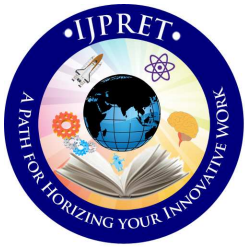
Research Article *ISSN: 2319-507X*
Rohit Jadhav, IJPRET, 2013; Volume 1(8): 948-957 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ANDROID BEAM AND FACE UNLOCK AS A SUPERIORS TECHNOLOGY FOR ANDROID

ROHIT JADHAV [1], SHRADDHA MANKAR[2], ROMIT JADHAV[3]

1. **Department of Computer Science & Engineering, P.R. Pote College of Engg.& Technology**
2. **Department of Information Technology, P.R. Patil College of Engg.& Technology**
3. **Department of Computer Science & Engineering, P.R. Pote College of Engg.& Technology**

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Histogram;
Local Binary Pattern (LBP);
Near Field Communication (NFC);
Personal Identification Number (PIN);
Radio Frequency Identification (RFID).

Corresponding Author

Mr. Rohit Jadhav

Abstract

Life on earth is incomplete without communication. Communication acts a bond between two individuals. As a means of communication, various techniques were invented, one of them being phones. With the commencement of 21st century, mobile phones have become the most sold product. Coupled with a craze and craving for speed and security with respect to everything including mobile phones have led to the creation of Android Beam and Face Unlock as a path breaking android technology for Android smart phones. Android Beam is a feature that lets users instantly share information about the applications they are using, just by touching two android beam enabled smart phones. This data sharing ensures faster exchange between the two devices than any other conventional sharing technologies. Face unlock is a unique security feature. It follows the growing trend of using human attributes as passwords to allow access to private information. This paper focuses the masked hardware technology behind Android Beam and software aspects of Face Unlock.

1. INTRODUCTION

Android is an operating system, developed for mobile devices like Smartphone's and tablet computer, which is based on Linux operating system. It was developed by Google in the year 2005. It is the Smartphone platform. Android 4.0 was announced on October 19, 2011. It includes Honeycomb features for smart phones and added new features including facial recognition unlock, network data usage monitoring and control, unified social networking contacts, photography enhancements, offline email searching, and information sharing using NFC. Within the last couple of years an expansive process has begun to emerge integrating computational logic into various kinds of objects of our everyday life and allowing us to persistently interact with those objects. The idea is to thoroughly connect virtual information to objects of the physical world and thus providing ubiquitous computing. Related to the concept of network ubiquity is the term Internet of Things referring to objects of daily use being identifiable, track able and even virtually connected via an internet-like structure. An essential enabler for this vision is the technology of Near Field Communication (NFC) that provides the possibility of linking virtual information between physical devices through proximity. As mobile phones are becoming increasingly powerful, security of the data stored in mobile phones like email, addresses, sensitive documents, etc., becomes very important. Most of the current phones have password protection to address security. However, a face recognition scheme is much more secure and flexible as it provides distinctive print to gain access and also the user need not remember passwords. This paper will provide a basic technical understanding of Near Field Communication with the capabilities of modern smart phones. It will explain the functionality of NFC and its underlying technique of Radio Frequency Identification (RFID). Its characteristics will be described and necessary hardware components including different modes of operation will be specified. Also, it will describe face recognizing unlock which could be used to unlock the phone or authorize a transaction when the registered user is recognized.

ANDROID BEAM

Android Beam is a NFC(Near field Communication) based feature that lets users instantly share information about the application they are using, just by touching two NFC-enabled phones together. NFC is built on the basis of RFID [1], [2].

2.1 RFID (Radio Frequency Identification)

It refers to small electronic devices that consist of a small chip and an antenna. Figure 1 shows the structure of the chip. The chip is typically capable of carrying 2,000 bytes of data or less. The electronic device is composed of RFID tag and RFID reader.

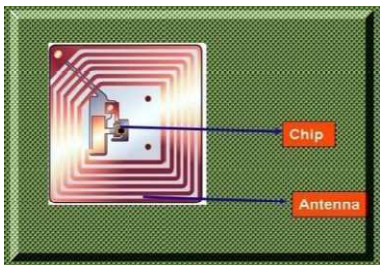


Fig 1: RFID Tag

2.1.1RFID Tag

RFID tag is a microchip combined with an antenna in a compact package; the packaging is structured to allow the RFID tag to be attached to an object to be tracked [3]. RFID tags can be as small as the size of a rice grain. There are two types of tags: active (with battery) and passive (without battery). Generally, passive tags are used. A passive tag is an RFID tag that does not contain a battery; the power is supplied

by the reader and works for shorter range of distances. When radio waves from the reader are encountered by a passive RFID tag, the coiled antenna within the tag forms a magnetic field. The tag draws power from it, energizing the circuits in the tag. The tag then sends the information encoded in the tag's memory.

2.1.2 An RFID Reader

An RFID reader as shown in Figure 2 is a device that is used to interrogate an RFID tag. The reader has an antenna that emits radio waves; the tag responds by sending back its data.

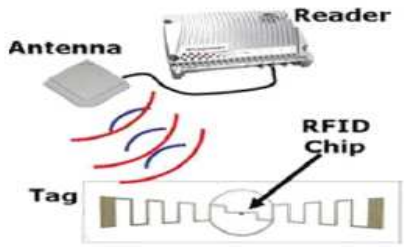


Fig. 2: RFID Reader

A number of factors can affect the read range which is the distance at which the tag can be read. The frequency used for identification, the antenna gain, the orientation and polarization of the reader antenna and the transponder antenna, as well as the placement of the tag on the object to be identified will all have an impact on the RFID systems read range. The reader reads the tag and computes the function it is

Programmed to do.

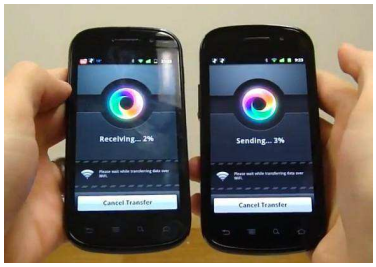


Fig. 3: NFC sharing

2.2NFC (Near Field Communication)

The acronym NFC stands for Near Field Communication. It is a two-way communication technology based on RFID. It is also called as a contactless technology. NFC technology is used in a wide array of applications such as payments at super markets and sharing content across other NFC enabled devices as in Figure 3. Near field communication technology builds on RFID advances. With the advent of Ice Cream Sandwich operating system based Android phones in the year 2011; NFC was introduced into Android phones. NFC isn't a ground breaking technology unlike Bluetooth and Wi-Fi but a wireless radio communications standard. Whereas RFID can be used from a distance, NFC readers work at a maximum range of about 4 inches (10 centimeters). NFC chips are embedded into Smartphones circuitry.

2.2.1 Working of NFC

NFC works using magnetic induction: a reader emits a small electric current, which creates a magnetic field that in turn bridges the physical space between the two devices. That field is received by a similar

coil in the client device, where it is turned back into electrical impulses to communicate data such as identification number, status information, or any other information. Passive NFC tags use the energy from the reader to encode their response, while 'active' or 'peer-to-peer' tags have their own power source and respond to the reader using their own electromagnetic fields [4]. Operating at 13.56 MHz and transferring data at up to 424 Kbits/second, NFC provides intuitive, simple, and safe communication between electronic devices. NFC is both a read- write technology.

2.2.2 Future of NFC

While NFC technology can do many things, the task most people think of tends to be making payments with a Smartphone. It's a clear, easy to understand scenario. You've finished shopping and you walk up to pay for your purchases. You whip out your Smartphone, hold it up to a receiver at the register, type in a quick PIN to identify yourself and the purchase charges to your electronic credit card.

FACE UNLOCK

Android is famous for its unique and exciting feature namely face unlock. It is introduced from version 4.x and onwards. The method behind face unlock goes like this, the front facing camera of the device scans your face and references it to the image you created while setting up the security process. If there is a match, the phone unlocks on its own. By making face recognition an optional security feature, Android Ice Cream Sandwich has followed the growing trend of using human attributes as passwords to allow access to private information. Face recognition science is neither new nor is it perfect yet. The first attempts to pinpoint a set of unique markers for each face were made in the 1960s. But the technology has got better now, with experts reporting 90 percent accuracy. In this paper, a new face recognition method based on local binary pattern (LBP) histogram is presented. First, the grey face image is divided into several parts, and then the LBP histogram of each part is calculated and concatenated together. Second, extract other concatenated histograms using different LBP operators and image blocking patterns.

All the histograms above are concatenated into the ultimate vector. The proposed approach was tested using Yale face database on Android platform. Experimental results demonstrate that the combined LBP histogram feature has an

Encouraging performance for face recognition.

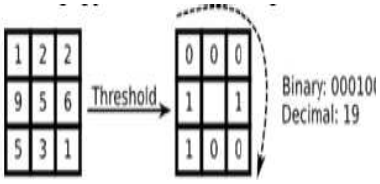


Fig 4: LPB code generator

3.1 Local Binary Pattern (LBP)

The local binary pattern (LBP) was introduced [6] originally designed for texture description [7]. The LBP was applied to texture classification in which achieved promising result [8]. In the last few years, the LBP method has been widely used for face recognition problems [9], [10]. Local Binary Pattern (LBP) operator it is possible to describe the texture and shape of a digital (grey scale) image. One LBP is a binary code for an image-pixel which tells something about the local neighborhood of that pixel. The original LBP operator was introduced by Ojala et al. [11]. This operator works with the eight neighbors of a pixel, using the value of this centre pixel as a threshold. If a neighbor pixel has a higher grey value than the centre pixel (or the same grey value) than a one is assigned to that pixel, else it gets a zero. The LBP code for the centre pixel is then produced by concatenating the eight ones or zeros to a binary code as shown in Figure 4.

3.1.1 LPB Patterns for face recognition

The original LBP operator labels the pixels of an image by threshold the 3x3 - neighborhood of each pixel with the centre value and considering the result as a binary number called the LBP code. Later the operator was extended to be applied in a

circular neighborhood of different radius size and was refined to represent the most important micro-structures with the uniform LBP [12]. The decimal form of the resulting 8-bit word (LBP code) can be expressed as follows: Where corresponds to the grey value of the center pixel (), to the grey values of the 8 surrounding pixels, and

function s is defined as: s(x) = Note that each bit of the LBP code has the same significance level and that two successive bit values may have a totally different meaning. Actually, The LBP code may be interpreted as a kernel structure index. By definition, the LBP operator is unaffected by any monotonic gray-scale transformation which preserves the pixel intensity order in a local neighborhood.

3.1.2 Face Recognition Easy Scenarios

Broadly speaking, the approaches proposed in the last years have been able to solve specific still face images recognition applications. Examples of scenarios where face recognition achieves very good results are given in Figure 5 and Figure 6 although many details are being skipped like the quality and size of the data base, scaling, feature extraction, face detection but it can be considered that in such scenarios the face recognition problem is very well focused and almost solved.

Fig 5: Easy Scenario 1

Fig 6: Easy Scenario 2

3.1.3Face Recognition Difficult Scenarios

When the scenario departs from the easy scenario, then face recognition approaches experience severe problems. Among the special challenges let us mention: pose variation, illumination conditions, scale variability, images taken years apart, glasses, moustaches, beards, low quality image acquisition, partially occluded faces etc. Figure 7 shows that position of a face isn't proper. An inclusion of addition objects

like a Hat and in Figure 8, a beard may not give proper outcome. Face recognition may fail.

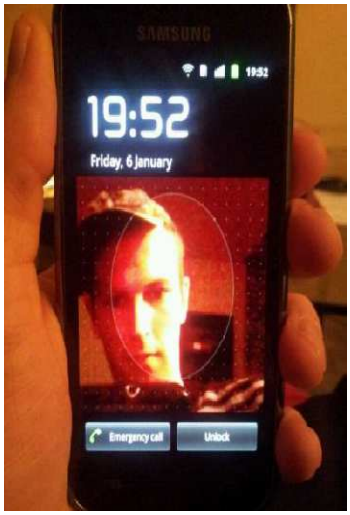


Fig 7: Difficult Scenario 1

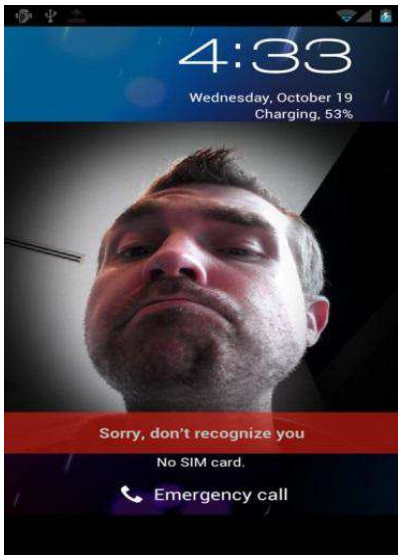


Fig 8: Difficult Scenario 2

2. CONCLUSION

Easy share ability of resources is the key to any data exchange application. Android Beam aids in seamless exchange of the same between two android beam enabled phones by just tapping the two devices. Having the ability to send data faster it removes the pairing requirements of the ageing Bluetooth

technology. The future android beam can be its usage for data transfer not only between the beam enabled phones but also for exchange between a phone and tablet or PC With changing times, mobile is soon turning into a personal diary. People prefer to keep all their important data like credit card PIN,

passwords, contacts mails fed into their mobile phones. But, at any point of time there is a constant fear of it being misused by unethical users, this led to the creation of password security by means of pin and later pattern. Both these ways still attract fraud, so to overcome it, face unlock is a better way. It maps the user's features and is a boon for the user as he doesn't have to remember codes and patterns. To further

add to development in this would be inclusion of retina scanning so as to avoid similar looking people to gain access to personal data In this paper, we have discussed the ideologies behind both the technologies so that we can make mobile phone experience more beautiful, faster as well as more secure.

3. REFERENCES

1. John R. Vacca, Radio Frequency Identification Security, Network and System Security, Syngress,2010,333-338

2. SandipLahiri, Technology Overview, RFID Sourcebook, IBM Press, 2005, 5-46

3. Pamela Zelbst, Victor Sower, : RFID Technology Essentials, RFID for the Supply Chain and Operations Professional, Business Expert Press, 2012, 14-18

4. VedatCoskun, Kerem Ok, BusraOzdenizci, NFC Essentials, Near Field Communication(NFC) : From Theory To Practise, John Wiley & Sons, 2011,55-58

5. http://www.technology.com/ct/Technology-Article.asp?ArtNum=2

6. T. Ahonen, A. Hadid and M. Pietikinen, Face recognition with local binary patterns. Computer Vision, ECCV 2004 Proceedings, Lecture Notes in Computer Science 3021, Springer, pp. 469-481, 2004.

7. T. Ojala, M. Pietikainen, and D. Harwood, A comparative study of texture measures with classification based on feature distributions,Pattern Recognition, vol. 29 , 1996, pp. 51-59.

8. T. Ojala, M. Pjetikainen, Multiresolution Grey-Scale and Rotation Invari-ant Texture Classification with Local Binary Patterns, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, pp.971-987, 2002.

9. T. Ahomen, A. Hadid, and M. Pietikainen, Face recognition with local binary patterns, Computer Vision, ECCV 2004 Proceedings, Lecture Notes in Computer Science 3021, Springer, 2004, pp. 469-481.

10. S. Marcel, Y. Rodriguez and G. Heusch: On the Recent Use of Local Binary Patterns for Face Authentication, International Journal on Image and Video Processing

Special Issue on Facial Image Processing, 2007.

11. T. Ojala, M. Pietikainen and D. Harwood. A comparative study of texture measures with classification based on feature distributions. Pattern Recognition vol. 29, 1996.

12. T. Ojala, M. Pietikinen and T. Maenpaa, Multiresolutiongray-scale and rotation invariant texture classification with local binary patterns, IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 24, pp. 971987, 2002.