Biometrics for Mobile Devices: A Comparison of Performance and Pattern Classification Approaches

M.Krishnasamy and N.L.Clarke

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

Mobile devices have become indispensable tools nowadays. With growing technologies, applications and services are being added to the mobile devices all the time. Its usage in business and enterprises need it to be secure from unauthorised access. The extent of protection currently available is not adequate for the services that are employed in mobile devices. Biometrics have the privilege of providing secure authentication through utilising the unique characters of a person. Reports on the theft and loss of information and the wide acceptance on biometric authentication paved the way in its research on mobile devices. Several performance issues are to be considered when implementing biometrics in mobile devices

This paper focuses on the comparison of different pattern classification approaches employed in Face, Fingerprint, Keystroke and Signature biometric techniques and their effect on the performance on these devices. A detailed study on different algorithms employed in each technique has been performed. Most of the algorithms that are used for authentication follows similar approach regardless of the techniques and are broadly categorised between statistical and neural network approaches. Processing time in each approach is spent for feature extraction and classification and the storage for holding these features. Neural network techniques performs authentication with higher accuracy but require huge memory capacity and longer training time which makes it infeasible to be employed in mobile devices. Statistical approaches although consumes less processing time than neural networks, still requires considerable processing time to perform authentication in real time.

Biometrics is a future technology which can provide secure authentication. Biometrics in mobile devices will become practical if the developments in technology in mobile architectures and software are implemented fully on these devices.

Keywords

Mobile Devices, Neural Network, Biometrics, Statistical, Pattern Classification

1. Introduction

Mobile device technology is one of the rapidly growing technologies in the past few years with some 1.5 billion devices currently in use all over the world which is more than three times the number of Personal Computers (PC) (Prensky, 2004).This exponential growth is due to its widespread emergence and rapid adoption of handheld computing devices. Mobile devices have become an inherent part of the business environment with its usage on online banking, share dealing, micropayment

and m-commerce. M-commerce which has predicted revenue of $554.37 by 2008 (Telecom Trend International, 2004) is a major application that has been facilitated by the features on mobile devices. It also has the promising future in business to consumer market. As more and more services are added to the mobile devices with the substantial increase in the number of devices, security risks on those device has become more apparent. So the success of m-commerce and services depends on how security is implemented on these devices.

Security in mobile devices is provided using Personal Identification Numbers (PIN), a widely used method for authenticating users. Some of the drawbacks on using this method are that they can be forgotten by the user, can be easily guessed, stolen or cracked. PINs are also weaker in providing strong authentication that is needed for the services and applications available in current 3G phones. There are several incidents published on the loss of information or theft from PDAs, phones and converged devices (CSO Online, 2004). It was reported that in 2002, a mobile phone was stolen every three minutes on average in the UK which made the UK government to ask the mobile manufacturers to improve the security of the mobile devices that will make them difficult to use after stolen (Techplus, 2002).

In addition to that, a survey on mobile phone subscribers showed that about 45% of the mobile phone users responded that PIN is an inconvenient method of authentication and 81% of users were interested in improving security in the mobile devices and also want an authentication method which is different from the traditional way of using PINs (Clarke *et al*, 2003A). Smart cards are another alternative to PINs which is based on what the user has, but it can also be lost or stolen. From the aforementioned survey, with 81% of respondents believing on higher security, authentication using biometrics is one of the solutions to it.

2. Biometrics and Mobile Devices

Biometrics is the process of identifying an individual using his/her physiological or behavioural characteristics which are unique to that individual. It is an excellent candidate for identity verification which uniquely differentiates a user by authenticating him with the characteristic possessed by him. Physiological techniques measure the physiological characteristics of an individual, such as fingerprint which are unalterable and remain relatively stable over time. Behavioural techniques such as signature and keystroke measure the behavioural characteristics of a person. Behavioural characteristics however tend to vary to a greater degree over time due to a variety of reasons.

Performance of biometric devices is governed by the False Rejection Rate (FRR), the rate at which an authorised user (genuine user) is rejected from the system and the False Acceptance Rate (FAR), the rate at which an unauthorised user (impostors) are authenticated to the system. Equal Error Rate (EER) is used to compare between the FAR and FRR which determines the accuracy of the system with lower the EER the more accurate the system.

2.1 Biometric System

A biometric system is a device which uses a single or multiple biometric techniques to identify an individual and provide access to the system. Centralised and distributed are two types of architectural design used in biometric systems. In centralised system the feature values extracted from the raw data are sent to the common system which will perform the comparison with the stored features and produce the output whereas in distributed systems extracted features are compared locally on the device and the result is produced. Even though centralised systems has the advantage of being supervised and maintained easily they consume higher communication bandwidth and also has a greater risk of a system-wide failure when compared with the distributed systems (Kung *et al*, 2005).

2.2 Biometrics in Mobile Devices

Mobile devices can be used both in centralised and distributed systems. Studies on mobile devices in centralised systems have been carried out by (Massachusetts Institute of Technology, 2004; Tsai *et al*, 2003; Weinstein *et al*, 2002; Hazen *et al*, 2003; Clarke *et al*, 2003B; Clarke *et al*, 2004), where the data was collected and sent though the network for verification, authentication is performed if it matches with the stored features on the database. Implementing authentication as a distributed system in a mobile device is not popular and requires considerable development in technology on the mobile devices to be adapted widely. This paper focuses on evaluating the processing and storage requirements needed to implement a distributed mobile device biometric authentication. Personalisation is one of the features that can facilitate distributed biometric authentication in mobile devices because it allows the user templates to be stored on to the local device.

The performance of biometric authentication on a mobile device will depend on the pattern recognition and classification algorithms used for enrolment and verification of the extracted data. Algorithms which require more complex functions for execution will consume more processing time, more power and storage which are the critical components in a mobile device, so the success of biometric authentication will depend on the algorithms employed. Statistical and neural network approaches are widely used pattern recognition methods in biometrics.

3. Mobile Specific Biometric Approaches

Several biometric techniques are available which can be used to recognise a user. The following techniques are chosen for its employability in mobile devices. Different algorithms used in each technique are discussed in relation to their performances.

3.1 Fingerprint Recognition

In fingerprint recognition, authentication can be performed using a sensor device which senses the fingerprint of a user to provide authentication. Some of the main

characteristics of a fingerprint image are area, resolution, number of pixels, geometric accuracy, contrast and geometric distortion. Minutiae based method, k-Nearest Neighbour (k-NN), SVM and Backpropagation neural network algorithms are compared and the results were concluded based on the studies of (Yao *et al*, 2001) in Table 1.

Algorithm	Minutiae	k-NN	SVM	Neural Network
Accuracy (%)	95	87.9	88	86
Advantages	Reduce minutiae's will reduce processing time	Simple Algorithm Less processing	Requires less training Accuracy is high	Efficient output once trained
Disadvantages	Accuracy reduced with few minutiae's	Execution time increases with k	Requires considerable development	Requires more time for training

Table 1: Performance Comparison of Fingerprint Recognition Algorithms

3.2 Face Recognition

Face recognition is the process of identifying an individual from the images of their faces using the extracted features which are stored in the database. In mobile devices, face authentication can be performed by capturing the image using the built in camera. The presence of input devices like this facilitate easier authentication. Eigenface method, Elastic Graph Matching (EGM), Support Vector Machines (SVM) and Backpropagation Neural Network are the extraction and classification algorithms that are compared on face recognition and the results were concluded based on the studies of (Ho-Man, 2003; Jun Zhang *et al*, 1997) in the Table 2 (calculated using a 1400 MHz desktop PC)

Algorithm	Eigenface	EGM	SVM	Neural Network
Storage (ORL) (MB)	5	1.5	38	32 KB
Accuracy (%)	80.3	81.5	95.5	91.5
Avg. Running Time (Seconds)	2.1	16.3	6	1.4
Advantages	Provides lossless data Less execution time	Higher accuracy in less lighting conditions, face positions and expressions Uses only key point of the image	Higher accuracy in less lighting conditions	Faster authentication time More accurate
Disadvantages	Lower accuracy in varying light intensities, scale and orientations	Longer computational time	Longer time to train	Longer training time More data for trained Affected by lighting small variations

Table 2 Performance Comparison of Face Recognition Algorithms

3.3 Keystroke Recognition

Keystroke dynamics is the behavioural way of authenticating a user by analysing the way a user types on the keyboard input and identifying a rhythm pattern which can vary with time. It is considered to be a most attractive biometric authentication scheme for its transparency to the user. There is no requirement of additional tool or hardware need to implement authentication where the keypad itself acts as a tool to authenticate the user. k-NN and Neural networks are algorithms that are compared and the results were concluded based on the studies of (Wagacha, 2003; Cho *et al*, 2000; Clarke *et al*, 2003B) in the Table 3.

Algorithm	k-NN	Neural Network
Accuracy (%) – EER	14.2	11.3
Advantages	Easy to program without the need for optimisation or training Accuracy can increased by increasing k	Highly accurate (low EER)
Disadvantages	Execution time is more when k is high and more data is applied	More sample data to get trained Retraining when new user added

Table 3: Performance Comparison of Keystroke Recognition Algorithms

3.4 Signature Recognition

In Signature authentication the dynamic characteristics like speed, acceleration, direction, pressure, etc are compared. In a mobile device, on-line signature recognition can be implemented by writing using a pressure sensitive pen on the touch screen of the mobile device. Similar to keystroke, signature authentication does not require any additional hardware; instead the stylus of the mobile device can be used. Hidden Markov Model (HMM) and Dynamic Time Warping (DTW) algorithms that are compared (Griess, 2000).

Algorithm	HMM	Neural Network	DTW
Accuracy (%) - EER	1 - 4	4	2 - 3
Advantages	Can model wide range of variation Increase in state increases accuracy	Higher Accuracy	Finds the exact points during matching
Disadvantages	Longer training time when the states increased	Requires more time to be trained	More computation Suffer from warping forgeries

Table 4: Performance Comparison of Signature Recognition Algorithms

4. Discussion

In biometrics, the authentication time is the time required for the system to process the request made by the user to authenticate into the system which depends on the algorithm used. For a more accurate output the algorithm employed will perform more calculations which in turn consumes more time and for a less accurate output the algorithm consumes lesser time for authentication so there needs to be a trade-off between the accuracy and execution time.

Biometrics application on mobile devices is currently on development with number of studies being performed on it. This paper analysed the four different biometric techniques and their algorithms used to perform authentication. From the study it is revealed that each different technique has some features that facilitate to be implemented in mobile devices.

Face recognition in mobile devices are performed by (Massachusetts Institute of Technology, 2004; Tsai *et al*, 2003; Weinstein *et al*, 2002; Hazen *et al*, 2003) used dedicated servers which consumed more time in transmitting the data over the network and this can be improved by performing the processing in mobile device itself. SVM and EBGM approaches have the advantage of performing face detection even in less lighting conditions which will make them suitable to be used in mobile devices, where the authentication needs to be performed with variable background environment which depends on the user location.

Experiments performed by (Clarke *et al*, 2003B; Clarke *et al*, 2004) used mobile keypads interfaced with a desktop PC to provide the necessary processing and suggested that the neural network patterns performed well in producing keystroke recognition. Although neural networks performed authentication in higher accuracy, it requires more training time, so k-NN can only be possible in mobile devices.

Fingerprint biometrics for mobile devices needs a dedicated hardware such as sensors to be fabricated to the mobile device hardware. Dedicated processors or chips are being developed to perform fingerprint recognition in mobile devices. Minutiae method can be a possible solution in mobile devices where a reduced minutiae has the capability to perform accurate and faster authentication

Signature recognition has the capability to be used in mobile devices such as smart phones and PDAs which has a touch screen and digital pen that allows the user to sign on the device to perform authentication. HMM method has the advantage of modelling wide range of variation with increased accuracy and less execution time.

Algorithms are available in each technique with low computation time and higher accuracy that can be used for authentication. But practical implementation requires issues such as mobile device architecture needs to be considered for authentication in real time. As computation of the algorithm becomes more complex there will be more processing done by the registers and other processing components in the mobile device and this will also have a significant influence on the battery life time if those algorithms had to run many times.

Neural networks had more success in producing accurate output with less FAR and FFR in most biometric techniques and it also produced a quicker authentication when trained. But training requires a large number of features with huge storage. Accuracy can be increased with multiple layers which increases processing time for training as the complexity of the algorithm is increased. Since current mobile devices come with a moderate storage capacity, storing will not become a big issue but the processing time in neural networks make it impossible to be used in mobile devices. Mobile devices are personal devices so it is wasteful to store the features of other users or impostors to make the comparison, so neural network techniques are not recommended for biometric authentication in mobile devices.

Most of the pattern recognition algorithms require floating point operations for their complex mathematical functions but the current mobile devices include processors which are unable to perform floating point calculations. They perform floating point operations by converting them to fixed point numbers which results in longer processing and execution time. One of the method to reduce processing and execution time is by choosing an algorithm which requires less arithmetic and floating point operations like k-NN algorithms where there is no arithmetic operations involved instead the result can be obtained using the shift and logical operations. Other method can be employing code optimisation, in this approach codes are written by making changes in the algorithms implementation that can utilise the processor efficiently in order to save energy and reduce execution time when applying the complex algorithms. Dynamic voltage scaling is another approach that can change the processing frequency and voltage at run-time to reduce the energy consumption.

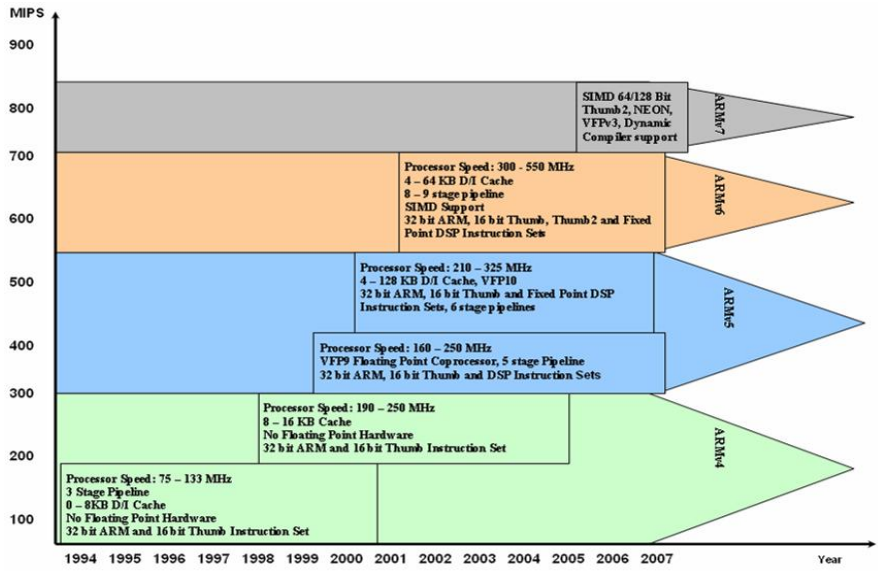

Figure 1: Trends in Mobile Technology

The technology trend in mobile architecture of ARM (ARM, 2005) is given in Figure 1. The figure show that although there is a gradual increase in processor speed over the years, a considerable change in instruction set has been taken place such as an addition of DSP and Thumb instructions which improved the programme flow and its efficient code size improved the power and performance of the mobile devices. NEON technologies on ARMv7 will be implemented in future mobile devices which can provide an extensive set of new instructions to provide an accelerated output when compared to all the other previous technologies (3x performance when compared with ARMv5 and 2x performance of ARMv6 on DSP applications). Floating point coprocessors are being added along with increasing MIPS. The addition of SIMD instructions can also increase the performance of software applications and increasing pipeline stages are being taking place which can facilitate parallel processing. These new technologies will allow biometrics authentication to succeed in mobile devices.

Multi-model biometrics can also be another solution to reduce the processing time where multiple less accurate, low processing algorithms from different techniques can be implemented, providing an accurate and reliable authentication with less EER so that the combined computational time is less than the computational time for executing a more accurate algorithm. This can be facilitated by inbuilt facilities like camera, sound input, touch screen and keypad in the mobile devices.

5. Conclusion and Future Work

Secure mobile communication enables users to use application such as mobile payment and finance, mobile ticketing, mobile voting and location based services with increased convenience and confidence. In providing security the current form of authentication is a cheap solution but it suffers from a number of security weaknesses and biometrics is a strongest approach when compared to all other forms of authentication.

Even though biometrics seems to be a perfect solution, issues of performance and its ability to provide authentication in real time has to be considered before implementing them in the mobile devices. Applications that perform biometric authentication will become feasible if those devices are equipped with large memory storage and high speed processor that has low power consumption. The memory storage is being increasing to facilitate more services but the issue of processing and power requirement affected by the complexity of the algorithms still remains an issue on mobile devices.

Neural network approach requires larger processing time and memory during its training phase which makes them infeasible to be employed in mobile devices. While in statistical approaches, algorithms with less mathematical operations or using architectural and algorithmic optimisation on the codes has been suggested to improve the processing time.

As this study analysed various algorithms and their performance in terms of the processing, it provided an efficient starting point for further research on its deployment in mobile devices. In future, the study on the instruction sets and architecture of the processor employed in the devices will allow writing software codes with code optimisation that can evaluate the processing time and storage requirements for each algorithm practically and determine its efficiency.

Mobile device are personalised devices and authentication can be preformed using one to one verification, but the success of this approach will depend on the accuracy of the algorithms which is used to perform authentication. Technological trends discussed showed that there are improvements being taking place that can facilitate biometric authentication using statistical approaches and also the usage of neural networks can become viable on the development of cell processor technology that facilitates parallel processing. So biometrics in mobile devices will become a practical reality within a few years.

6. References

ARM (2005), "Processor Core Families", http://www.arm.com/products/CPUs/families.html, (Accessed 1 September 2005)

Cho, S., Han, C., Han, D.H. and Kim, H. (2000), "Web-Based Keystroke Dynamics Identity Verification Using Neural Network", *Journal of Organisational Computing and Electronic Commerce*, 10(4), pp295-307.

Clarke, N.L., Furnell, S.M., Lines, B.M. and Reynolds, P.L. (2003A), Keystroke dynamics on a mobile handset: A feasibility study, *Information Management & Computer Security*, Vol. 11, No. 4, pp161-166.

Clarke, N.L., Furnell, S.M., Lines, B.M. and Reynolds, P.L. (2003B), Using Keystroke analysis as a mechanism for Subscriber Authentication on Mobile Handsets, *Proceedings of the IFIP SEC 2003 Conference*, May, Athens, Greece, pp 97-108.

Clarke, N.L., Furnell, S.M., Lines, B.M. and Reynolds, P.L. (2004), Application of Keystroke Analysis to Mobile Text Messaging, *Proceedings of the 3rd Security Conference*, 14-15 April, Las Vegas, USA.

CSO Online (2004), "Managing and Securing Mobile Devices", http://www.csoonline.com/analyst/report2794.html, (Accessed 1 September 2005)

Griess, F.D. (2000), "On-line Signature Verification", http://www.cse.msu.edu/cgi-user/web/tech/document?ID=449, (Accessed 12 September 2005)

Hazen, T.J., Weinstein, E., Kabir, R. and Park A. (2003), "Multi-Modal Face and Speaker Identification on a Handheld Device", *Proceedings of the Workshop on Multimodal User Authentication*, December, Santa Barbara, California.

Ho-Man, T. (2003), *Face Recognition Committee Machine: Methodology, Experiments and A System Application*, MPhil Thesis, The Chinese University of Hong Kong.

Jun Zhang, Yong Yan and Lades, M. (1997), "Face Recognition: Eigenface, Elastic Matching, and Neural Nets", *Proceedings of the IEE*, 85(9), pp 1423-1425.

Kung, S.Y., Mak, M.W. and Lin, S.H. (2005), *Biometric Authentication: A Machine Learning Approach*, Prentice Hall PTR, ISBN: 0-13-147824-9

Massachusetts Institute of Technology (2004), "MIT Project Oxygen", http://oxygen.lcs.mit.edu/H21.html, (Accessed 1 September 2005)

Prensky, M. (2004), "What can you learn from a cell phone? – almost anything!", http://www.marcprensky.com/writing/Prensky-What_Can_You_Learn_From_a_Cell_Phone-FINAL.pdf, (Accessed 1 September 2005)

Techplus (2002), "Why the interest in mobile phone security?", http://www.tekplus.com/TP0039A02V01.html, (Accessed 1 September 2005).

Telecom Trend International (2004), "Mobile Commerce Takes-off", http://telecomtrends.net/pr_MIIS-1.htm (Accessed 1 September 2005).

Tsai, Y., Fu, R., Huang, L., Huang, C. and Liu, C. (2003), "Handheld Person Verification System Using Face Information", In *7th International Conference on Digital Image Computing: Techniques and Applications*, 10-12 December, Sydney, Australia.

Wagacha, P.W. (2003), "Instance-Based Learning: *k*-Nearest Neighbour", http://www.uonbi.ac.ke/acad_depts/ics/course_material/machine_learning/kNN.pdf, (Accessed 1 September 2005)

Weinstein, E., Ho, P., Heisele, B., Poggio, T., Steele, K. and Agarwal, A., (2002), "Handheld Face Identification Technology in a Pervasive Computing Environment", http://cbcl.mit.edu/projects/cbcl/publications/ps/pervasive-2002.pdf, (Accessed 1 September 2005)

Yao, Y., Frasconi, P. and Pontil, M. (2001), "Fingerprint Classification with Combinations of Support Vector Machines", *Proceeding of the 3rd International Conference on Audio and Video based Biometric Person Authentication*, 6-8 June, Sweden, pp 253-258.