1

Biometrics on Mobile Phone

Shuo Wang and Jing Liu
Department of Biomedical Engineering,
School of Medicine, Tsinghua University
P. R. China

1. Introduction

In an era of information technology, mobile phones are more and more widely used worldwide, not only for basic communications, but also as a tool to deal with personal affairs and process information acquired anywhere at any time. It is reported that there are more than 4 billion cell phone users over the world and this number still continues to grow as predicted that by 2015 more than 86% of the world population will own at least one cell phone (Tseng et al., 2010).

The massive volume of wireless phone communication greatly reduces the cost of cell phones despite their increasingly sophisticated capabilities. The wireless communication capability of a cell phone has been increasingly exploited for access to remote services such as e-commerce and online bank transaction. Smart phones are providing powerful functionality, working as a miniaturized desktop computer or Personal Digital Assistant (PDA). More excitingly, most of the state-of-the-art mobile phones are now being incorporated with advanced digital imaging and sensing platforms including various sensors such as GPS sensors, voice sensors (microphones), optical/electrical/magnetic sensors, temperature sensors and acceleration sensors, which could be utilized towards medical diagnostics such as heart monitoring, temperature measurement, EEG/ECG detection, hearing and vision tests to improve health care (Wang & Liu, 2009) especially in developing countries with limited medical facilities.

These scenarios, however, require extremely high security level for personal information and privacy protection through individual identification against un-authorized use in case of theft or fraudulent use in a networked society. Currently, the most adopted method is the verification of Personal Identification Number (PIN), which is problematic and might not be secured enough to meet this requirement. As is illustrated in a survey (Clarke & Furnell, 2005), many mobile phone users consider the PIN to be inconvenient as a password that is complicated enough and easily forgotten and very few users change their PIN regularly for higher security as can been seen from Fig. 1. As a result, it is preferred to apply biometrics for the security of mobile phones and improve reliability of wireless services.

As biometrics aims to recognize a person using unique features of human physiological or behavioral characteristics such as fingerprints, voice, face, iris, gait and signature, this authentication method naturally provides a very high level of security. Conventionally, biometrics works with specialized devices, for example, infrared camera for acquisition of iris images, acceleration sensors for gait acquisition and relies on large-scale computer servers to perform identification algorithms, which suffers from several problems including bulky size, operational complexity and extremely high cost.

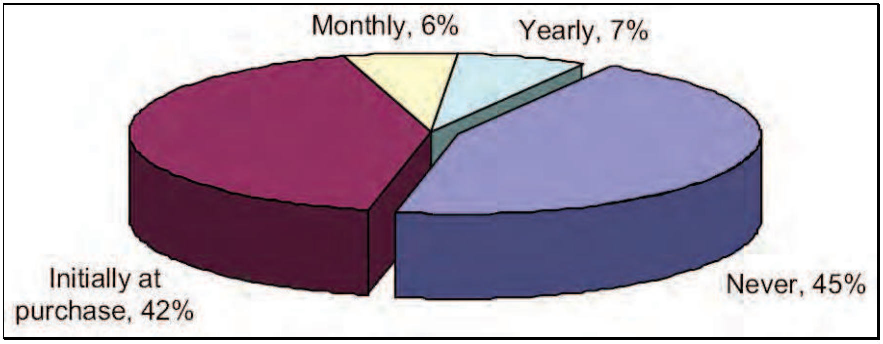


Fig. 1. Frequency of the change of PIN code. Reprinted from Computers & Security, Vol. 24, Clarke & Furnell, 2005, Authentication of Users on Mobile Telephones - A Survey of Attitudes and Practices, pp. 519-527, with permission from Elsevier

Mobile phone, with its unique features as small size, low cost, functional sensing platforms, computing power in addition to its wireless communication capability, is opening up new areas in biometrics that hold potentials for security of mobile phones, remote wireless services and also health care technology. By adding strong security to mobile phones using unique individual features, biometrics on mobile phones will facilitate trustworthy electronic methods for commerce, financial transactions and medical services. The increasing demand for pervasive biomedical measurement would further stimulate the innovations in extending the capabilities of a mobile phone as a basic tool in biometric area.
This chapter is dedicated to drafting an emerging biomedical engineering frontier--Biometrics on Mobile Phone. To push forward the investigation and application in this area, a comprehensive evaluation will be performed on the challenging fundamental as well as very practical issues raised by the biometrics on mobile phone. Particularly, mobile phone enabled pervasive measurement of several most important physiological and behavioural signals such as fingerprint, voice, iris, gait and ECG etc. will be illustrated. Some important technical issues worth of pursuing in the near future will be suggested. From the technical routes as clarified and outlined in the end of this chapter, it can be found that there is plenty of space in the coming era of mobile phone based biometric technology.

2. Feasible scenarios of biometrics on mobile phone

Incorporated with advanced sensing platforms which could detect physiological and behavioural signals of various kinds, many types of biometric methods could be implemented on cell phones. This offers a wide range of possible applications such as personal privacy protection, mobile bank transaction service security, and telemedicine monitoring. The use of sensor data collected by mobile phones for biometric identification and authentication is an emerging frontier and has been increasingly explored in the recent decade. A typical architecture of this technology can be seen in Fig. 2.

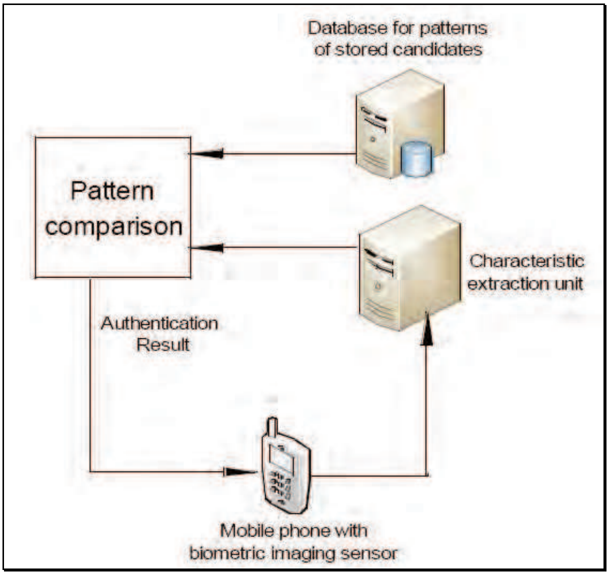

Database for patterns of stored candidates
Pattern comparison
Characteristic extraction unit
Authentication Result
Mobile phone with biometric imaging sensor

Fig. 2. Mobile biometric authentication system (Xie & Liu, 2010)

Several typical examples of recent advances which successfully implemented biometrics on mobile phones are described below.

2.1 Fingerprint identification on mobile phone

Fingerprint biometric has been adopted widely for access control in places requiring high level of security such as laboratories and military bases. By attaching a fingerprint scanner to the mobile phone, this biometric could also be utilized for phone related security in a similar manner.

A typical example can be seen from a research that utilizes a fingerprint sensor for acquisition of fingerprint images and implements an algorithm on internal hardware to perform verification of users (Chen et al., 2005). Experiment results show that this implementation has a relatively good performance. The prototype of this mobile phone based fingerprint system could be seen in Fig. 3.

Fig. 3. A schematic for fingerprint mobile phone (Redrawn from Chen et al., 2005)

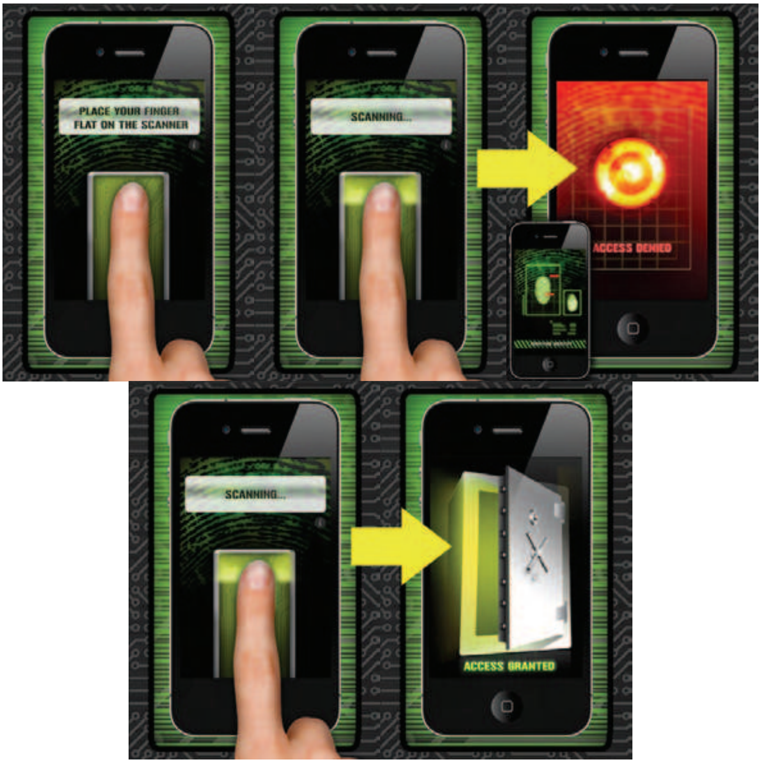


Fig. 4. Snapshots of fingerprint security - Pro (retrieved from company release news http://itunes. apple.com/us/app/fingerprint-security-pro/id312912865?mt=8)

One major inconvenience with mobile phone based fingerprint biometric is that it requires an external attachment as a scanner of fingerprint images. Recently, iPhone launched an application named Fingerprint Security by using its touch screen which does not require external scanner (shown in Fig. 4).

2.2 Speaker recognition on mobile phone

A voice signal conveys a person's physiological characteristics such as the vocal chords, glottis, and vocal tract dimensions. Automatic speaker recognition (ASR) is a biometric method that encompasses verification and identification through voice signal processing. The speech features encompass high-level and low level parts. While the high-level features are related to dialect, speaker style and emotion state that are not always adopted due to difficulty of extraction, the low-level features are related to spectrum, which are easy to be extracted and are always applied to ASR (Chen & Huang, 2009).

One major challenge of ASR is its very high computational cost. Therefore research has been focusing on decreasing the computational load of identification while attempting to keep the recognition accuracy reasonably high. In a research concentrating on optimizing vector quantization (VQ) based speaker identification, the number of test vectors are reduced by pre-quantizing the test sequence prior to matching, and the number of speakers are reduced by pruning out unlikely speakers during the identification process (Kinnunen et al., 2006). The best variants are then generalized to Gaussian Mixture Model (GMM) based modeling. The results of this method show a speed-up factor of 16:1 in the case of VQ-based modeling with minor degradation in the identification accuracy, and 34:1 in the case of GMM-based modeling.

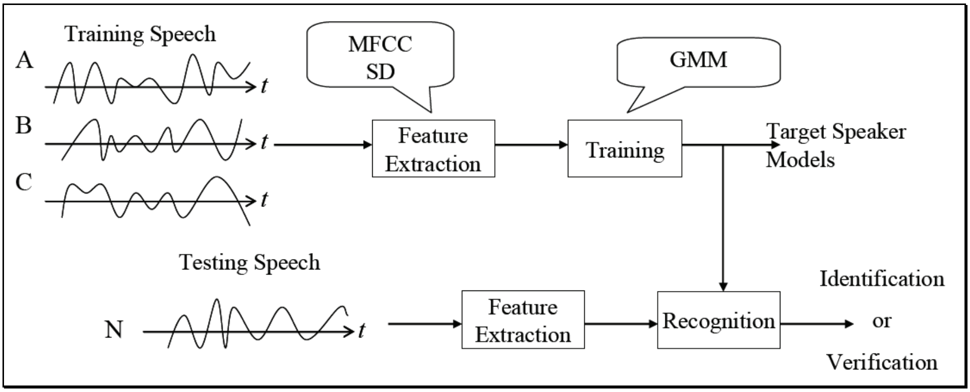


Fig. 5. Structure of a proposed ASR system. Reprinted from Proceedings of the 2009 Fourth International Multi-Conference on Computing in the Global Information Technology, Chen & Huang, 2009, Speaker Recognition using Spectral Dimension Features, pp. 132-137, with permission from IEEE

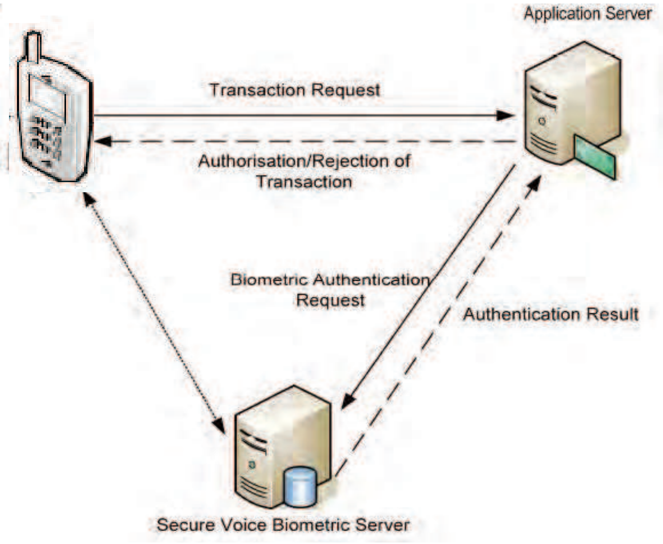

Application Server
Transaction Request
Authorisation/Rejection of Transaction
Biometric Authentication Request
Authentication Result
Secure Voice Biometric Server

Fig. 6. Voice biometric authentication for e-commerce transactions via mobile phone. Reprinted from Proceedings of 2006 2nd International Conference on Telecommunication Technology and Applications, Kounoudes et al., 2006, Voice Biometric Authentication for Enhancing Internet Service Security, pp. 1020-1025, with permission from IEEE

By far, Mel Frequency Cepstral Coefficients (MFCC) and GMM are the most prevalent techniques used to represent a voice signal for feature extraction and feature representation in state-of-the-art speaker recognition systems (Motwani et al., 2010). A recent research presents a speaker recognition that combines a non-linear feature, named spectral dimension (SD), with MFCC. In order to improve the performance of the proposed scheme as shown in Fig. 5, the Mel-scale method is adopted for allocating sub-bands and the pattern matching is trained by GMM (Chen & Huang, 2009).

Applications of this speaker verification biometric can be found in person authentication such as security access control for cell phones to eliminate cell phone fraud, an identity check during credit card payments over the Internet or for ATM manufacturers to eliminate PIN number fraud. The speaker's voice sample is identified against the existing templates in the database. If the claimed speaker is authenticated, the transaction is accepted or otherwise rejected as shown in Fig. 6 (Kounoudes et al., 2006).

Although the research of speech processing has been developed for many years, voice recognition still suffers from problems brought by many human and environmental factors, which relatively limits ASR performance. Nevertheless, ASR is still a very natural and economical method for biometric authentication, which is very promising and worth more efforts to be improved and developed.

2.3 Iris recognition system on mobile phone

With the integration of digital cameras that could acquire images at increasingly high resolution and the increase of cell phone computing power, mobile phones have evolved into networked personal image capture devices, which can perform image processing tasks on the phone itself and use the result as an additional means of user input and a source of context data (Rohs, 2005). This image acquisition and processing capability of mobile phones could be ideally utilized for mobile iris biometric.

Iris biometric identifies a person using unique iris patterns that contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles, and a zigzag collarette, some of which may be seen in Fig. 7 (Daugman, 2004). It is reported that the original iris patterns are randomly generated after almost three months of birth and are not changed all life (Daugman, 2003).

Recently, iris recognition technology has been utilized for the security of mobile phones. As a biometric of high reliability and accuracy, iris recognition provides high level of security for cellular phone based services for example bank transaction service via mobile phone.

One major challenge of the implementation of iris biometric on mobile phone is the iris image quality, since bad image quality will affect the entire iris recognition process. Previously, the high quality of iris images was achieved through special hardware design. For example, the Iris Recognition Technology for Mobile Terminals software once used existing cameras and target handheld devices with dedicated infrared cameras (Kang, 2010).

To provide more convenient mobile iris recognition, an iris recognition system in cellular phone only by using built-in mega-pixel camera and software without additional hardware component was developed (Cho et al., 2005). Considering the relatively small CPU processing power of cellular phone, in this system, a new pupil and iris localization algorithm apt for cellular phone platform was proposed based on detecting dark pupil and corneal specular reflection by changing brightness & contrast value. Results show that this algorithm can be used for real-time iris localization for iris recognition in cellular phone. In 2006, OKI Electric Industry Co., Ltd. announced its new Iris Recognition Technology for

Mobile Terminals using a standard camera that is embedded in a mobile phone based on the original algorithm OKI developed, a snapshot of which can be seen in Fig. 8.

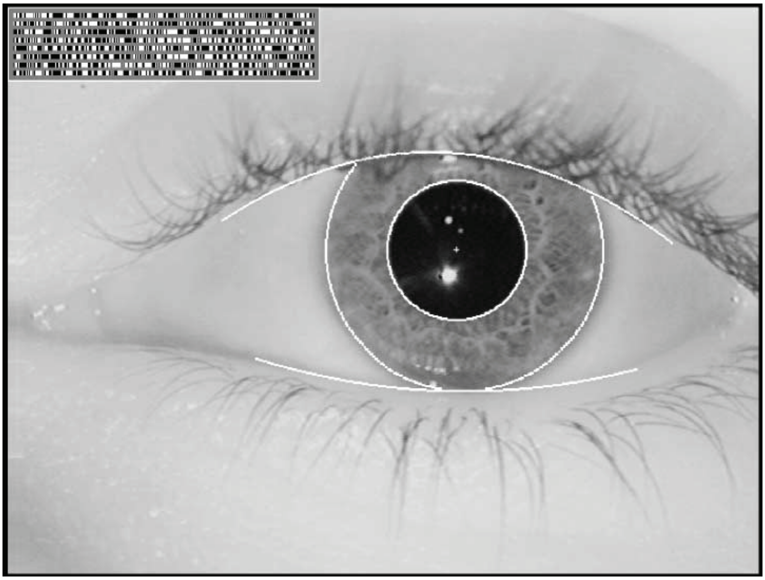


Fig. 7. Example of an iris pattern image showing results of the iris and pupil localization and eyelid detection steps. Reprinted from Pattern Recognition, Vol. 36, Daugman, 2003, The Importance of Being Random: Statistical Principles of Iris Recognition, pp. 279-291, with permission from Elsevier

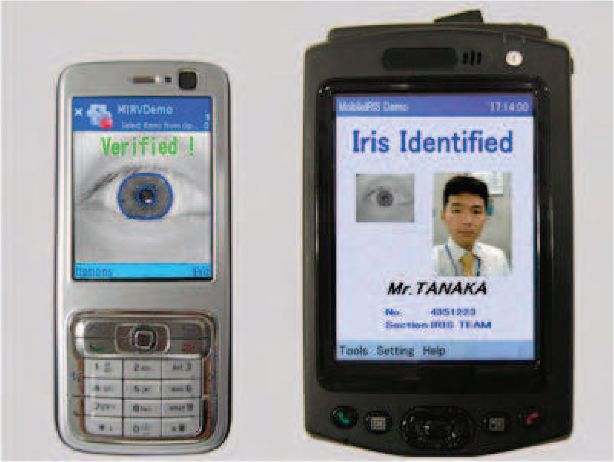


Fig. 8. Iris recognition technology for mobile terminals (OKI introduces Japan's first iris recognition for camera-equipped mobile phones and PDAs, In: *OKI Press Releases*, 27.11.2006, Available from http://www.oki.com/en/press/2006/z06114e.html)

Since iris image quality is less controllable with images taken by common users than those taken in the laboratory environment, the iris image pre-processing step is also very important for mobile applications. In recent research, a new pupil & iris segmentation method was proposed for iris localization in iris images taken by cell phone (Cho et al., 2006; Kang, 2010), the architecture and service scenarios of which is shown in Fig. 9. This method finds the pupil and iris at the same time, using both information of the pupil and iris together with characteristic of the eye image. It is shown by experimental results that this method has good performance in various images, even when they include motion or optical blurring, ghost, specular refection, etc.

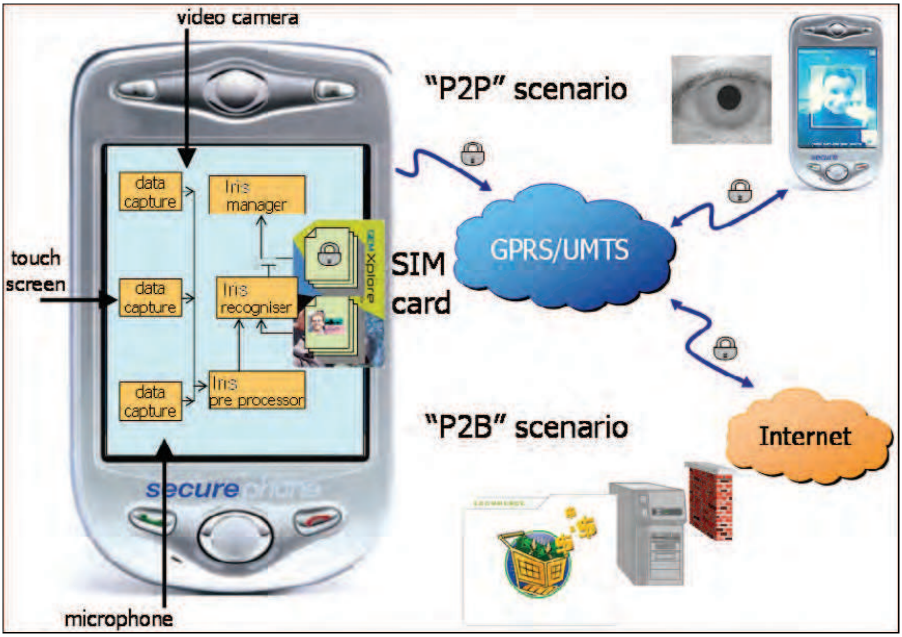


Fig. 9. Architecture and service models of mobile iris system. Reprinted from Procedia Computer Science, Vol. 1, Kang, 2010, Mobile Iris Recognition Systems: An Emerging Biometric Technology, pp. 475-484, with permission from Elsevier

2.4 Unobtrusive user-authentication by mobile phone based gait biometrics

Mobile phones nowadays contain increasing amount of valuable personal information such as wallet and e-commerce applications. Therefore, the risk associated with losing mobile phones is also increasing. The conventional method to protect user sensitive data in mobile phones is by using PIN codes, which is usually not secured enough. Thus, there is a need for improving the security level in protection of data in mobile phones.

Gait, i.e., walking manner, is a distinctive characteristic for individuals (Woodward et al., 2003). Gait recognition has been studied as a behavioral biometric for more than a decade, utilized either in an identification setting or in an authentication setting. Currently 3 major approaches have been developed for gait recognition referred to as the Machine Vision (MV) based gait recognition, in which case the walking behavior is captured on video and video processing techniques are used for analysis, the Floor Sensor (FS) based gait recognition by placing sensors in the floor that can measure force and using this information for analysis and Wearable Sensor (WS) based gait recognition, in which scenario the user wears a device that measures the way of walking and recognize the pattern recognition for recognition purposes (Bours & Shrestha, 2010). Smart phone, such as an iPhone, is now incorporated with accelerometers working along three primary axes (as shown in Fig. 10), which could be utilized for gait recognition to identify the user of a mobile phone (Tanviruzzaman et al., 2009).

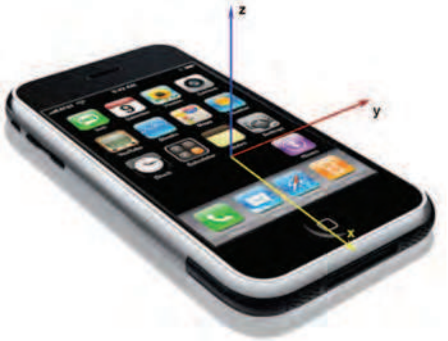


Fig. 10. Three axes of accelerometers on an iPhone (Redrawn from Tanviruzzaman et al., 2009)

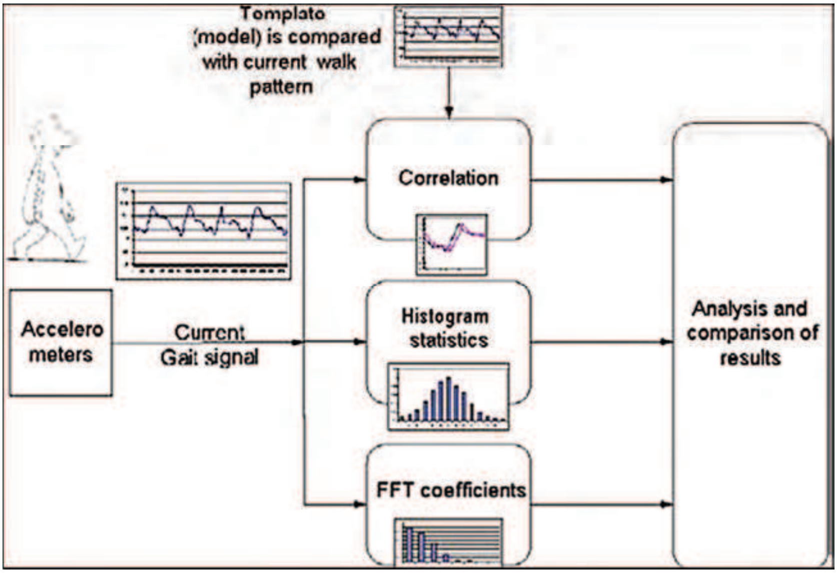

Templato (model) is compared with current walk pattern
Correlation
Accelero meters
Current Gait signal
Histogram statistics
Analysis and comparison of results
FFT coefficients

Fig. 11. Block diagram of a gait based identification method. Reprinted from Proceedings of 2005 30th IEEE International Conference on Acoustics, Speech and Signal Processing, Mäntyjärvi et al., 2005, Identifying Users of Portable Devices from Gait Pattern with Accelerometers, pp. 973-976, with permission from IEEE

Mobile phone based biometrics uses the acceleration signal characteristics produced by walking for verifying the identity of the users of a mobile phone while they walk with it. This identification method is by nature unobtrusive, privacy preserving and controlled by the user, who would not at all be disturbed or burdened while using this technology. The principle of identifying users of mobile phones from gait pattern with accelerometers is presented in Fig. 11. In this scenario, the three-dimensional movement produced by walking is recorded with the accelerometers within a mobile phone worn by the user. The collected data is then processed using correlation, frequency domain methods and data distribution statistics. Experiments show that all these methods provide good results (Mäntyjärvi et al., 2005).

The challenges of the method come from effect of changes in shoes, ground and the speed of walking. Drunkenness and injuries also affect performance of gait recognition. The effect of positioning the mobile phone holding the accelerometers in different places and positions also remains to be studied in future.

2.5 ECG biometrics for mobile phone based telecardiology

Cardiovascular disease (CVD) is the number one killer in many nations of the world. Therefore, prevention and treatment of cardiovascular disorders remains its significance in global health issues.

With the development of telemedicine, mobile phone based telecardiology has been technologically available for real-time patient monitoring (Louis et al., 2003; Sufi et al., 2006; Lee et al., 2007; Lazarus, 2007; Chaudhry et at., 2007; Plesnik et al., 2010), which is becoming increasingly popular among CVD patients and cardiologists. In a telecardiology application, the patient's Electrocardiographic (ECG) signal is collected from the patient's body which can be immediately transmitted to the mobile phone (shown in Fig. 12) using wireless communication and then sent through mobile networks to the monitoring station for the medical server to perform detection of abnormality present within the ECG signal. If serious abnormality is detected, the medical server informs the emergency department for rescuing the patient. Prior to accessing heart monitoring facilities, the patient first needs to log into the system to initiate the dedicated services. This authentication process is necessary in order to protect the patient's private health information. However, the conventional user name and password based patient authentication mechanism (as shown in Fig. 13) might not be ideal for patients experiencing a heart attack, which might prevent them from typing their user name and password correctly (Blount et al., 2007). More efficient and secured authentication mechanisms are highly desired to assure higher survival rate of CVD patients.

Recent research proposed an automated patient authentication system using ECG biometric in remote telecardiology via mobile phone (Sufi & Khalil, 2008). The ECG biometrics, basically achieved by comparing the enrollment ECG feature template with an existing patient ECG feature template database, was made possible just ten years ago (Biel et al., 2001) and has been investigated and developed by a number of researchers (Shen et al., 2002; Israel et al., 2005; Plataniotis et al., 2006; Yao & Wan, 2008; Chan et al., 2008; Fatemian & Hatzinakos, 2009; Nasri et al., 2009; Singh and Gupta, 2009; Ghofrani & Bostani, 2010; Sufi et al., 2010b). The common features extracted from ECG signals contain three major feature waves (P wave, T wave and QRS complex) as shown in Fig. 14. The use of this sophisticated ECG based biometric mechanism for patient identification will create a seamless patient authentication mechanism in wireless telecardiology applications.

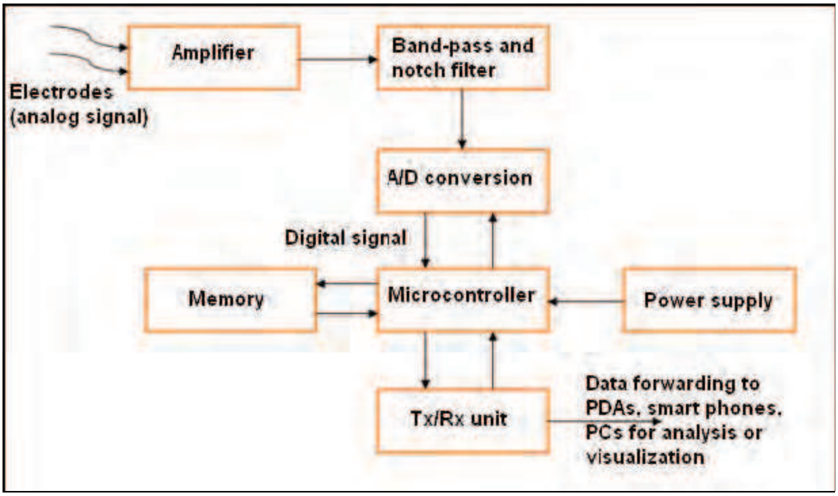
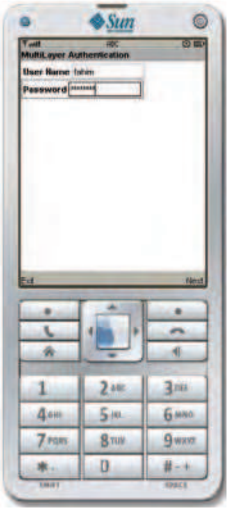

Amplifier
Band-pass and notch filter
Electrodes (analog signal)
A/D conversion
Digital signal
Memory
Microcontroller
Power supply
Tx/Rx unit
Data forwarding to PDAs, smart phones, PCs for analysis or visualization

Fig. 12. Architecture of an ECG acquisition and remote monitoring system. Reprinted from Proceedings of 2010 15th IEEE Mediterranean Electrotechnical Conference, Plesnik et al., 2010, ECG Signal Acquisition and Analysis for Telemonitoring, pp. 1350-1355, with permission from IEEE


MultiLayer Authentication

User Name fahim

Password ********

Fig. 13. Username and password based authentication mechanism for mobile phone dependent remote telecardiology. Reprinted from Proceedings of 2008 International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Sufi & Khalil, 2008, An Automated Patient Authentication System for Remote Telecardiology, pp. 279-284, with permission from IEEE

In the proposed system, the patient's ECG signal is acquired by a portable heart monitoring device, which is capable of transmitting ECG signals via Bluetooth to the patient's mobile phone. The mobile phone directly transmits the compressed and encrypted ECG signal to the medical server using GPRS, HTTP, 3G, MMS or even SMS. Upon receiving the compressed ECG, the original ECG of the patient is retrieved on the medical server through decompression and decryption. Then the medical server performs extraction of ECG feature template and matches the template against the ECG biometric database. The patient identification is achieved after the closest match is determined.

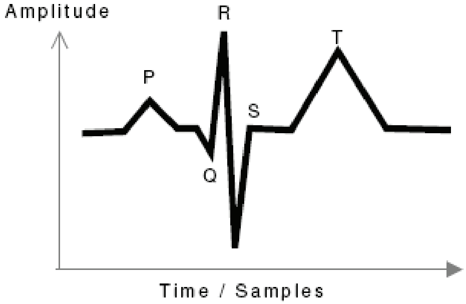


Fig. 14. Typical ECG feature waves (Sufi et al., 2010a)

In a later research (Sufi and Khalil, 2011), a novel polynomial based ECG biometric authentication system (as shown in Fig. 15) was proposed to perform faster biometric matching directly from compressed ECG, which requires less storage for storing ECG feature template. The system also lowered computational requirement to perform one-to-many matching of biometric entity.

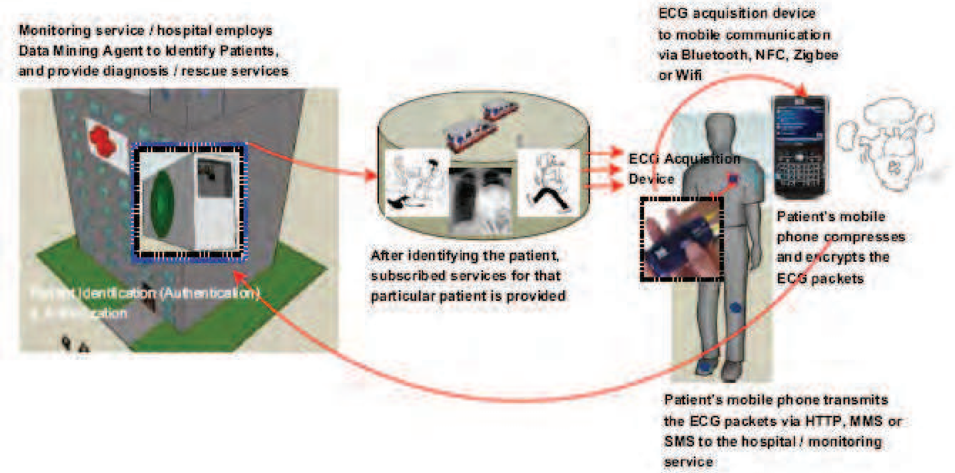

Monitoring service / hospital employs Data Mining Agent to Identify Patients, and provide diagnosis / rescue services
ECG acquisition device to mobile communication via Bluetooth, NFC, Zigbee or Wifi
ECG Acquisition Device
Patient's mobile phone compresses and encrypts the ECG packets
After identifying the patient, subscribed services for that particular patient is provided
Identification (Authentication)
Patient's mobile phone transmits the ECG packets via HTTP, MMS or SMS to the hospital / monitoring service

Fig. 15. Architecture of patient identification from compressed ECG based on data mining. Reprinted from Journal of Network and Computer Applications, Vol. 34, Sufi & Khalil, 2011, Faster Person Identification Using Compressed ECG in Time Critical Wireless Telecardiology Applications, pp. 282–293, with permission from Elsevier

With this new ECG biometric authentication mechanism in place, the CVD patients log into the medical server and then have access to the monitoring facility without human intervention and associated delays, making the telecardiology application faster than existing authentication approaches, which eventually leads to faster patient care for saving life.

Challenges for this ECG based biometric system involve the security of transmitting ECG from the patient to the medical server for privacy protection and the pertinence of ectopic beats, the presence of which either with the enrolment ECG or the recognition ECG could result in possible false non-match for a patient.

2.6 Summary and discussion on different systems

There are many more types of biometrics that could be implemented on mobile phones in addition to the above systems introduced in this section. Generally, several key factors should be considered when implementing such biometrics within a mobile phone. These factors will include user preference, accuracy and the intrusiveness of the application process. Table 1 illustrates how these factors vary for different types of biometrics.

Biometric technique	User preference from survey	Sample acquisition capability as standard?	Accuracy	Non-intrusive?
Ear shape recognition	NA	×	High	✓
Facial recognition	Medium	✓	High	✓
Fingerprint recognition	High	×	Very high	×
Hand geometry	Medium	×	Very high	×
Handwriting recognition	NA	✓	Medium	✓
Iris scanning	Medium	×	Very high	×
Keystroke analysis	Low	✓	Medium	✓
Service utilization	NA	✓	Low	✓
Voiceprint verification	High	✓	High	✓

Table 1. Comparison of different biometric techniques for mobile phone. Reprinted from Computers & Security, Vol. 24, Clarke & Furnell, Authentication of Users on Mobile Telephones - A Survey of Attitudes and Practices, pp. 519-527, 2005 with permission from Elsevier

The user preference is investigated in a survey (Clarke et al., 2003). The assigned accuracy category is based upon reports by the International Biometric Group (IBG, 2005) and National Physical Laboratory (Mansfield et al., 2001). The judgement of intrusiveness is performed according to whether or not the biometrics could be applied transparently.

It could be seen that apparent disparity exists between high authentication security and transparent authentication process. Biometric approaches that have the highest accuracy are also the more intrusive techniques. When implementing biometrics on mobile phones, a compromise between security and the convenience to the user is required.

3. Open issues with biometrics on mobile phone

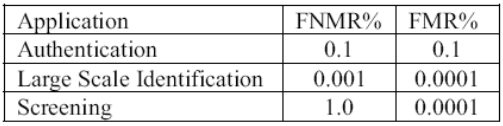
Biometrics on mobile phone, as an emerging frontier, is very promising while still holding many technical problems to be well addressed in order to be widely and ideally adopted. Issues worth pursuing in future research not only involve biometrics and mobile phones alone, but also come with the applications and styles of implementation i.e. scenarios in which specific biometrics are used.

3.1 Issues with biometrics

The most critical issue with biometrics that needs continuous effort to work on is to recognize biometric patterns with higher accuracy. A biometric system does not always make absolutely right decisions, it can make two basic types of errors, the false match and false non-match. Error rates of typical biometrics are shown in Table 2. Correspondingly, Table 3 lists requirements on typical accuracy performance. It is apparent that there is still a large gap between the currently available technology and requirements of performance.

Biometric	FTE %	FNMR %	FMR1 %	FMR2 %	FMR3 %
Face	n/a	*4*	*10*	*40*	12
Finger	*4*	*2*	*2*	*0.001*	<1
Hand	2	1.5	1.5	n/a	n/a
Iris	7	6	<0.001	n/a	n/a
Voice	1	*15*	*3*	n/a	n/a

Table 2. Typical biometric accuracy performance numbers reported in large third party tests. FTE refers to failure to enroll, FNMR is non-match error rate, FMR1 denotes verification match error rate, FMR2 and FMR3 denote (projected) large-scale identification and screening match error rates for database sizes of 1 million and 500 identities, respectively. Reprinted from IEEE publication title: Proceedings of 2004 17th International Conference on Pattern Recognition, Jain et al., 2004, Biometrics: A Grand Challenge, pp. 935-942, with permission from IEEE



Application	FNMR%	FMR%
Authentication	0.1	0.1
Large Scale Identification	0.001	0.0001
Screening	1.0	0.0001

Table 3. Typical intrinsic matcher (1:1) performance requirements. Reprinted from Proceedings of 2004 17th International Conference on Pattern Recognition, Jain et al., 2004, Biometrics: A Grand Challenge, pp. 935-942, with permission from IEEE

Other problems that need to be further studied include assurance of infeasibility of fraudulence and exploration of new features with existing biometrics and novel types of biometrics. Moreover, as computing power of current mobile phones is still very limited, processing methods of biometric patterns need to be adapted for lower burden on computation.

3.2 Challenges to mobile phone

In order to ensure the accuracy and efficiency of biometrics recognition on mobile phones, computing power and storage capacity of mobile phones are still needed to be significantly enhanced. Currently, the implementation of biometrics on mobile phones usually requires the simplification of algorithm used in conventional biometrics in order to be adapted for the relatively small CPU processing power of a cellular phone. This adaption will inevitably reduce the accuracy and security level, which highly limits the performance of mobile phone enabled biometric techniques.

In addition, the essential hardware i.e. biometric sensors embedded on mobile phones are also required to provide better performance, e.g. higher resolution of image acquired with digital cameras on mobile phones, at lower cost while maintaining their miniaturization feature.

3.3 Optimal implementation of biometrics on mobile phone

Reasonable implementation of biometrics on mobile phone is important for wide adoption of this technology as the application of mobile phone based biometrics must work in a non-intrusive manner for the convenience of users. Examples of feasible scenarios are described as keystroke analysis while texting messages, handwriting recognition while using transcriber function and speaker recognition whilst using microphones (Clarke & Furnell, 2005). Another problem needs to be addressed is the compatibility with multiple platforms of mobile phones during the development of algorithms and software.

3.4 Outlook of future development in mobile phone based biometrics

Numerous types of biometrics hold the potentials of being implemented on mobile phones. According to the different types of signals needed to be collected for feature extraction, applicable biometric methods can be classified into the imaging type, mechanical type and electrical type.

The imaging type includes, but is not limited to the recognition of face, teeth and palm print in addition to fingerprint and iris, utilizing images captured by the camera embedded in the mobile phone. The mechanical type involves voice, heart sound using microphones and blood pressure by specific and miniaturized sensors attached to the mobile phone. Not only ECG can be used in mobile biometrics, the electroencephalography (EEG) identification (Paranjape et al., 2001; Nakanishi et al., 2009; Bao et al., 2009) also has applicability in this new area.

The mobile phone based biometrics is also developing towards a multimodal functionality, which combines several biometric recognition methods to provide more reliable and flexible identification and authentication.

Promising applications include personal privacy security, e-commerce, mobile bank transactions, e-health technology, etc. A grand outlook of future development in mobile phone based biometrics is outlined in the diagram below (Fig. 16).

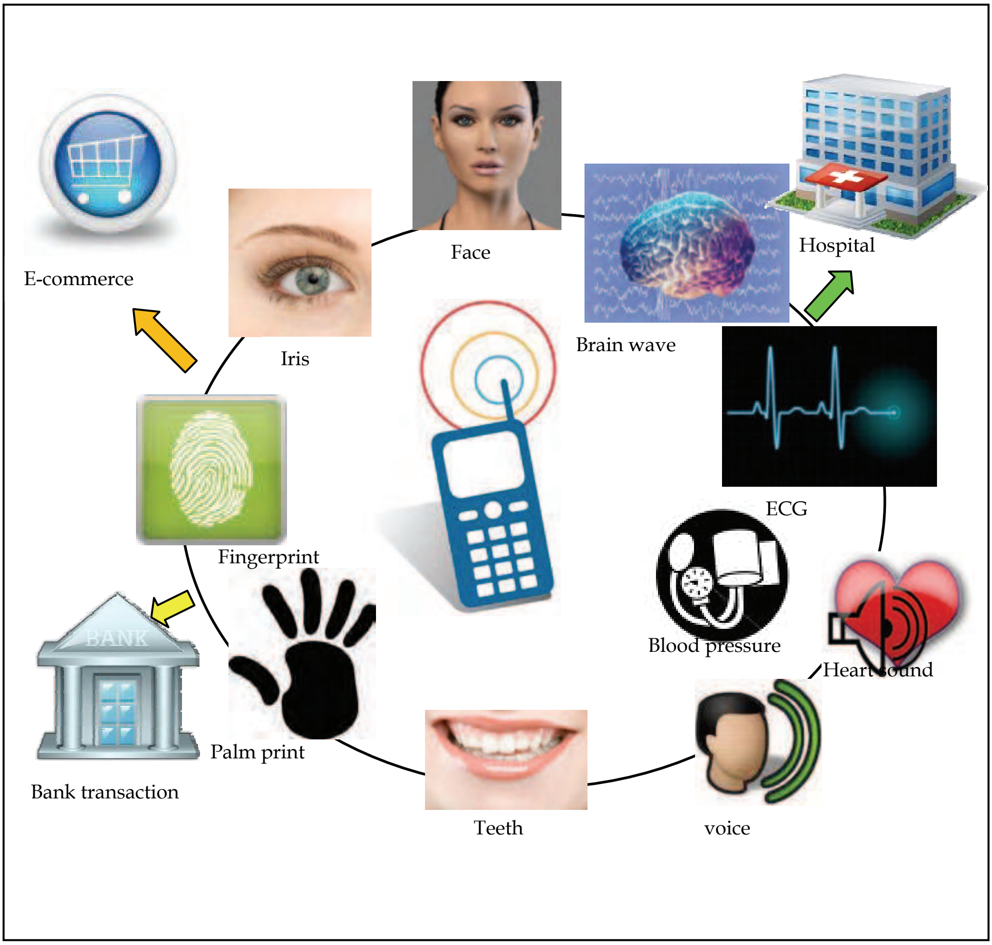


Fig. 16. An outline of future development in biometrics on mobile phone

4. Conclusion

In this chapter, we study how the mobile phone can be used in biometrics. This versatile technique has so far proven to be a unique and promising participant in the areas of biometrics. Not only can mobile phone deliver successful solutions in the traditional biometric arenas of human identification and authentication, it has also been instrumental in securing the resource-constrained body sensor networks for health care applications in an efficient and practical manner. At the same time, there remain many challenges to be addressed and a lot more new technologies to be explored and developed. Before successful consumer-ready products are available, a great deal of research and development is still needed to improve all aspects of the mobile phone based biometric system. With a modicum of expectation, it is hoped that this chapter will play a part in further stimulating the research momentum on the mobile phone based biometrics.

5. Acknowledgement

This work was partially supported by the National "863" Program of China, the Tsinghua-Yue-Yuen Medical Sciences Fund and the Funding of the National Lab for Information Science and Technology at Tsinghua University.

6. References

Bao, X.; Wang, J. & Hu, J. (2009). Method of Individual Identification based on Electroencephalogram Analysis. *Proceedings of 2009 International Conference on New Trends in Information and Service Science*, pp. 390-393, ISBN 978-0-7695-3687-3, Beijing, P.R.China, June 9-July 2, 2009

Biel, L.; Pettersson, O.; Philipson, L. & Wide, P. (2001). ECG Analysis: A New Approach in Human Identification. *IEEE Transactions on Instrumentation and Measurement*, Vol. 50, No. 3, (June 2001), pp. 808-812, ISSN 0018–9456

Blount, M.; Batra, V.; Capella, A.; Ebling M.; Jerome, W.; Martin, S.; Nidd, M.; Niemi, M. & Wright, S. (2007). Remote Health-Care Monitoring Using Personal Care Connet. *IBM Systems Journal*, Vol. 46, No. 1, (Jan 2007), pp. 95-113, ISSN 0018-8670

Bours, P. & Shrestha, R. (2010). Eigensteps: A giant Leap for Gait Recognition. *Proceedings of 2010 2nd International Workshop on Security and Communication Networks*, pp. 1-6, ISBN 978-1-4244-6938-3, Karlstad, Värmland, Sweden, May 26-28, 2010

Chan, A.; Hamdy, M.; Badre, A. & Badee V. (2008). Wavelet Distance Measure for Person Identification Using Electrocardiograms. *IEEE Transactions on Instrumentation and measurement*, Vol. 57, No. 2, (February 2008), pp. 248-253, ISSN 0018–9456

Chaudhry, S.; Phillips, C.; Stewart, S.; Riegel, B.; Mattera, J.; Jerant, A. & Krumholz, H. (2007). Telemonitoring for Patients With Chronic Heart Failure: A Systematic Review. *Journal of Cardiac Failure*, Vol. 13 No. 1, (February 2007), pp. 56-62, ISSN 1071-9164

Chen, W. & Huang, J. (2009). Speaker Recognition using Spectral Dimension Features. *Proceedings of 2009 4th International Multi-Conference on Computing in the Global Information Technology*, pp. 132-137, ISBN 978-0-7695-3751-1, Cannes, La Bocca, France, August 23-29, 2009

Chen, X.; Tian, J.; Su, Q.; Yang, X. & Wang, F. (2005). A Secured Mobile Phone Based on Embedded Fingerprint Recognition Systems. In: *Intelligence and Security Informatics*, Kantor, P. et al., (Eds.), pp. 549-553, Springer Berlin / Heidelberg, Retrieved from http://dx.doi.org/10.1007/11427995_57

Cho, D.; Park, D. & Rhee, D. (2005). Real-time Iris Localization for Iris Recognition in Cellular Phone. *Proceedings of 2005 6th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and 1st ACIS International Workshop on Self-Assembling Wireless Networks*, pp. 254-259, ISBN 0-7695-2294-7, Towson, Maryland, USA, May 23-25, 2005

Cho, D.; Park, K.; Rhee, D.; Kim, Y. & Yang, J. (2006). Pupil and Iris Localization for Iris Recognition in Mobile Phones. *Proceedings of 2006 7th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, pp. 197-201, ISBN 0-7695-2611-X, Las Vegas, Nevada, USA, June 19-20, 2006

Clarke, N. & Furnell, S. (2005). Authentication of Users on Mobile Telephones - A Survey of Attitudes and Practices. *Computers & Security*, Vol. 24, No. 7, (October 2005), pp. 519-527, ISSN 0167-4048

Daugman, J. (2003). The Importance of Being Random: Statistical Principles of Iris Recognition. *Pattern Recognition*, Vol. 36, No. 2, (February 2003), pp. 279-291, ISSN 0031-3203

Daugman, J. (2004). How Iris Recognition Works. *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, No. 1, (January 2004), pp. 21-30, ISSN 1051-8215

Fatemian, S. & Hatzinakos, D. (2009). A New ECG Feature Extractor for Biometric Recognition. *Proceedings of 2009 16th International Conference on Digital Signal Processing*, pp. 1-6, ISBN 978-1-4244-3298-1, Santorini-Hellas, Fira, Greece, July 5-7, 2009

Ghofrani, N. & Bostani, R. (2010). Reliable Features for an ECG-based Biometric System. *Proceedings of 2010 17th Iranian Conference of Biomedical Engineering*, pp. 1-5, ISBN 978-1-4244-7484-4, Isfahan, Isfahan, Iran, November 3-4, 2010

Israela,S.; Irvine, J.; Cheng, A.; Wiederhold, M.& Wiederhold, B. (2005). ECG to Identify Individuals. *Pattern Recognition*, Vol. 38, No. 1, (January 2005), pp. 133 – 142, ISSN 0031-3203

Jain, A.; Pankanti, S.; Prabhakar, S.; Hong, L. & Ross, A. (2004). Biometrics: A Grand Challenge. *Proceedings of 2004 17th International Conference on Pattern Recognition*, pp. 935-942, ISBN 0-7695-2128-2, East Lansing, Michigan, USA, August 23-26, 2004

Kang, J. (2010). Mobile Iris Recognition Systems: An Emerging Biometric Technology. *Procedia Computer Science*, Vol. 1, No. 1, (May 2010), pp. 475-484, ISSN 1877-0509

Kinnunen, T.; Karpov, E. & Fränti, P. (2006). Real-Time Speaker Identification and Verification. *IEEE Transactions on Audio, Speech, and Language Processing*, Vol. 14, No. 1, (January 2006), pp. 277-288, ISSN 1558-7916

Kounoudes, A.; Kekatos, V. & Mavromoustakos, S. (2006). Voice Biometric Authentication for Enhancing Internet Service Security. *Proceedings of 2006 2nd International Conference on Telecommunication Technology and Applications*, pp. 1020-1025, ISBN 0-7803-9521-2, Damascus, Syria, April 24-28, 2006

Lazarus, A. (2007). Remote, Wireless, Ambulatory Monitoring of Implantable Pacemakers, Cardioverter Defibrillators, and Cardiac Resynchronization Therapy Systems: Analysis of a Worldwide Database. *Pacing and Clinical Electrophysiology*, Vol. 30, No. S1, (January 2007), pp. S2-S12, ISSN 1450-8159

Lee, R.; Chen, K.; Hsiao, C. & Tseng, C. (2007). A Mobile Care System With Alert Mechanism. *IEEE Transactions on Information Technology in Biomedicine*, Vol. 11, No. 5, (September 2007), pp. 507-517, ISSN 1089-7771

Louis, A.; Turner, T.; Gretton, M.; Baksh, A. & Cleland, J. (2003). A Systematic Review of Telemonitoring for the Management of Heart Failure. *The European Journal of Heart Failure*, Vol.5 , No. 5, (October 2003), pp. 583–590, ISSN 1388-9842

Mäntyjärvi, J.; Lindholm, M.; Vildjiounaite, E.; Mäkelä, S. & Ailisto, H. (2005). Identifying Users of Portable Devices from Gait Pattern with Accelerometers. *Proceedings of 2005 30th IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 973-976, ISBN 0-7803-8874-7, Philadelphia, Pennsylvania, USA, March 18-23, 2005

Motwani, R.; Dascalu, S. & Harris, F. (2010). Voice Biometric Watermarking of 3D Models. *Proceedings of 2010 2nd International Conference on Computer Engineering and Technology*, pp. 632-636, ISBN 978-1-4244-6347-3, Chengdu, Sichuan, P.R.China, April 16-18, 2010

Nakanishi, I.; Baba, S. & Miyamoto, C. (2009). EEG Based Biometric Authentication Using New Spectral Features. *Proceedings of 2009 International Symposium on Intelligent Signal Processing and Communication Systems*, pp. 651-654, ISBN 978-1-4244-5015-2, Kanazawa, Ishikawa, Japan, December 7-9, 2009

Nasri, B.; Guennoun, M. & El-Khatib, K. (2009). Using ECG as a Measure in Biometric Identification Systems. *Proceedings of 2009 IEEE Toronto International Conference - Science and Technology for Humanity*, pp. 28-33, ISBN 978-1-4244-3878-5, Toronto, Ontario, Canada, September 26-27, 2009

OKI Introduces Japan's First Iris Recognition for Camera-equipped Mobile Phones and PDAs, In: *OKI Press Releases*, 27.11.2006, Available from http://www.oki.com/en/press/2006/z06114e.html

Paranjape, R.; Mahovsky, J.; Benedicenti, L. & Koles, Z. (2001). The Electroencephalogram as a Biometric. *Proceedings of 2001 Canadian Conference on Electrical and Computer Engineering*, pp. 1363-1366, ISBN 0-7803-6715-4, Toronto, Ontario, Canada, May 13-16, 2001

Plataniotis, K.; Hatzinakos, D. & Lee, L. (2006). ECG Biometric Recognition Without Fiducial Detection. *Proceedings of 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference*, pp. 1-6, ISBN 978-1-4244-0487-2, Baltimore, Maryland, USA, September 19-21, 2006

Plesnik, E.; Malgina, E.; Tasič, J. & Zajc, M. (2010). ECG Signal Acquisition and Analysis for Telemonitoring. *Proceedings of 2010 15th IEEE Mediterranean Electrotechnical Conference*, pp. 1350-1355, ISBN 978-1-4244-5793-9, Valletta, Malta, April 26-28, 2010

Rohs, M. (2005). Real-World Interaction with Camera Phones, In: *Ubiquitous Computing Systems*, Murakami, H.; Nakashima, H.; Tokuda, H. & Yasumura, M., (Eds.), pp. 74-89, Springer Berlin / Heidelberg, Retrieved from http://dx.doi.org/10.1007/11526858_7

Shen, T.; Tompkinsl, W. & Hu, Y. (2002). One-Lead ECG for Identity Verification. *Proceedings of 2002 2nd Joint Conference of the IEEE Engineering in Medicine and Biology Society and the Biomedical Engineering Society*, pp. 62-63, ISBN 0-7803-7612-9, Houston, Texas, USA, October 23-26, 2002

Singh, Y. & Gupta, P. (2009). Biometrics Method for Human Identification Using Electrocardiogram. In: *Advance in Biometrics*, Tistarelli, M. & Nixon, M., (Eds.), pp. 1270-1279, Springer Berlin / Heidelberg, Retrieved from http://dx.doi.org/10.1007/978-3-642-01793-3_128

Sufi, F.; Fang, Q; Mahmoud, S. & Cosic, I. (2006). A Mobile Phone Based Intelligent Telemonitoring Platform. *Proceedings of the 3rd IEEE-EMBS International Summer School and Symposium on Medical Devices and Biosensors*, pp. 101-104, ISBN 0-7803-9787-8, Boston, USA, September 4-6, 2006

Sufi, F. & Khalil, I. (2008). An Automated Patient Authentication System for Remote Telecardiology. *Proceedings of 2008 International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pp. 279-284, ISBN 978-1-4244-2957-8, Sydney, Australia, December 15-18, 2008

Sufi, F.; Khalil, I. & Tari, Z. (2010a). A Cardiod based Technique to Identify Cardiovascular Diseases using Mobile Phones and Body Sensors. *Proceedings of 2010 32nd Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5500-5503, ISBN 978-1-4244-4123-5, Buenos Aires, Argentina, August 31 - September 4, 2010

Sufi1, F.; Khalil, I. & Habib, I. (2010b). Polynomial Distance Measurement for ECG Based Biometric Authentication. *Security and Communication Networks*, Vol. 3, No. 4, (August 2010), pp. 303 – 319, ISSN 1939-0114

Sufi, F. & Khalil, I. (2011). Faster Person Identification Using Compressed ECG in Time Critical Wireless Telecardiology Applications. *Journal of Network and Computer Applications*, Vol. 34, No. 1, (January 2011), pp. 282–293, ISSN 1084-8045

Tanviruzzaman, M.; Ahamed, S.; Hasan, C. & O'brien, C. (2009). ePet: When Cellular Phone Learns to Recognize Its Owner. *Proceedings of the 2009 2nd ACM Workshop on Assurable and Usable Security Configuration*, pp. 13-17, ISBN 978-1-60558-778-3, Chicago, Illinois, USA, November 9, 2009

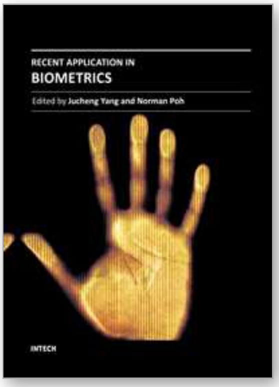
Tseng, D.; Mudanyali, O.; Oztoprak, C.; Isikman, S.; Sencan, I.; Yaglidere, O. & Ozcan, A. (2010), Lensfree Microscopy on a Cellphone. *Lab on a Chip*, Vol. 10, No. 14, (July 2010), pp. 1782-1792, ISSN 1473-0197

Wang, H. & Liu, J. (2009). Mobile Phone Based Health Care Technology. *Recent Patents on Biomedical Engineering*, Vol. 2, No. 1, (January 2009), pp. 15-21, ISSN 1874-7647

Woodward, J. & Orlans, N. (2003). Esoteric Biometrics, In: *Biometrics: Identity Assurance in the Information Age*, Gatune, J., (Ed.), pp. 115-136, McGraw-Hill Professional Publishing, ISBN 0-07-222227-1, Berkeley, California, USA

Xie, Q. & Liu, J. (2010). Mobile Phone Based Biomedical Imaging Technology: A Newly Emerging Area. *Recent Patents on Biomedical Engineering*, Vol. 3, No. 1, (January 2010), pp. 41-53, ISSN 1874-7647

Yao, J. & Wan, Y. (2008). A Wavelet Method for Biometric Identification Using Wearable ECG Sensors. *Proceedings of the 2008 5th International Workshop on Wearable and Implantable Body Sensor Networks, in conjunction with The 5th International Summer School and Symposium on Medical Devices and Biosensors*, pp. 297-300, ISBN 978-1-4244-2253-1, Hong Kong, P.R.China, June 1-3, 2008



Recent Application in Biometrics
Edited by Dr. Jucheng Yang

ISBN 978-953-307-488-7
Hard cover, 302 pages
Publisher InTech
Published online 27, July, 2011
Published in print edition July, 2011

In the recent years, a number of recognition and authentication systems based on biometric measurements have been proposed. Algorithms and sensors have been developed to acquire and process many different biometric traits. Moreover, the biometric technology is being used in novel ways, with potential commercial and practical implications to our daily activities. The key objective of the book is to provide a collection of comprehensive references on some recent theoretical development as well as novel applications in biometrics. The topics covered in this book reflect well both aspects of development. They include biometric sample quality, privacy preserving and cancellable biometrics, contactless biometrics, novel and unconventional biometrics, and the technical challenges in implementing the technology in portable devices. The book consists of 15 chapters. It is divided into four sections, namely, biometric applications on mobile platforms, cancelable biometrics, biometric encryption, and other applications. The book was reviewed by editors Dr. Jucheng Yang and Dr. Norman Poh. We deeply appreciate the efforts of our guest editors: Dr. Girija Chetty, Dr. Loris Nanni, Dr. Jianjiang Feng, Dr. Dongsun Park and Dr. Sook Yoon, as well as a number of anonymous reviewers.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821