Near Field Communication in Smart Sensing Applications

Charl A. Opperman[1] and Gerhard P. Hancke[2]
Department of Electrical, Electronic and Computer Engineering
University of Pretoria[1], Private Bag X20, Hatfield, Pretoria 0028
Tel: +27 12 420 3738
and ISG Smart Card Centre, Royal Holloway
University of London[2]
email: charlopperman1988@gmail.com[1]; ghancke@ieee.org[2]

Abstract-High-end smartphones have recently started to feature NFC capability. Since these smartphones are capable of performing an array of sensing tasks, in addition to having powerful processing and memory specifications, the possibility exists to use them as a platform for smart sensing. NFC communication can aid in making sensing applications more user-friendly by allowing quick data transfers between peer devices. In addition, NFC can be used to store data on RFID tags or to communicate with low power external sensors that may feature a passive NFC interface. In this way, low power or passive sensors can effectively outsource their processing and long-range communication needs to a smartphone. This paper discusses the implementation of a biometric verification system on an Android smartphone as a proof-of-concept.

Index Terms—NFC, biometrics, smart sensing, mobile computing, smartphones, Android

I. INTRODUCTION

After the invention of RFID technology, sensing applications utilising RFID soon followed. Sensors were provided with the ability to communicate wirelessly, with very low to zero effect on power consumption [1]. However, when the data generated by these sensors needed to be processed, a computer was required, which meant that a link was necessary between a computer and the sensor. Traditionally, a specialised RFID reader would be used to gather data from the sensor, after which the reader would be physically or wirelessly connected to a PC in reasonably close proximity [2]. Another approach would be to fit the sensor with a processor or microcontroller, to enable local processing of data, but this meant that the sensor would consume much more power. These approaches are becoming increasingly outdated and a quicker, more mobile approach is required in many applications.

Near Field Communication or NFC, a successor to RFID, was standardised by the NFC Forum, which was founded in 2004 [3]. The main NFC standard is defined in ISO 18092 or the equivalent ECMA-340 standard and is compatible with RFID tags that comply with the ISO 14443 standard. NFC devices are also specifically compatible with the well-known RFID tag brands MIFARE and FeliCa, by Philips and Sony, respectively [4].

NFC provides the following advantages over legacy RFID:

- NFC provides a new peer-to-peer transmission function in addition to the standard RFID tag reading and writing functions. This means that NFC "reader/writer" devices can also communicate with each other [5].
- NFC can be used to initialise faster connections such as Bluetooth and Wi-Fi seamlessly. This is known as "Connection Handover" [6].
- NFC is incorporated into mobile phones, which are ubiquitous. This means simple, low-power RFID sensors can connect to mobile phones to gain internet access indirectly via GPRS or HSPA. These low-power sensors can also take advantage of the processing power of NFC-enabled smartphones [7].
- NFC reader/writer devices can also emulate RFID tags. This function is used for electronic keys and ticketing, as well as mobile payments. Data is stored on a secure element on the phone [5], [8].

NFC has recently moved into the smartphone arena, where it is envisioned to have a plethora of applications, among which are the following:

- Mobile payments or m-payments. Google Wallet is the first major deployment of m-payments using NFC based payment systems with wide retail functionality [9].
- Electronic ticketing [5].
- Location-based services [10].
- Smart posters and large displays. Posters with embedded RFID tags can be touched with phones to get additional information on certain subjects [11]. Large displays can also be touched with the phone if a large screen is required temporarily to display content that cannot be viewed on the phone itself [12].
- Sensing and digital control applications [7], [13].
- Shopping (as a replacement for barcodes) [5].
- Health and medical applications.
- General data transfer.
- Identification. Electronic passports or e-passports and electronic ID documents or eIDs are already being issued in many countries [14], [15]. In South Africa, a pilot project will commence in late 2012 to systematically replace ordinary ID documents with smart-IDs [16].

This paper focuses on the applicability of NFC in various sensing scenarios. Having NFC present in high-end smartphones provides two possibilities for smart sensing. Firstly, the original RFID sensing scenario, mentioned previously, is still valid but additionally smartphones have 3rd generation HSPA connectivity for faster transmission of large amounts of data to a computer. Alternatively, transmission of data for processing may not be necessary at all, because smartphones themselves are quite powerful. And secondly, smartphones themselves are fitted with a wide range of sensors, which means the phone can be used alone for sensing applications. In this scenario, NFC is simply an enabling technology in the sense that NFC can be very user-friendly, but NFC can also help to give context to the sensing application by providing location information (possibly combined with GPS). An example of such a context function for NFC would be when NFC was used for ticketing and the phone then expects certain types of noise in sensor readings that will be performed on a train or bus. This could help in interpreting sensing data more accurately.

Low-power, cheap sensors can have access to a very powerful processor as well as fast internet access, using the smartphones. The exact application scenario will always determine whether or not a standalone sensor will be required or whether a smartphone alone is sufficient. Some applications may also still require a back-end PC if a large display is required, for example (or the large display function of NFC could be used). A smartphone with NFC would still be advantageous in all these scenarios, and the advantage of its utilisation is that these phones do not need to be bought specifically for these applications, because they are utilised for many other applications.

II. RESEARCH CONTRIBUTION AND SIMILAR WORK

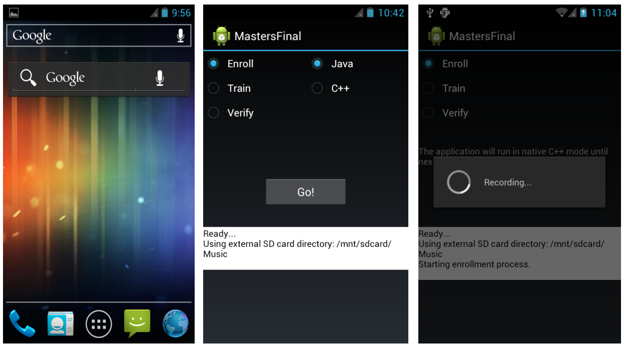
A mobile biometrics application can benefit from using NFC for the passing of data in the form of biometric templates or identification information, such as business, cards between phones at close physical proximity. It is proposed as the enabling communications technology mainly because it is considered the most human-centric or user-friendly wireless technology and the quickest for the passing of small amounts of data at close range [17], [18]. NFC can also be used to store biometric templates on RFID tags.

In other research papers, NFC has been utilised, together with identification information stored electronically in a secure element on a mobile phone, to replace paper-based ID documents. This method enhances the privacy of persons by allowing only certain identification information to be requested and transmitted electronically, instead of having to present an ID document with exhaustive information about a person that may be irrelevant to certain circumstances [17]. The feasibility of mobile biometrics on phones and PDAs in terms of processing time has been studied in detail, especially for multimodal biometrics (combinations of different biometric methods), which provides a solution to the somewhat low quality of biometric measurements made by mobile devices [19], [20], [21]. The study of biometric methods on mobile devices has also lead to novel unimodal approaches for gesture and gait recognition using acceleration sensors present in mobile phones [22], [23], [24].

The contribution of this paper is to analyse the usability of a peer-to-peer biometric verification system, in conjunction with NFC, and to measure the processing differences between native and non-native code on smartphones. The most applicable mobile biometric techniques for the mobile arena are image based methods, such as face recognition and hand geometry recognition, as well as speaker or voice recognition, by using the built-in camera and microphone respectively. Gait and hand gesture recognition can also be implemented accurately using the accelerometer and gyroscopic sensors.

III. SYSTEM IMPLEMENTATION

A biometric verification system was implemented on a Google Nexus S smartphone. Open-source libraries for feature extraction and classification were ported to the Android platform. For comparative purposes, the system was also identically implemented on a desktop PC. Speaker recognition was implemented in Java and a simple face recognition application was implemented in native C++ code. This was done to analyse the difference in performance between native and non-native code on the Android platform. The Google Nexus S runs Android 4, has a 1 GHz processor and 512 MB of RAM. The phone also possesses two 5 megapixel cameras, a microphone with software noise cancellation, a three-axis gyroscope and an accelerometer [25]. The PC applications were implemented on a desktop computer with a quad core (4 x 2.66 GHz) processor and 3 GB of RAM.



Ready...
Using external SD card directory: /mnt/sdcard/Music

The application will run in native C++ mode until nex

Ready...
Using external SD card directory: /mnt/sdcard/Music
Starting enrollment process.

Fig. 1. Screenshots of Android 4 and the biometric verification App that was designed for this research project. These screenshots were taken on a Google Nexus S smartphone

Porting of Java libraries to Android is relatively simple because the Dalvik virtual machine that Android uses is mostly compatible with the standard JVM. Android does not provide implementations of the AWT and Swing graphics libraries and code involving these GUI libraries must be removed in the porting process. Incompatibilities were also encountered in audio I/O functions, which is to be expected. The porting process of C++ libraries is much more involved. Android provides an open-source implementation of the standard C library known as bionic, together with various C++ libraries. The included C and C++ libraries provide much more limited functionality than on a desktop PC. For the porting process Android provides a method to create a standalone GCC/G++ toolchain, which can then be used to cross-compile open-source code using a standard UNIX/Linux build system such as CMAKE. If source code is not shipped with a build system, the Android GCC or G++ compiler may simply be invoked directly or an Android makefile may be used. Many standard C and C++ libraries are not provided with Android and code that use these libraries need to be modified or removed in the porting process. Some deficiencies that were encountered include limitations in the "Portable Thread" library (pthread) and some functions in the "stdlib" header, among others. In many cases, open source software is dependent on other open source libraries. In these cases the required libraries need to be ported as well.

A. Non-native code (Java libraries)

For the implementation of speaker recognition in Java, the MARF (Modular Audio Recognition Framework) library was initially used. The MARF library is specifically aimed at speaker and voice recognition and includes preprocessing, feature extraction and basic classification algorithms. A basic speaker recognition system was implemented using MARF. Fig. 2 shows the results of the preprocessing and feature extraction stages when training a classifier in MARF with a single audio sample.

For later implementations, specialised feature extraction libraries such as jAudio was used with the general machine learning and data mining library WEKA, which provides general classifiers such as Naive Bayes, neural networks and supports vector machines. For face recognition in Java, some options include FAINT, which provides a pure Java implementation of the PCA (principal component analysis) algorithm, and a Java interface to OpenCV. Specialised feature extraction and image processing libraries can also be utilised directly with WEKA.

B. Native code (C/C++ libraries)

For an initial face recognition implementation in C++ native code, OpenCV (the open computer vision library) was used. The library provides a large number of algorithms for image processing, as well as support vector machines and artificial neural networks, among other classifiers. The initial implementation consisted of the popular PCA or Eigenface algorithm for feature extraction, together with a simple distance-based classifier. Fig. 3 shows examples of the "average face" and the first 4 eigenfaces calculated for a database of faces.

Other libraries that were utilised, or are still in the process of being ported and implemented include

- libxtract, sPro and marsyas – feature extraction libraries mainly for audio.
- the shogun toolkit – a large scale machine learning toolkit with various classification algorithms.

IV. INITIAL RESULTS

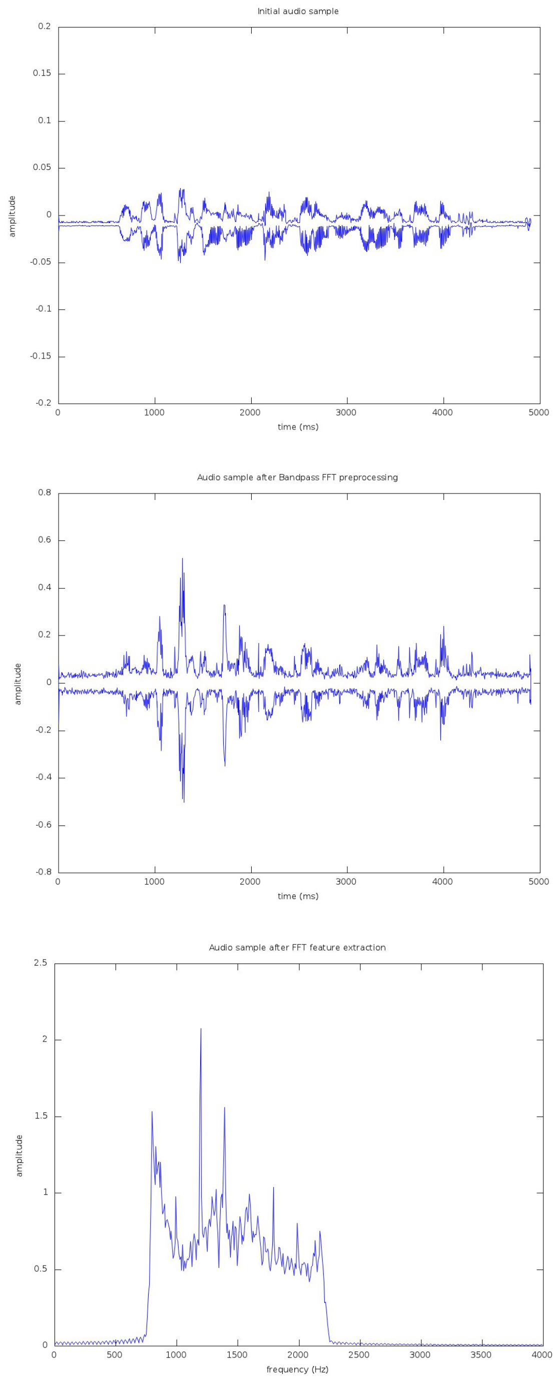


Fig. 2. A plot of a speech signal is shown as it goes through the stages from raw form, through bandpass FFT preprocessing, and then FFT-based feature extraction. These plots were made using GNU Octave

Table I gives the timing results when compared between the PC and the smartphone implementations. On average, the phone performed about 26 times slower than a PC. The accuracy obtained for some of the best algorithm combinations were quite reasonable, with the false reject rate (FRR) being in the vicinity of 20%. The accuracy can be increased by combining biometric methods (multimodal biometrics). From the table it is clear that the processing times on the smartphone were good enough for the implementation of a user-friendly biometrics system on a smartphone.

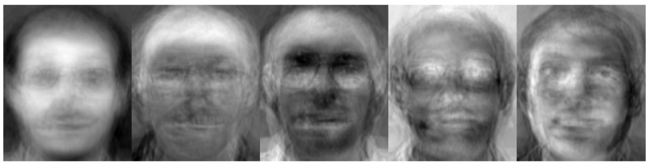


Fig. 3. From the left, the average face and the first 4 eigenfaces calculated from a face database

TABLE I. A COMPARISON OF THE TIME MEASURED FOR THE IDENTIFICATION OF A SINGLE AUDIO/IMAGE SAMPLE ON A NEXUS S SMARTPHONE WITH A PC

Average identification time (per sample)	**PC Implementation**	**Smartphone Implementation**
Java Speaker Recognition	1.73 seconds	51.94 seconds
C++ Face Recognition	6.98 ms	146.55 ms

V. CONCLUSION

The use of biometrics provides many benefits over other security mechanisms such as having to remember one or multiple PIN (personal identification number) codes. Easy-to-remember PIN codes are easily guessed, while hard-to-guess PIN codes are easily forgotten by the legitimate user. PIN code security relies on what a person knows or remembers and key-based security relies on what a person possesses, while biometric security relies on who a person is [26], [27]. This will be a very important security consideration in the future because of the use of smartphones for banking, credit card payments and other confidential activities, in addition to using NFC capabilities to enable the use of a phone for mobile payments, electronic keys to unlock car and building doors, electronic tickets with monetary value and many more. Many people also store sensitive information on their smartphones which could lead to damage if compromised [21].

In summary, smartphones are envisioned to replace all loose items that people currently carry around, such as keys, ID books, credit cards, and paper, and the security of data on mobile phones is already becoming a great concern. Biometrics provides a possible alternative for securing important mobile data.

ACKNOWLEDGMENT

The research was made possible via the support from our industry partners Telkom, Unisys, Tellumat, EMC and Alvarion; and the Technology and Human Resources for Industry Program (THRIP) managed by the National Research Foundation (NRF), financed by the Department of Trade and Industry (DTI), South Africa.

REFERENCES

[1] R. Want, “Enabling ubiquitous sensing with RFID,” *Computer*, vol. 37, no. 4, pp. 84-86, Apr. 2004.

[2] R. Want, K. P. Fishkin, A. Gujar, and B. L. Harrison, “Bridging physical and virtual worlds with electronic tags,” *Proceedings of the CHI 99 Conference: CHI is the Limit - Human Factors in Computing Systems*, pp. 370-377, 1999.

[3] NFC Forum. (2004, Mar.). Nokia, Philips And Sony Establish The Near Field Communication (NFC) Forum. [Online]. Available: http://www.nfc-forum.org/news/pr/view?item_key=d8968a33b4812e2509e5b74247d1366dc8ef91d8

[4] NXP Semiconductors. (2009, Apr.). NFC Forum Type Tags, White paper v1.0. [Online]. Available: http://www.nfc-forum.org/resources/white_papers/NXP_BV_Type_TTTT_White_Paper-Apr_09.pdf

[5] K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, 3rd edition. West Sussex, United Kingdom: Wiley, 2010.

[6] NFC Forum. (2010, Jul.). NFC Forum Connection Handover Technical Specification v1.2. [Online]. Available: http://www.nfc-forum.org/specs/spec_list/

[7] C. A. Opperman, and G. P. Hancke, “Using NFC-enabled phones for remote data acquisition and digital control,” in *Proc. IEEE Africon 2011*, Victoria Falls, Livingstone, 2011, pp. 1–6.

[8] E. E. Imhontu, and Y. O. Kumah, “A survey on Near Field Communication in mobile phones and PDAs”, M.S. thesis, School Inform. Sci., Comput., Elect., Halmstad, Univ., Halmstad, Sweden, 2010.

[9] J. Blum. (2011, Oct.). Is Google Wallet the Next Step in Mobile Payments? *Entrepreneur*. [Online]. Available: http://www.entrepreneur.com/blog/220500

[10] J. Sieck, “Location based services and museum information systems,” in *Proc. 3rd International Conference on Intelligent Systems Modelling and Simulation*, Kota Kinabalu, 2012, pp. 663–666.

[11] I. L. Ruiz, and M. A. Gómez-Nieto, “University smart poster: Study of NFC technology applications for university ambient,” *Advances in Soft Computing*, vol. 51, pp. 112-116, 2009.

[12] R. Hardy, E. Rukzio, M. Wagner, and M. Paolucci, “Exploring expressive NFC-based mobile phone interaction with large dynamic displays,” in *Proc. 2009 1st Int. Workshop Near Field Communication*, Hagenberg, Austria, 2009, pp. 36–41.

[13] C. A. Opperman, and G. P. Hancke, “A generic NFC-enabled measurement system for remote monitoring and control of client-side equipment,” in *Proc. 2011 3rd Int. Workshop Near Field Communication*, Hagenberg, Austria, 2011, pp. 44–49.

[14] K. Hyppönen, M. Hassinen, and E. Trichina, “Combining biometric authentication with privacy-enhancing technologies”, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4968, pp. 155-165, Mar. 2008.

[15] A. Juels, D. Molnar, and D. Wagner, “Security and privacy issues in e-passports”, in *1st Int. Conf. Security and Privacy for Emerging Areas in Commun. Networks*, Athens, 2005, pp. 74-85.

[16] News24. (2012, Apr.). ID smartcards not far off. *News24*. [Online]. Available: http://www.news24.com/SouthAfrica/Politics/ID-smartcards-not-far-off-20120425

[17] K. Hyppönen, M. Hassinen, and E. Trichina, “Combining biometric authentication with privacy-enhancing technologies”, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),* vol. 4968, pp. 155-165, Mar. 2008.

[18] E. E. Imhontu, and Y. O. Kumah, “A survey on Near Field

Communication in mobile phones and PDAs", M.S. thesis, School Inform. Sci., Comput., Elect., Halmstad, Univ., Halmstad, Sweden, 2010.

[19] A. Morris, S. Jassim, H. Sellahewa, L. Allano, J. Ehlers, D. Wu, J. Koreman, S. Garcia-Salicetti, B. Ly-Van, and B. Dorizzi, "Multimodal person authentication on a smartphone under realistic conditions", in Proc. *SPIE – Int. Soc. for Optical Eng.,* vol. 6250, Kissimmee, 2006.

[20] L. Allano, A. C. Morris, H. Sellahewa, S. Garcia-Salicetti, J. Koreman, S. Jassim, B. Ly-Van, D. Wu, and B. Dorizzi, "Non intrusive multi-biometrics on a mobile device: a comparison of fusion techniques", in Proc. *SPIE – Int. Soc. for Optical Eng.,* vol. 6202, Kissimmee, 2006.

[21] D. J. Kim, K. W. Chung, and K. S. Hong, "Person authentication using face, teeth and voice modalities for mobile device security", *IEEE Transactions on Consumer Electronics,* vol. 56, no. 4, pp. 2678-2685, Nov. 2010.

[22] M. O. Derawi, C. Nickely, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition", in *6th Int. Conf. Intelligent Inform. Hiding and Multimedia Signal Process.,* Darmstadt, 2010, pp. 306-311.

[23] J. R. Kwapisz, G. M. Weiss, and S. A. Moore, "Cell Phone-Based Biometric Identification", in *4th IEEE Int. Conf. Biometrics: Theory, Applicat. and Syst.,* Washington, DC, 2010.

[24] F. Okumura, A. Kubota, Y. Hatori, K. Matsuo, M. Hashimoto, and A. Koike, "A Study on Biometric Authentication based on Arm Sweep Action with Acceleration Sensor", in *Int. Symp. Intelligent Signal Process. and Commun.,* Yonago, 2006, pp. 219-222.

[25] Google Inc. (2010, Dec.). Nexus S owner's guide. [Online]. Available: http://www.samsung.com/us/Nexus_S_Owners_GuidG

[26] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition", *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 14, no. 1, pp. 4-20, Jan. 2004.

[27] K. Delac, M. Grgic, "A survey of biometric recognition methods", in *46th Int. Symp. Electronics in Marine,* Zadar, 2004, pp. 184-193.

Charl Opperman received his undergraduate degree in 2010 from the University of Pretoria and is presently studying towards his Master of Engineering degree at the same institution. His research interests include mobile computing, pattern recognition, and close-range communication protocols such as NFC and RFID.