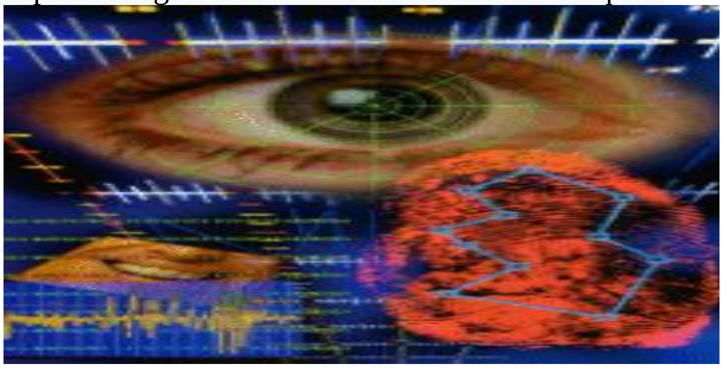
ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 2, April 2012

Evaluating the Capability of Biometric Technology

Sanjay Tiwari, Guangmei Zhai# , Sue A. Carter, and Shikha Tiwari*
Department of Physics, University of California,Santa Cruz ,CA 95060 USA
#Huazhong University of Science and Technology, Wuhan, Hubei 430074, China
*State Forensic Science Laboratory, Raipur (CG) 492010 India

Abstract:

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. “Biometrics is a complex technology but when supported by new services and improved processes, this technology can lead to profound improvements.The biometrics methods have seen significant improvement in performance and robustness over the last few years, but most of the systems reported perform well in controlled operating scenarios, and their performance deteriorates significantly under real world operating conditions, and far from satisfactory in terms of robustness and accuracy, vulnerability to fraud and forgery, and use of acceptable and appropriate authentication protocols. To address some challenges, and the requirements of new and emerging applications, and for seamless diffusion of biometrics in society, there is a need for development of novel paradigms and protocols, and improved algorithms and authentication techniques.

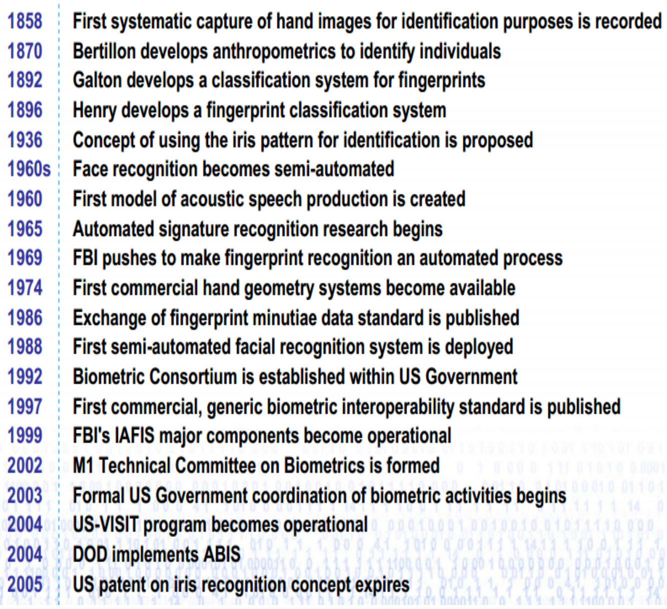


I INTRODUCTION

Biometrics is a sparkling word in the world of science and technology. Since, after 9/11 biometrics is getting a titanic attention all over the world by scientist, researchers and engineers. Now days everywhere in the world, especially in the western part of the world, security is given the top priority to counter the possible treats from terrorists and hence biometrics and security are the synonyms. Biometric systems are spreading rapidly at all security prone areas such as airports, banks, offices also with documentation like passport, identity card, driving license, etc. Reliable user identification is increasingly becoming important in the Web enabled world today and there has been a significant surge in the use of biometrics for user identification. Many corporate heads use laptops and personal digital assistants (PDAs) loaded with sensitive business and personal information. According to the Gartner group, over 250,000 mobile gadgets are lost or stolen every year, and only 25-30 per cent of these ever make it back to their rightful owners. Such mishaps have created a dire need to ensure denial of access to classified data by unauthorized persons.Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

Business organizations have been highlighting the importance of ascertaining a user's identity before permitting access to confidential information. In a race to improve security infrastructures faster than hackers and stealers can invent to penetrate passwords and firewalls, new technologies are being evaluated to confirm or deny user authentication.

Given the pervasive use of passwords and identification codes for user authentication across all aspects of our daily life, attackers have developed powerful password cracking codes. Well, thanks to biometrics, there is a way. Biometrics modes of identification have been found to be the most compelling and intriguing authentication technique. Biometrics are automated methods of recognizing a person based on his physiological or behavioural characteristics. Tokens can be lost, stolen or duplicated and passwords can be forgotten or shared. However, biometrics can authenticate you as you. The Timeline of Biometrics is given:

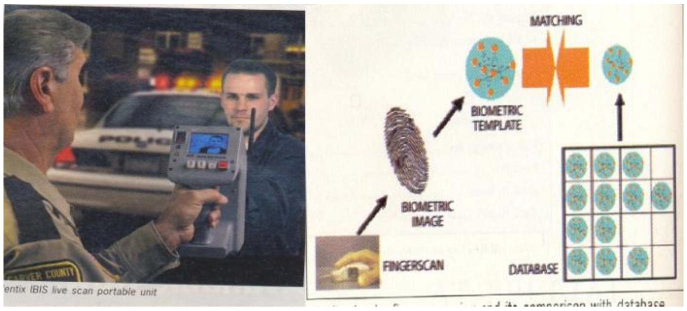


1858	First systematic capture of hand images for identification purposes is recorded
1870	Bertillon develops anthropometrics to identify individuals
1892	Galton develops a classification system for fingerprints
1896	Henry develops a fingerprint classification system
1936	Concept of using the iris pattern for identification is proposed
1960s	Face recognition becomes semi-automated
1960	First model of acoustic speech production is created
1965	Automated signature recognition research begins
1969	FBI pushes to make fingerprint recognition an automated process
1974	First commercial hand geometry systems become available
1986	Exchange of fingerprint minutiae data standard is published
1988	First semi-automated facial recognition system is deployed
1992	Biometric Consortium is established within US Government
1997	First commercial, generic biometric interoperability standard is published
1999	FBI's IAFIS major components become operational
2002	M1 Technical Committee on Biometrics is formed
2003	Formal US Government coordination of biometric activities begins
2004	US-VISIT program becomes operational
2004	DOD implements ABIS
2005	US patent on iris recognition concept expires

Biometrics is a means of using parts of the human body as a kind of permanent password. Just as your fingerprints are unlike those of any other person, your eyes, ears, hands, voice, and face are also unique. Technology has advanced to the point where computer systems can record and recognize the patterns, hand shapes, ear lobe contours, and a host of other physical characteristics. Using this biometrics, laptop and other portable devices can be empowered with the ability to instantly verify your identity and deny access to everybody else.

II THE UNDERLYING IDEA

Once identified, the physical characteristics can be exactly measured and analyzed. The statistical use of the characteristic variations in unique elements of living organisms is known as biometrics. Biometrics data of human beings can be collected and analyzed in a number of ways, and has been introduced as a mode of personal identification. Biometric systems automatically verify or recognize the identity of a living person based on physiological or behavioral characteristics. Physiological characteristics pertain to visible parts of the human body. These include fingerprint, retina, palm geometry, iris, facial structure, etc. Behavioural characteristics are based on what a person does. These include voice prints, signatures, typing patterns, keystroke pattern, gait, and so on. A variety of factors, such as mood, stress, fatigue, and how long ago you woke up, can affect behavioural characteristics. Voice print is a fine series of spectral power density plots that depict how the energy in one's voice at different frequencies varies with time as one vocalizes a word or phrase. Voice experts say that sufficient characteristics of one's voice print remain constant under all circumstances, enabling these plots to reliably verify one's identity while physiological traits are usually more stable than behavioural traits; systems incorporating them are typically more intrusive and more expensive to implement



III HIGHER SECURITY COUPLED WITH CONVENIENCE

Using biometrics for identifying and authenticating human beings offers unique advantages over traditional methods. Tokens, such as smart cards, magnetic stripe cards, and physical keys can be lost, stolen, or duplicated. Passwords can be forgotten, shared, or unintentionally observed by a third party. Forgotten passwords and lost smart cards are a nuisance for users and waste the expensive time of system administrators. In biometrics the concerned person himself is the password, as biometrics authentication is based on the identification of an intrinsic part of a human being.

The biometrics technique can be integrated into applications that require security, access control, and identification or verification of users. Biometrically secured resources effectively eliminate risks, while at the same time offering a high level of security and convenience to both the users and the administrators.

IV APPLICATIONS IN USE

Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies.

Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming socially acceptable and cost effective. More information about biometrics, standards activities, government and industry organizations and research initiatives on biometrics can be found throughout this website.

A number of fascinating biometric applications are already in use, with many more on the drawing boards. Banks and financial institutions are experimenting with biometric modes of authentication in automated teller machines (ATMs) to combat card fraud.

Nationwide Building Society, the UK, has incorporated an iris recognition system at ATMs. A camera takes a digital record of each user's iris. The iris print is stored in a database to verify personal identity during transactions.

Iris recognition subsystem is also being incorporated into ATMs in Japan.

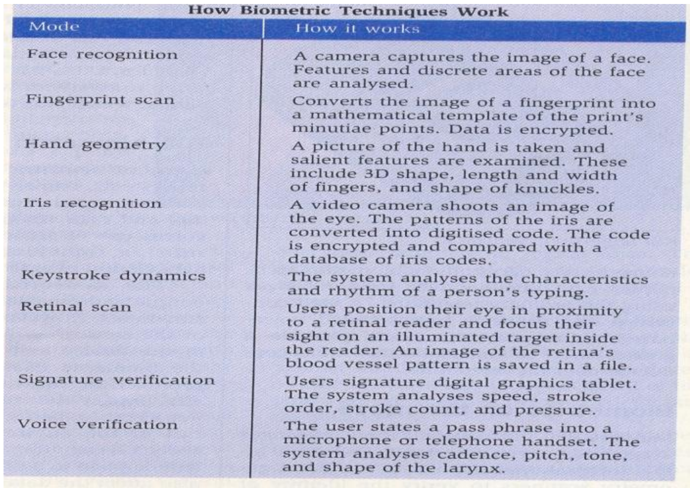
Keystroke biometrics provides a foolproof authentication solution. The gap between consecutive keystrokes when typing the access code and typing rhythm are unique to a user, so even if an unauthorized person discovers the access code, he can't access the system unless he knows the user's typing rhythm also.

A multi application travel card would enable the holders to participate in various frequent flier and border control systems as well as pay for air ticket, hotel room, etc. all with one convenient token.

A biometric chip reader incorporated into a PC can facilitate secure Internet based online transactions. Applications that are being developed to accept biometric data include computer networks, cars, cellular phones, and hoards of other types of embedded systems. Biometrics could authenticate e-mail and other documents transmitted via computer networks.

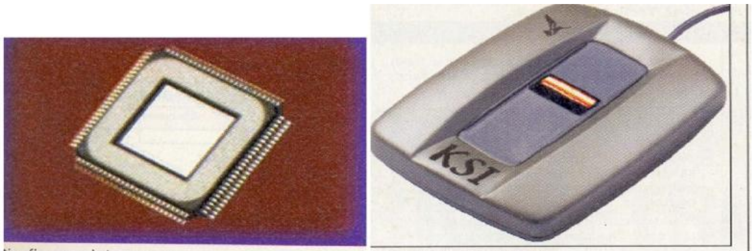
In hospitals, biometric techniques could replace ID bracelets to establish patients' identities, for instance, during blood administration.

With existing voice-transmission technology, voice recognition biometric techniques can function over long distances using the ordinary telephone. A well-conceived and properly implemented voice based security system could provide a greater safety to financial transactions conducted over the telephone



How Biometric Techniques Work

Mode	How it works
Face recognition	A camera captures the image of a face. Features and discrete areas of the face are analysed.
Fingerprint scan	Converts the image of a fingerprint into a mathematical template of the print's minutiae points. Data is encrypted.
Hand geometry	A picture of the hand is taken and salient features are examined. These include 3D shape, length and width of fingers, and shape of knuckles.
Iris recognition	A video camera shoots an image of the eye. The patterns of the iris are converted into digitised code. The code is encrypted and compared with a database of iris codes.
Keystroke dynamics	The system analyses the characteristics and rhythm of a person's typing.
Retinal scan	Users position their eye in proximity to a retinal reader and focus their sight on an illuminated target inside the reader. An image of the retina's blood vessel pattern is saved in a file.
Signature verification	Users signature digital graphics tablet. The system analyses speed, stroke order, stroke count, and pressure.
Voice verification	The user states a pass phrase into a microphone or telephone handset. The system analyses cadence, pitch, tone, and shape of the larynx.



io fingerprint sensor

KSI fingerprint sensor

.

V BIOMETRICS ON THE MOVE

Immigration and naturalization passenger accelerated service systems (INP ASS) allow international airports to use hand geometry scanners to verify the identity of travelers. Airports are testing face recognition scanners to help weed out terrorists.

One of the most hotly pursued applications of biometrics is handheld. Researchers are working on means to integrate eye scanners, fingerprint readers, and voice recognition systems into mobile phones, PDAs, and laptops. Scanners are getting smaller, cheaper, and more accurate, and can be used in mobile gadgets without sprucing up the size, cost, and power consumption. Not only biometrics renders handheld and laptops worthless to would-be stealers, it could also eliminate fraudulent transactions. Mobile manufacturers and wireless operators are incorporating voice and fingerprint scanning techniques in their devices.

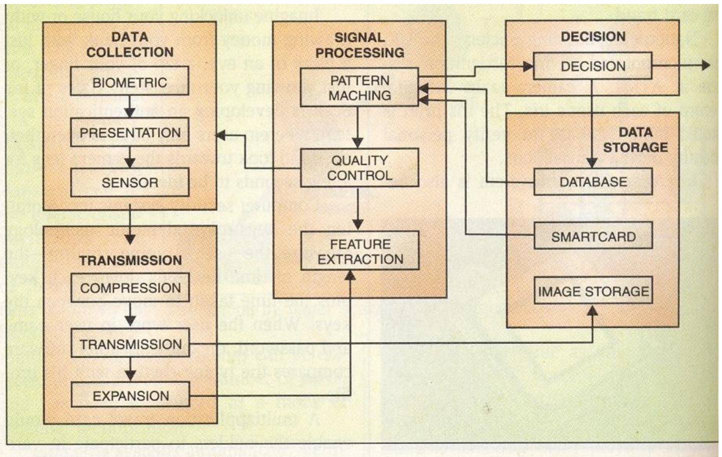
Voice is an obvious preference for mobile phones. Since it doesn't require any extra hardware in the device, it is naturally integrated into the way people use phones. All the processing is done on the mobile phone system that stores the reference voiceprints, which are as unique as a fingerprint, looking for particular patterns of tone, inflection, and behaviour in a voice. This ensures that a real person, not a tape recording, is on the line.

VI THE BIOMETRIC MODEL

A generic biometric model consists of five subsystems, namely, data collection, transmission, signal processing, decision making, and data storage. Data collection involves use of sensors to detect and measure an individual's physiological or behavioural characteristics.

The measured biometric must be unique and repeatable over multiple measurements. However, technical parameters of the sensor, as well as the ergonomics of the device and the manner in which the biometric characteristic is presented to effect the measurement, could eventually impact the outcome of the system. For instance, background noise and acoustics of the environment may impact a speech recognition system, while the pressure applied to a fingerprint scanner might also affect the data. The data collection subsystem most directly impacts the user. Sensor specifications determine the intrusiveness of the system. Intrusiveness is the degree to which the user feels that the measurement process violates his personal space, and is often correlated to how close the user has to be near the sensor. For instance, a retinal scan, which requires close proximity to the camera, is considered far more intrusive than a voice recognition system.

Not all biometric systems process and store data on the measuring device. Often measurement is made using a relatively simple device to a computer or server for processing and/or storage. Depending on the system, the data may be relatively large and thus would need to be compressed for quick transfer. The compression algorithm needs to be selected carefully, otherwise it may introduce some artifacts that



Block diagram of a biometric model

In fingerprint scanning systems, wavelet scalar quantisation is often preferred to JPEG compression due to the blockiness that the latter produces at high compression ratios. The data can also be transmitted to the database for storage as raw data.

The signal processing subunit uses feature extraction algorithms to extract true biometric information from the sample in the presence of noise introduced during data collection and transmission. Additional measurements are made if any flaw or corruption is noted, to ensure good quality.

Pattern matching involves comparing the feature sample to a stored sample. (Biometric data can be stored locally on the biometric device, some central database/ server, or on a smart card issued to users.) The result of comparison is sent to the decision system to determine the match.

The decision subsystem uses statistical methods to confirm authentication if the variance between the sample and template data is within a certain threshold.

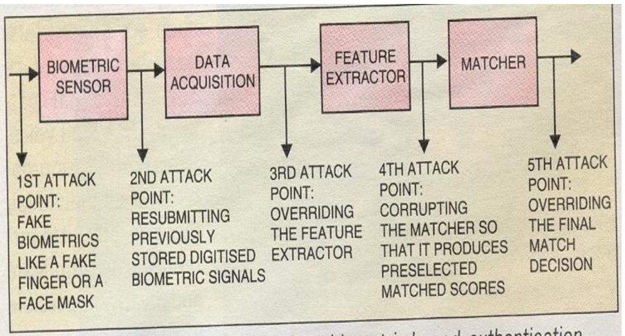
VII SYSTEM QUALITY:

The quality of a biometrics authentication algorithm is specified in terms of false rejection rate (FRR) and false acceptance rate (FAR). FRR indicates the percentage of instances an authorised individual is falsely rejected by the system. FAR states the percentage of instances an unauthorised individual is falsely accepted by the system. FRR and FAR are diametrically opposed, therefore increasing the FAR will lower the FRR, and vice-versa. FRRs and F ARs can be adjusted according to the needs of a given security system.

The biometric system should be able to account for permanent/semi-permanent changes in authorized / unauthorized users. For instance, a user's biometric characteristics, even if these are physiological, can change over time. People can grow beards, injure their hands, change their accent become better typists, change their hairstyles, and so on. Robust biometric systems are able to meet these contingencies by slightly modifying the template for accepted authentication situations. The user's profile in the database adapts to changes in the user's biometric features.

IX VULNERABILITY TO ATTACKS

In a biometrics based authentication system,there are fine points vuleranable to attacks by invaders as shown in the figure


BIOMETRIC SENSOR
DATA ACQUISITION
FEATURE EXTRACTOR
MATCHER
1ST ATTACK POINT: FAKE BIOMETRICS LIKE A FAKE FINGER OR A FACE MASK
2ND ATTACK POINT: RESUBMITTING PREVIOUSLY STORED DIGITISED BIOMETRIC SIGNALS
3RD ATTACK POINT: OVERRIDING THE FEATURE EXTRACTOR
4TH ATTACK POINT: CORRUPTING THE MATCHER SO THAT IT PRODUCES PRESELECTED MATCHED SCORES
5TH ATTACK POINT: OVERRIDING THE FINAL MATCH DECISION

Five points vulnerable to attacks in a biometric-based authentication system

X INDIAN INITIATIVES

In India our security system rely on old fashioned system adopted by police and other couple of security agencies like CBI and RAW. With changed world scenario due to continual treats from terrorist organizations, India is also facing many challenges including cross border terrorism, drug trafficking, ill-legal immigrants from neighboring countries. Now slowly but steadily Indian security systems are also adapting the biometric system. In India not many institute are involved with their research activities related with biometrics. Bio Enable Technologies, Pune, is a software company that develops biometric products to cater to the tough Indian working conditions and environments. The firm has developed intelligent biometric solutions for physical access control, banking transaction, timing, and attendance applications.

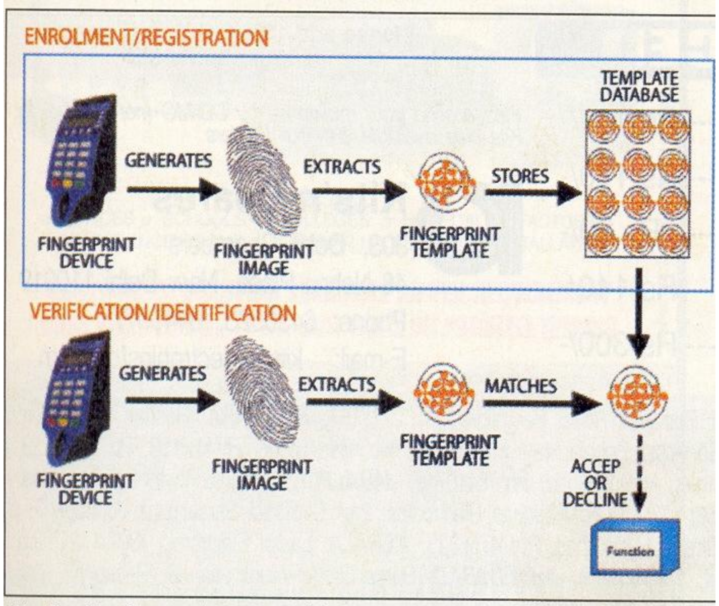
“With advances in**biometrics technology** and improvements in IT infrastructure, there is a growing acceptance of **biometric recognition technologies** in our daily lives and this acceptance will grow with time. In the coming years, Accenture believes businesses and governments alike will introduce **biometric technologies** into many of their operations to enable secure access to services, drive efficiencies, and increase public safety and security.” There is talk of using **ATM** machines in **India’s rural areas**, where a user can conduct a transaction by simply pressing his or her thumb on the senor, pushing appropriate, colour-coded button for desired denominations and walking away with cash and a receipt. “The latest commercially viable biometric solution is the **‘car seat’** developed by the scientists of **‘Advanced Institute of Industrial Technology** ‘which can identify a person who is sitting on it. The success rate is 98 percent. Now we are hearing that some researchers are conducting research on the dog’s heightened olfactory ability,”

Social sector schemes in **India** are also planning to use **biometric devices** for ensuring proper identification of those who are entitled to their payments. The **government of India’s** MNREGA initiative for creating jobs in the rural areas has made use of ICT devices and biometric databases in some pilot projects. At times such projects have been plagued with the problem of ghost workers and of the local leaderships appropriating the job cards. But with the use of biometric and **GPS** enabled ICT devices on work sites, it will become possible to conduct biometric attendance of the workers.

The **UIDAI** initiative of the **government** is using **biometric systems** for providing unique digital identity to**India’s** billions of people, including the poor and underprivileged communities. As the poor in this country often lack the documents to prove that they are entitled to government schemes, they are forced to pay bribe for obtaining benefits. The **foolproof biometric systems** like retina scan, face scan and fingerprinting that are being used for creation of unique UID Cards will make it possible for many more Indians to gain easy access to all kinds of benefits. The UID could eventually turn into the world’s largest biometric database.

Bio Enable has introduced a fingerprint-based identification terminal for use in factories, defence installations, public Kiosks, offices, retail outlets, etc.The fingerprint system translates illuminated images of fingerprints into digital code. The digital code is subjected to system software code for verification/ authentication of requested users and enrollment/registration of new users' fingerprints.

CMOS image sensors capture high-contrast, high-resolution fingerprint images that are virtually distortion-free. Powerful algorithms developed by Bio enabled extract minutiae data from the images to map the distinguished characteristics of fingerprint ridge ends, bifurcation, loops, splits, and upper and lower cores. The data is then converted into a template and stored in the database.



Bio Enable fingerprint recognition system

. To identify or verify, the algorithm compares the new template with the extracted minutiae points from the stored sample. The entire matching process takes roughly one second.

Siemens Information Systems Ltd (SISL), Bangalore, has developed a text independent autonomous speech recognition system to identify and authorize a speaker by analyzing his voice. Central Forensic Science Laboratories, Chandigarh, uses this system to track down and identify criminals by comparing their voice samples using SISL software. Other innovations of SISL include fingerprint identification and management system (FIMS, language-independent speech recognition system, and optical character recognition system. SISL is developing low-cost chips that can be fitted into cars and toys. These chips will store fingerprint of the user and allow selective access to devices and homes.

Axis Software, Pune, deals in fingerprint, iris, and face recognition technology and is planning to add voice recognition technology to its range of authentication products and systems. The Axis system stores biometric records in an record by itself is of no use to a stealer and cannot be reconstructed to reveal , person's identity to someone else.

Biometric Society of India (INBIOS), affiliated to the International Society of Computational Biology (ISCB), provides innovative professional solutions and services dedicated to bioinformatics.

XI **GLOBAL DEVELOPMENTS**

.

Internet security. Litronix, USA, a leading provider of public key infrastructure (PKI)based Internet security solutions, has developed biometric identification techniques for use in electronic data applications such as digital networks and smart cards. Apart from iris, voice and handwritten signature recognition can be used for authentication purposes when digitally signing a document or obtaining access to secure WebPages. The smart card, integrating voice and handwritten functions, incorporates the appropriate biometric template to deliver the final match and authorization.

The company plans to incorporate capture, manipulation, enrollment, and extraction features in the smart card reader also.

Biometric smart cards. Polaroid and Atmel have developed secure identity cards that merge ultra-secure smart cards, fingerprint verification, biometric identification, and digital imaging. These cards will be used in e-commerce, online, remote access, and any IT environment where authentication is required.

The information stored in the card is protected by circuits inside the card that perform encryption/decryption of the data in the card. The tiny smart card circuits in these ID cards are actually integrated circuits, called smart card ICs, supplied by Atmel. Atmel's smart card ICs can perform critical encryption; decryption functions within the card and are able to securely identify the person or system reading the card.

Biometrics cellulars. Fujistu Microelectronics has developed an innovative fingerprint identification system that combines sweep sensor technology with advanced algorithms to provide a powerful, dependable, easy-to-use authentication for PDAs, cell phones, and other mobile devices. The sensor measures just 1.28xO.20 cm and is powered by sophisticated algorithms that generate unique minutiae templates that correspond to specific fingerprint features. A single-fingerprint sweep across the sensor captures fingerprint features to rapidly authenticate users of cell phones and PDAs.

Cyber security. Cyber SIGN, USA, has built-in signature security management features of Adobe Acrobat 4.0 software. This software enables the handwritten signature to be included as an electronic signature in any Acrobat portable document format

(PDF) file on the Web. Anyone can online use his handwritten signature to authorize and sign electronic Acrobat documents. Costs involved in businesses are reduced, as signed documents and forms are available online, and productivity and security are increased when vendors and suppliers can quickly access signed, secure, and trusted electronic documents.

Recently the **leading technology company,IBM**, presented its forecast for 2012 in a blog, which carried this interesting quote, "Biometric data – facial definitions, retinal scans and voice files – will be composited through software to build your DNA **unique online password**." The technology that can be used to identify oneself without using passwords and IDs is already there. "Fingerprint reader, **Face recognition**, Iris scanning, **Voice recognition**, Palm Scanners and Retina Scanners have been deployed according to the sensitivity and security needs of the respective organizations," . In times to come you might not even need to use your debit card for withdrawing money from **ATM**. You will only have to look into the camera at the **ATM** booth and speak your name

XII MULTIBIOMETRICS

Multibiometrics is a system, which implements two or more biometric systems and performs the function of verification or identification. For instance, mutibiometrics can combine fingerprint recognition and hand geometry with iris recognition and speaker verification to give foolproof identification. In fact, a multimodal biometric system has been introduced, which integrates face recognition, fingerprint recognition, and speaker verification in making a personal identification. XIII

CONCLUSION

Different modes of biometrics have individual advantages suiting specific applications. Because of their security, speed, efficiency and convenience, biometric authentication systems might soon become the standard for access control. For the success of a particular biometric in a given application, one has to consider factors like performance in terms of false acceptance and False Rejection Rates, scalability, user privacy and system security. Adequate consideration should be given to the aspect of social acceptance, system cost and ease of use as well. With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data. The unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks may be prevented by replacing PINs by biometric techniques. PINs and passwords may be forgotten, and token-based methods of identification like passports and driver's licenses may be forged, stolen, or lost. The increased need of privacy and security in our daily life has given birth to this new area of science. It will be interesting to watch the future impact that they will have on our day-today lives.

REFERENCES

1. A. Rattani, B. Freni, G. L. Marcialis and F. Roli, "Template update methods in adaptive biometric systems: a critical review," 3rd International Conference on Biometrics, Alghero, Italy,2009, pp. 847-856,
2. M. McConnell"KeyNote Address.". Biometric Consortium Conference. Tampa Convention Center, Tampa, Florida,2009

3. . B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs," Pattern Analysis and Machine Intelligence, IEEE Transactions on, 2006,vol. 28, pp. 1892-1901

4. M. Savvides, B. V. K. V. Kumar, and P. K. Khosla, ""Corefaces"- Robust Shift Invariant PCA based Correlation Filter for Illumination Tolerant Face Recognition," presented at IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'04), 2004.

5. M. A. Dabbah, W. L. Woo, and S. S. Dlay, "Secure Authentication for Face Recognition," presented at Computational Intelligence in Image and Signal Processing, 2007. CIISP 2007. IEEE Symposium on, 2007.

6. A.K. Jain. And A.Ross "Introduction to Biometrics". In Jain, AK; Flynn, P; Ross, A. *Handbook of Biometrics*. Springer.2008, pp. 1–22. .

Dr. Sanjay Tiwari is a US Fulbright Scholar and Senior Associate ICTP Trieste Italy, post graduated from India and joined Cavendish Laboratory, University of Cambridge, UK as Visiting Fellow for Post-doctoral advanced research on Fabrication and Physical simulation of Organic Light emitting Diodes for Display applications. He has been conferred ,UKIERI Award of British Council, London ,Commonwealth fellowship and SAARC Fellowship,UGC Research Award and Best Young Scientist Award of India for his research contributions. He has been at University of California, Santa Cruz as Visiting Professor and Distinguished Visiting Fellow at IBM Almaden Research Center, San Jose California.