shape, head resonance, ECG and body odor are being developed all of the time. Because of the broad range of characteristics used, the imaging requirements for the technology vary greatly. Systems might measure a single one-dimensional signal, several simultaneous one-dimensional signals, a single two-dimensional image, multiple two dimensional measures, a time series of two-dimensional images or a three dimensional image [2].

II. BIOMETRIC AUTHENTICATION SYSTEM

Practically all the biometric authentication 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

978-1-4673-1719-1/12/$31.00©2013IEEE

appropriate measurement, translate this information into a template 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 verification or identification is done as shown in figure 1.

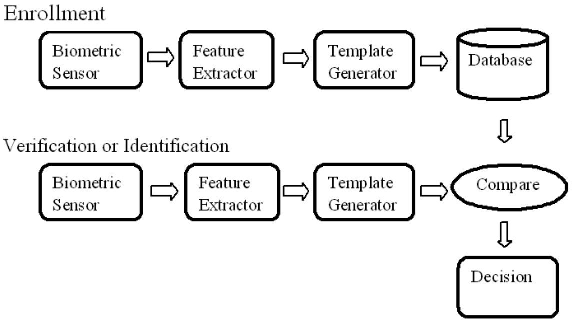


Fig.1 Biometric authentication process

An important distinction between biometric verification and identification lies in that verification is a one-to-one comparison, while identification is a one-to-many search in a database. They perform different functions since verification is used to confirm one's identity and identification is used to find one's identity [3].

III. Overview of Biometric Authentication Techniques

There are number of physiological and behavioral characteristics are used in automated biometric authentication system. Each biometric characteristic has its own strengths and weaknesses, and the choice depends on the application. No single biometric characteristic is expected to effectively meet the requirements of all the applications. The match between a specific biometric authentication technique and an application is depending upon the operational mode of the application and the properties of the biometric characteristic. A brief introduction to the biometric characteristic that is either currently in use or under development is given below [4]. At the end brief comparison of the biometric techniques based on seven factors is provided in Table I.

1. Fingerprint

Fingerprint-based authentication has been the longest serving, most successful and popular method for person identification and verification. Fingerprints of identical twins are different and also the prints on each finger of the same person. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. The uniqueness of a fingerprint is exclusively determined by the local ridge characteristics and their relationships. The ridges and valleys in a fingerprint alternate, flowing in a local constant direction. The two most prominent local ridge characteristics are: ridge ending and ridge bifurcation. A ridge ending is defined as the point where a ridge ends abruptly. A ridge bifurcation is defined as the point where a ridge diverges into branch ridges. Collectively, these features are called *minutiae*. Most fingerprint matching systems are based on four types of fingerprint representation schemes: grayscale image, phase image, skeleton image and minutiae. Due to its distinctiveness, compactness, and compatibility with features used by human fingerprint experts, minutiae-based representation has become the most widely adopted fingerprint representation scheme [5].

2. Palm Print

Like fingerprints, palms of the human hands contain unique pattern of ridges and valleys. The area of the palm is much larger than the area of a finger and, as a result, palm prints are expected to be even more distinctive than the fingerprints. Since palm print scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper [6]. Finally, when using a high resolution palm print scanner, all the features of the palm such as geometry features(width, length and area of a palm), ridge and valley features(minutiae and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric authentication system [4]. Generally in palm print based authentication system hand image of an individual is collected and then image preprocessing steps like Image thresholding, border tracing, segmentation, and ROI location are sequentially executed to obtain a square region which possesses the palm-print data.

3. Hand Geometry

Hand geometry based identification systems utilize the geometric features of the hand like length and width of the fingers, diameter of the palm and the perimeter. Hand geometry based biometric systems are gaining acceptance in low to medium security applications. One of the earliest automated biometric systems was installed during late 60s and it used hand geometry and stayed in production for almost 20 years. The technique is very simple, relatively easy to use and inexpensive. Dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy. Since hand geometry is not very distinctive it cannot be used for identification of an individual from a large population, but it can be used in a verification mode. Further, hand geometry information may not be invariant during the growth period of children. Limitations in dexterity (arthritis) or even jewelry may influence extracting the correct hand geometry information. There are even verification systems available that are based on measurements of only a few fingers instead of the entire hand. These devices are smaller than those used for hand geometry [7].

4. Iris

The iris is a thin, circular structure in the eye, responsible for controlling the diameter and size of the pupil and thus the amount of light reaching the retina. The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual

978-1-4673-1719-1/12/$31.00©2013IEEE

texture of the iris is formed during fetal development and stabilizes during the first two years of life. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. It is extremely difficult to surgically tamper the texture of the iris. Further, it is rather easy to detect artificial irises. An iris-recognition algorithm first has to localize the inner and outer boundaries of the iris (pupil and limbus) in an image of an eye. Further subroutines detect and exclude eyelids, eyelashes, and specular reflections that often occlude parts of the iris. The set of pixels containing only the iris is then analyzed to extract a bit pattern encoding the information needed to compare two iris images. A careful balance of light, focus, resolution and contrast is necessary to extract a feature vector from localized image. Although, the early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user-friendly and cost-effective [4].

5. Retina

The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. The network of blood vessels in the retina is so complex that even identical twins do not share a similar pattern. Although retinal patterns may be altered in cases of diabetes, glaucoma or retinal degenerative disorders, the retina typically remains unchanged from birth until death. The image acquisition requires a person to peep into an eye-piece and focus on a specific spot in the visual field so that a predetermined part of the retinal vasculature could be imaged. The image acquisition involves cooperation of the subject, entails contact with the eyepiece, and requires a conscious effort on the part of the user. All these factors adversely affect the public acceptability of retinal biometric. Retinal vasculature can reveal some medical conditions, e.g., hypertension, which is another factor deterring the public acceptance of retinal scan-based biometric system [4].

6. Face

Humans often use faces to recognize individuals and advancement in computing capability over the past few decades now enable similar recognition automatically. Face Recognition algorithms can be divided into two main approaches, geometric, which looks at distinguishing features(the location and shape of facial attributes such as the eyes, eyebrows, nose, lips and chin, and their spatial relationships), or photometric, which is a statistical approach that distills an image into values and compares the values with templates to eliminate variances. As researcher interest in face recognition continued, many different algorithms developed. Some of the Popular recognition algorithms include Principal Component Analysis , Linear Discriminate Analysis, Elastic Bunch Graph Matching Hidden Markov model and Multilinear Subspace Learning. A newly emerging trend, claimed to achieve improved accuracies, is three-dimensional face recognition. This technique uses 3D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin [8]. Another emerging trend uses the visual details of the skin, as captured in standard digital or scanned images. This technique, called skin texture analysis, turns the unique lines, patterns, and spots apparent in a person’s skin into a mathematical space [9]. Methods for face detection and recognition systems can be affected by pose, presence or absence of structural components, facial expression, occlusion, image orientation and imaging conditions. Available applications developed by researchers can usually handle one or two effects only; therefore they have limited capabilities with focus on some well-structured application. A robust face recognition system is difficult to develop which works under all conditions with a wide scope of effect.

978-1-4673-1719-1/12/$31.00©2013IEEE

7. Ear

Researchers have suggested that the shape and appearance of the human ear is unique to each individual and relatively little change occurs during the lifetime of an adult [10]. The ear growth between four months to eight years old is approximately linear, and after that it is constant until around 70 when it increases again [11]. Due to its stability and predictable changes, ear recognition is being investigated as potential biometric [10,11]. Generally, ear images can be acquired in a manner similar to face images, and used in the same scenarios. The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual [4].

8. Infrared thermogram

Thermographic cameras detect radiation in the infrared range of the electromagnetic spectrum and produce images of that radiation, called thermograms. Since infrared radiation is emitted by all objects above absolute zero according to the black body radiation law, thermography makes it possible to see one's environment with or without visible illumination. So it is possible to capture the pattern of heat radiated by the human body with an infrared camera. That pattern is considered to be unique for each person. It is a noninvasive method, but image acquisition is rather difficult where there are other heat emanating surfaces near the body. A related technology using near infrared imaging is used to scan the back of a fist to determine hand vein structure, also believed to be unique. Like face recognition, it must deal with the extra issues of three-dimensional space and orientation of the hand. Infrared sensors are prohibitively expensive which is a factor inhibiting wide spread use of the thermograms.

9. Voice

Voice recognition is the identification of the person who is speaking by characteristics of their voices, also called voice biometrics. Voice recognition has a history dating back some four decades and uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (size and shape of the throat and mouth) and learned behavioral patterns (voice pitch, speaking style). Physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions, and emotional state, etc. Voice is also not very distinctive and may not be appropriate for large-scale identification. A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text-independent voice recognition system recognizes the speaker independent of what she speaks. A text-independent system is more difficult to design than a text-dependent system but offers more protection against fraud. A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel [4].

10. Signature

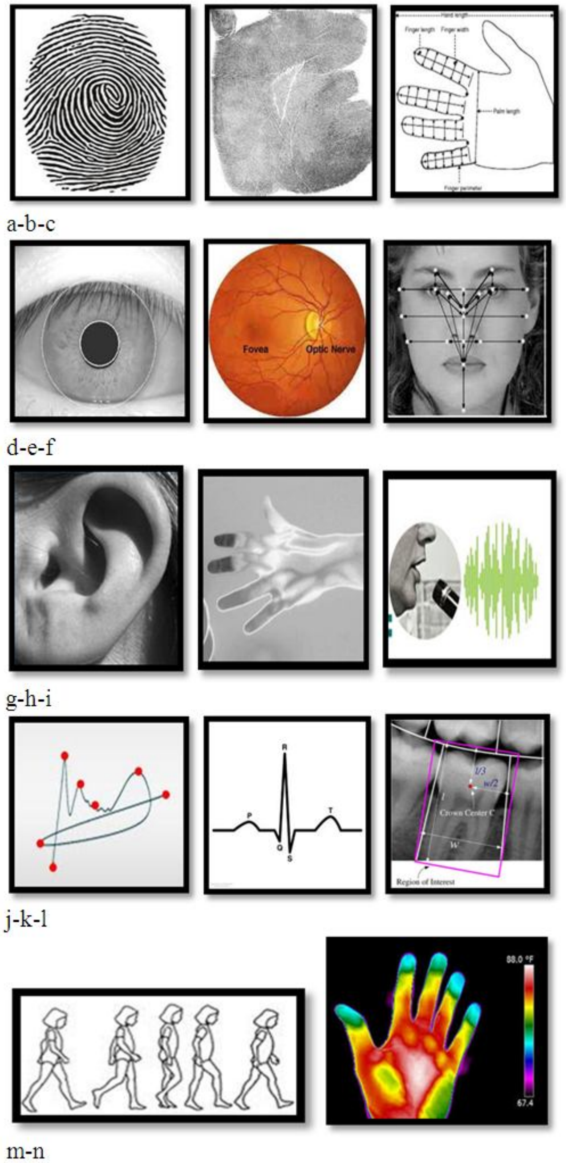
The way a person signs his or her name is known to be a characteristic of that individual. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of verification In addition to the general shape of the signed name, a signature recognition system can also measure pressure and velocity of the point of the stylus across the sensor pad. It can be operated in two different ways: Static and Dynamic. In Static mode, users write their signature on paper, digitize it through an optical scanner or a camera, and the biometric system recognizes the signature analyzing its shape, which is also known as "off-line". In dynamic mode, users write their signature in a digitizing tablet, which acquires the signature in real time. Dynamic recognition is also known as "on-line". Signatures may be change over a period of time and are influenced by physical and emotional conditions of a subject. Further, professional forgers may be able to reproduce signatures that fool the system.

11. Gait

Gait is the pattern of movement of the limbs of animals, including humans, during locomotion over a solid substrate. Gait is not supposed to be very distinctive, but is sufficiently discriminatory to allow verification in some low-security applications. Gait is a behavioral biometric and may not remain the same over a long period of time, due to change in body weight or major injuries involving joints or brain. Gait (an individual's way of walking) is captured using a video-camera from distance. Video and image processing techniques are employed to extract gait features for recognition purposes. Features used for person verification can be stride and cadence or static body parameters like height, the distance between head and pelvis, the maximum distance between pelvis and feet, and the distance between feet. Since gait-based systems use the video-sequence footage of a walking person to measure several different movements of each articulate joint, it is input intensive and computationally expensive.

12. Keystroke

It is believed that each person types on a keyboard in a characteristic way. This is also not very distinctive but it offers sufficient discriminatory information to permit identity verification. The technology uses a keyboard compatible with PCs and examines keystroke dynamics such as speed of typing, pressure on the key and timing information of the key down/hold/up events. Keystroke biometrics can use static text, where keystroke dynamics of a specific pre-enrolled text, such as a password is analyzed at a certain time, e.g., during the log on process. For more secure applications, free text should be used to continuously authenticate a user.



a-b-c

d-e-f

g-h-i

j-k-l

m-n

Fig.2 Biometric Characteristics: (a) fingerprint, (b) palm-print, (c) hand geometry, (d) iris, (e) retina, (f) face, (g) ear, (h) hand vein, (i) voice, (j) signature, (k) ECG, (l) dental X-ray, (m) gait, (n) hand thermogram

13. Odor

Each object spreads around an odor that is characteristic of its chemical composition and this could be used for distinguishing various objects. Odor recognition is a contactless physical biometric that attempts to confirm a person's identity by analyzing the olfactory properties of the human body odor. This is the perspective technique and still under development. There are no available commercial applications on the market yet.

14. DNA

Deoxyribonucleic acid (DNA) is a molecule that encodes the genetic instructions used in the development and functioning of all known living organisms and many viruses. DNA testing is a technique with a very high degree of accuracy. The statistical sampling shows a 1-in-6 billon chance of two people having the same profile. It is the most distinct biometric identifier available for human beings except for monozygotic twins. DNA does not change throughout a person's life; therefore its permanence is incontestable. The current processes for obtaining DNA samples are quite intrusive, requiring some form of tissue, blood or other bodily sample. Forensic scientists use DNA in blood, semen, skin, saliva or hair found at a crime scene to identify a matching DNA of an individual. This process is formally termed DNA profiling, but may also be called "genetic fingerprinting". In DNA profiling, the lengths of variable sections of repetitive DNA, such as short tandem repeats and minisatellites, are compared between people. Three issues limit the utility of this biometrics for other applications: 1) DNA matching is not done in real-time, 2) a physical sample must be taken, while other biometric systems only use an image or a recording, 3) privacy issues since DNA sample taken from an individual is likely to show susceptibility of a person to some diseases.

15. ECG & EEG

In recent times, biometrics based on ECG (electrocardiogram) and EEG (electroencephalogram) signals have emerged [12, 13]. The research group at University of Wolverhampton lead by Ramaswamy Palaniappan has shown that people have certain distinct brain and heart patterns that are specific for each individual. The advantage of such 'futuristic' technology is that it is more fraud resistant compared to conventional biometrics like fingerprints. However, such technology is generally more cumbersome and still has issues such as lower accuracy and poor reproducibility over time.

16. Dental X-ray

Forensic dentistry involves the identification of people based on their dental records, mainly available as radiograph images. The main purpose of forensic dentistry is to identify deceased individuals, for whom other cues of biometric identification may not be available. In forensic dentistry, the postmortem (PM) dental record is compared against antemortem (AM) records pertaining to some presumed identity. A manual comparison between the AM and PM records is based on a systematic dental chart prepared by forensic experts [14,15]. In this chart, a number of distinctive features are noted for each individual tooth. These features include properties of the teeth, periodontal tissue features, and anatomical features. Depending on the number of matches, the forensic expert rejects or confirms the tentative identity. There are several advantages for automating this procedure. First, an automatic process will be able to compare the PM records against AM records pertaining to multiple identities in order to determine the closest match. Second, while a manual system is useful for verification on a small data set, an automatic system can perform identification on a large database. Many researchers have successfully automated this process using image processing and pattern recognition techniques.

TABLE I

COMPARISON OF VARIOUS BIOMETRIC CHARACTERISTICS. H, M AND L REPRESENT HIGH, MEDIUM AND LOW RESPECTIVELY.

Biometric Characteristics	**Universality**	**Uniqueness**	**Permanence**	**Measurability**	**Performance**	**Acceptability**	**Circumvention**
Finger print	M	H	H	M	H	M	M
Palm print	M	H	H	M	H	M	M
Hand Geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Retina	H	H	M	L	H	L	L
Face	H	L	M	H	L	H	H
Ear	M	M	H	M	M	H	M
Thermogram	H	H	L	H	M	H	L
Voice	M	L	L	M	L	H	H
Signature	L	L	L	H	L	H	H
Gait	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
ECG	H	M	M	M	L	L	M

17. Multimodal biometrics

Due to external manufacturing constraints in sensing technologies as well as inherent limitations within each biometric, no single biometric method to date can warrant a 100% authentication accuracy and usage by itself. The situation can nevertheless be improved through a combination of multiple biometric sources and methods. This combination of multiple biometric methods or modalities is commonly referred to as multimodal biometrics fusion and such a system is often called a multibiometric system [16]. Such systems are expected to be more reliable due to the presence of multiple, independent pieces of evidence [17]. These systems are also able to meet the strict performance requirements imposed by various applications [l8].

IV. INDIA'S UNIVERSAL IDENTIFICATION PROGRAMME

India is currently implementing its Universal Identification (UID) program to provide a unique identification number based on biometric identifiers to each of its 1.25 billion

978-1-4673-1719-1/12/$31.00©2013IEEE

citizens. The government will then use the information to issue identity cards the word which is popularly known as *Aadhar Card*. The physical count began on February 2011. The Universal ID program is administered by the Unique Identification Authority of India (UIDAI). Although it is in early stages, the UID program is already the largest biometric identification program in the world with more than 200 million people enrolled as of January 2012[19].

UIDAI agents collect two iris scans, ten fingerprints, and a digital photograph from each enrollee. This multimodal system is advantageous because different biometrics is better suited to different tasks. Iris scans provide more data than fingerprints, essential for de-duplication, but fingerprints are easier and cheaper to authenticate. Having multiple measures also reduces the failure-to-enroll rate, as some people have worn fingerprints or damaged eyes [19]. The UID program is designed to be an "identity service provider" for both government programs and the private sector. Users from public and private agencies can verify people's identity against their biometric traits and Aadhar number. When queried, the UID database returns a simple yes or no response to the match; no personal information is provided, but users can prove their identity [19]. The total number of Aadhaar issued as of 16-September-2013 is 425 Million (42.5 Crore). This is more than 35% of the population of India. One in every three residents of India have an Aadhaar now. More details are available at the UIDAI portal [20].

V. CONCLUSION

In this age of digital impersonation, biometric techniques are being used increasingly as a hedge against identity theft. The premise is that a measurable physiological or behavioral characteristic is a more reliable indicator of identity than legacy systems such as passwords and PINs. The principal objective of this paper is to give an overview of the fast developing and exciting area of automated biometrics. Various biometric authentication techniques are presented that are either currently in use across a range of environments or still in limited use or under development or still in the research realm.

VI. REFERENCES

[1] Jain, A.K.; Bolle, R.; Pankanti, S., eds. (1999). Biometrics: Personal Identification in Networked Society. Kluwer Academic Publications. ISBN 978-0-7923-8345-1.

[2] James Wayman, Anil Jain, Davide Maltoni and Dario Maio, "An Introduction to Biometric Authentication Systems". In *Biometrics:Technology, Design and performance evaluation*. Springer Publications. ISBN 978-0-7923-8345-1.

[3] Qinghan Xiao. *Biometrics—Technology, Application, Challenge And Computational Intelligence Solutions*, May 2007 | Ieee Computational Intelligence Magazine.

[4] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 14, No. 1, pp 4-19, January 2004.

[5] Naser Zaeri, Minutiae-based Fingerprint Extraction and Recognition, *Biometrics*, Edited by Jucheng Yang, ISBN 978-953-307-618-8.

[6] D. Zhang and W. Shu, "Two novel characteristic in palmprint verification: Datum point invariance and line feature matching," *Pattern Recognit.*, vol. 32, no. 4, pp. 691–702, 1999.

[7] Kresimir Delac, Mislav Grgic, "a survey of biometric recognition methods", *46th International Symposium Electronics in Marine*, ELMAR-2004, 16-18 June 2004, Zadar, Croatia.

[8] Williams, Mark. "Better Face-Recognition Software". Retrieved 2008-06-02.

[9] Bonsor, K. "How Facial Recognition Systems Work". Retrieved 2008-06-02.

[10] A. Iannarelli. *Ear Identification*. Paramont Publishing Company, 1989.

[11] M. Burge and W. Burger. "Ear biometrics in computer vision". In 15th *Inter-national Conference of Pattern Recognition*, volume 2, pages 822–826, 2000.

[12] R. Palaniappan, "Electroencephalogram signals from imagined activities: A novel biometric identifier for a small population," published in E. Corchado et al. (eds): "Intelligent Data Engineering and Automated Learning – IDEAL 2006", Lecture Notes in Computer Science, vol. 4224, pp. 604–611, Springer-Verlag, Berlin Heidelberg, 2006. DOI:10.1007/11875581_73.

[13] R. Palaniappan, and S. M. Krishnan, "Identifying individuals using ECG signals," Proceedings of International Conference on Signal Processing and Communications, Bangalore, India, pp.569–572, 11–14 December 2004. DOI:10.1109/SPCOM.2004.1458524.

[14] I.A. Pretty, D. Sweet, A look at forensic dentistry—Part 1: the role of teeth in the determination of human identity, Br. Dent. J. 190 (7) (2001) 359–366.

[15] American Board of Forensic Odontology, Body identi'cation guidelines, J. Am. Dent. Assoc. 125 (1994) 1244–1254.

[16] Ross, A. A., Nandakumar, K., and Jain, A. K. Handbook of Multibiometrics(Springer Publisher), International Series on Biometrics, Vol. 6, 2006.

[17] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, R. P. W. Duin, "Is independence good forcombining classifiers?," *in Proc. Int. Conf. Pattern Recognition (ICPR)*, Vol. 2, Barcelona, Spain, 2001, pp. 168-171.

[18] L. Hong, A. K. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Trans. Pattern Analysis Machine Intell.*, Vol. 20, pp. 1295-1307, December 1998.

[19] Building a Biometric National ID: Lessons for Developing Countries from India's Universal ID Program, Alan Gelb and Julia Clark, The Center for Global Development, October 2012, http://www.cgdev.org/doc/full_text/GelbClarkUID/1426583.html

[20] Aadhaar - Unique Identification. Portal.uidai.gov.in (17 November 2010).