Cellular Phone: A Contemporary Tool for Biometric Implications

Neeraj Kumar, Raees A. Khan, and Dhirendra Pandey, *Senior Member, IACSIT*

***Abstract*—The specific functionality in current inventions of smart cell phones is attracting biometric engineering globally. With sensors, including GPS, vision, audio, light, temperature, direction, and acceleration sensors, cellular communication technologies are being as an imperative tool for biometrics in application to self monitoring and inflexible security. In present, cellular phones are most common electronic device in the world but most of cellular phone users are unaware about the advance biometric technology instead of PIN security. The subscribers of wireless technology have a need for better service to secure their unique identification into a running carrier device. The popularity of cell phones, embryonic nature of the cellular communication and easy to deliver desired information, are attracting to bioengineers for adopting as a prospected biometrics tool. This paper presents a discussion and theoretical concepts regarding biometric implications in smart cell phones to get a transparent unique identification globally.**

***Index Terms*—Biometric, smart cellular phone, identification, security, unique identity.**

I. Introduction

In information technology, biometrics refers to technologies that measure and analyzes human body characteristics, such as such as fingerprint, iris pattern, retina image, face or hand geometry, or a behavioral characteristic such as voice, gait or signature for authentication purposes [1]. Biometric technology uses these characteristics to identify individuals automatically. Ideally the characteristic should be universally present, unique to the individual, stable over time and easily measurable. No biometric characteristics have been formally proven to be unique, although they are usually sufficiently distinct for practical uses. Different biometrics will be more suitable for different applications depending, for example, on whether the aim is to identify someone with their co-operation or from a distance without their knowledge. The biometric can be defined as life - measure. It is used in security and access control applications to mean measurable physical characteristics of a person that can be checked on an automated basis. Biometric technology has been around for more than a decade with little fanfare. However, interest is heating up for biometric security devices in communications. Iris scanners, voice recognition modules and fingerprint readers promise to raise the bar on locking down access to computers, networks, Web sites and even cell phones [2]. Authentication by biometric verification is becoming increasingly common in industry or corporate, defense and public security systems, and consumer electronics applications. In addition to security, the driving force behind biometric verification has been convenience. Biometric identification is being used for secure self identity in areas of Theft Investigation, Criminal forensics, Personal Investigation, Forensic Science Investigation, and Digital investigation. The investigations are taking through voice verification, keystroke detection, face detection, Signature recognition and eye scanning. With assembling different detective and verification devices inside the cell phone, it has started to say biometric cell phone instead of mobile phone or cell phone [3].

Fig. 1. Biometric tool application in smart cellular phone.

As we are aware about the number of advantages of biometric technology, but common applications are:

- Biometric identification may provide unique data set, accurate, secured access to information, fingerprints, retinal and iris scans when done properly.
- Easy to verify password when individual have forgot or unable to assess the correct password.
- Automated biometric identification may be done very rapidly and uniformly, with a minimum of training.
- Individual's identity may be verified without resort to documents that may be stolen, lost or altered.

Innovators are approaching regularly for quality metrics to upgrade the advance tools and technology for biometric identification [2], [4]-[6]. In this article, we are lighting a discussion on important biometric authentications and basic mechanism involved for biometric applications in cell phone to justify for being contemporarily tool for biometrics implications.

Manuscript received April 10, 2012; revised June 15, 2012.This work was supported in part by the Uttar Pradesh Council of Science and Technology, India.

Neeraj Kumar, Raees A. Khan, and Dhirendra Pandey are with the Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, UP 226 025 INDIA (phone: +91-947-359-4960; fax: +91-522-244-1888; e-mail: neerajmtech@gmail.com, khanraees@yahoo.com, prof.dhiren@gmail.com).

DOI: 10.7763/IJIET.2012.V2.174

II. Biometric Authentication

Biometric authentication depends on requirement of investigation. There does not appear to be any one method of biometric data gathering and reading that does the 100% ensuring secure authentication [7]. Different biometric authentication methods have different identifications as per need to recommend accordingly such as some are less invasive, some can be done without the knowledge of the subject, and some are very difficult to fake [8]. The popular authentication methods may adopt in communication biometric technology.

A. Face Recognition

Of the various biometric identification methods, face recognition is one of the most flexible, working even when the subject is unaware of being scanned. It also shows promise as a way to search through masses of people who spent only seconds in front of a scanner - that is, an ordinary digital camera. Face recognition systems work by systematically analyzing specific features that are common to everyone's face - the distance between the eyes, width of the nose, position of cheekbones, jaw line, chin and so forth. These numerical quantities are then combined in a single code that uniquely identifies each person.

B. Fingerprint Recognition

Fingerprint identification involves comparing the pattern of ridges and furrows on the fingertips, as well as the minutiae points (ridge characteristics that occur when a ridge splits into two, or ends) of a specimen print with a database of prints on file [9]. Fingerprints remain constant throughout life. In over 140 years of fingerprint comparison worldwide, no two fingerprints have ever been found to be alike, not even those of identical twins. Good fingerprint scanners have been installed in Personal digital access like the iPaq, Pocket PC etc. Micro-scanners are being added in cellular phones and such smart cell phones may also be able to identify fingerprints of individuals.

C. Hand Geometry Biometrics

Hand geometry readers work in harsh environments, do not require clean conditions, and forms a very small dataset. It is not regarded as an intrusive kind of test. It is often the authentication method of choice in industrial environments and may be added inside the cellular phone successfully.

D. Retina Scan

There is no known way to replicate a retina. As far as anyone knows, the pattern of the blood vessels at the back of the eye is unique and stays the same for a lifetime. However, it requires about 15 seconds of careful concentration to take a good scan. Retina scan remains a standard in military and government installations.

E. Iris Scan

An iris scan provides unique biometric data that is very difficult to duplicate as like Retina scan and remains the same for a lifetime. Iris scan may be difficult for children or the infirm. However, there are ways of encoding the iris scan biometric data in a way that it can be carried around securely in a barcode format. Iris recognition is a biometric identification technology that uses high-resolution images of the irides of the eye. The iris of the eye is well suited for authentication purposes. Iris scans are extremely accurate.

F. Voice Recognition

The voice biometrics provides a way to authenticate identity without the subject's knowledge. It is easier to fake. It is not possible to fool an analyst by imitating another person's voice.

III. Characteristics for Biometrics

Biometric Identification requires some of the following characteristics for successful identification:

- The physical characteristic should not change over the course of the person's lifetime
- The physical characteristic must identify the individual person uniquely
- The physical characteristic needs to be easily scanned or read in the field, preferably with inexpensive equipment, with an immediate result
- The data must be easily checked against the actual person in a simple, automated way.
- Ease of use by individuals and system operators
  The enthusiastic participation of the subject is not required

IV. Basic Mechanism of Biometric Cellular Phone

To convert the biometric input, a software application is used to identify specific points of data as match points. The match points in the database are processed using an algorithm that translates that information into a numeric value. The database value is compared with the biometric input the end user has entered into the scanner and authentication is either approved or denied.

Biometric devices, such as finger scanners, consist of:

- A reader or scanning device
- Software that converts the scanned information into digital form and compares match points
- A database that stores the biometric data for comparison

V. Advancement of Biometric Technology

Some leading edge applications are:

- Fingerprint scanners including software to store and compare fingerprints, have already been installed in laptop computers and PDAs like the iPad & smart cell phones.
- Sensors installed in cell phones that can identify the environmental factors like weather conditions, rain etc.
- Special readers can measure various elements of hand geometry, comparing the result with data on file for individuals.
- Surveillance cameras can search crowds for missing persons or criminal suspects.

- Face recognition software can be modified to recognize gestures, leading to improved assistive technologies for quadriplegic patients.

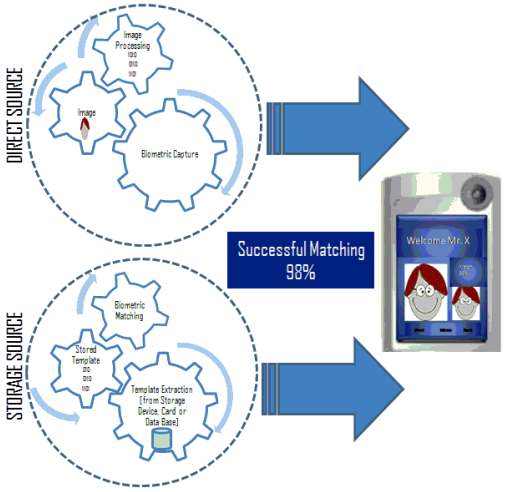

Fig. 2. Implicit image of biometric processing in smart cellular phone.

VI. Ethical Issues

A variety of ethical concerns with biometric identification methods have been registered by users. These ethical concerns are limited to biometric security. The issues for discussions are as:

- Some biometric identification methods are relatively intrusive like retina scans.
- The gathering of biometric information like fingerprints is associated with criminal behavior in the minds of many people.
- Traditionally, detailed biometric information has been gathered by large institutions, like the military or police; people may feel a loss of privacy or personal dignity.
- People feel embarrassed when rejected by a public sensor

Automated face recognition in public places could be used to track everyone's movements without their knowledge or consent.

But these ethical concerns may be limited if biometric cell phone accepted regularly at common places. These dives may contribute better to identify the individual's identity without loss of privacy and personal dignity. There may be very few chances for rejection from individual's own device. Then they may better realize that biometrics is much more convenient that PIN security and may also be assure for their unique identification and inflexible security.

VII. Conclusion

No doubt, advances in Biometric systems technology are offering a secure identity. Biometric cell phones may able to secure privacy of individuals, remote transactions, airport security, and visa identification etc. The sensors including global positioning system, vision, audio, light, temperature, direction, and acceleration are being assembled with new cell phone offerings. Secure identifications and security issues in cell phones are becoming a top priority and individuals. These features are functioning in smart phones without adding additional hard wares. Biometric Phone and security features would play a vital role to get the unique identification at National and International level. Biometric Phones may be the future technology of communication engineering.

References

[1] V. M. Mane and D. V. Jadhav, "Review of Multimodal Biometrics: Applications, challenges and Research Areas," *International Journal of Biometrics and Bioinformatics*, vol. 3, pp. 99-95, 2010.

[2] J. Bigun, "Multimodal biometric authentication using quality signals in mobile communications," in *Proc. of IAPR International Conference on Image Analysis and Processing (ICIAP)*, 2003, pp. 2-13.

[3] N. Kumar, K. Shukla, V. K. Khanna, and V. P. Sharma, "Wireless Communication-A Progressive Tool of IT With Some Challenges for Human Health and Safety," in *IEEE Explore*, 2007, pp. 125-130.

[4] J. Fierrez-Aguilar, "Kernel-based multimodal biometric verification using quality signals," in *Biometric Technology for Human Identification, Proceedings of the SPIE*, 2004, pp. 544-554.

[5] L. M. Wein and M. Baveja, "Using Fingerprint image quality to improve the identification performance of the U.S. Visitor and Immigrant Status Indicator Technology Program," in *Proc. of National Academy Science*, vol. 102, pp. 7772-7775, 2005.

[6] K. Nandakumar, Y. Chen, A. K., Jain, and S. C. Dass, "Quality-based score level fusion in multibiometric systems," in *Proc.* of *18th International Conference on Pattern Recognition*, pp. 473-476, 2006.

[7] Y. Chen, S. Dass, and A. J. Jain, "Fingerprint quality indices for predicting authentication performance," in *Proc.of Fifth International Conference AVBPA*, pp. 160-170, 2005.

[8] J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzales-Rodriguez, "Discriminative multimodal biometric authentication based on quality measures," *Pattern Recognition*, vol. 38, pp. 777-779, 2005.

[9] E. Tabassi, C. Wilson, and C. Watson, "Fingerprint image quality" 2004.

N. Kumar was born on June 10, 1982; in Unnao-INDIA. He is a young researcher and pursuing research since 2006. Recently he has earned his doctorate degree from the prestigious Babasaheb Bhimrao Ambedkar University (Central University) in Lucknow, India. As an extremely knowledgeable researcher, he is actively working in the multidisciplinary area of research particularly in Bioelectromagnetics, E-Health and Wireless Communication System. He is senior member of IACSIT.

He is working as RA-UPCST (Young Scientist Scheme) at the BBAU Lucknow. He earned more than 3 years research experiences at CSIR-Indian Institute of Toxicology Research, Lucknow. He has published more than 15 research publications and several papers were indexed by IEEE, Elsevier, Springer, LNCS, and Science Direct, Willey Blackwell etc. He is approaching to establish a correlation between the exposures of electromagnetic radiation (EMR) though wireless communicating devices or mobile phones and associated possibilities of Electromagnetic Hypersensitivity in terms of self reported symptoms and sensations in different ethnicity.

Dr Kumar is the active member of the many National and International professional bodies viz. Health Physics Society, USA, International Society for Neurochemistry, UK, Organization for Computational Neuroscience, USA, International Brain Research Organization, USA, Society of Neuroscientists of Africa, Africa, Movement Disorders Society, USA, International Association of Engineers etc.