Finger Print Matching Algorithm for Android

Authors :

Kavita Rathi
P G Student Datta Meghe College of Engg.
Airoli ,Navi Mumbai.400708

Sudhir Sawarkar
Principle of Datta Meghe College of Engg.

Abstract

We propose a secure robust, and low cost biometric authentication system on the mobile devices. Mobile computing devices such as Smartphone's, tablets and wireless enabled laptops are getting widely popular and being frequently used to access information in secure networks through third party providers. With the increasing number of intrusion, device and identity theft incidents, improved security measures are becoming essential for accessing devices as well as various mobile applications. Hence security is of paramount importance in today's world. The project we propose to make will firstly need the user to register with application the user will have to provide credentials along with his fingerprints and the fingerprint of the member to grant his access to information. After registering with one just has to authenticate using fingerprint if the fingerprint matched with that of the stored in database the required information is displayed in this way, the user need not remember any password in order to log in to application. This will reduce the cumbersome task of remembering the password and increase the security as the fingerprint is unique. The proposed architecture is expected to provide secure access to only legitimate users of a system within a short period of time and prohibit intruders from gaining any access.

Keywords - biometrics, information security, mobile computing, systems flowchart

1. Introduction

Recently, performance of mobile devices, such as cellular phones and personal digital assistants (PDAs), has improved dramatically the. Mobile devices are now able to store large amounts of information. In addition, applications of these mobile devices have been broadened to include services requiring security functions, e-banking, e-commerce, etc. These have caused mobile-device manufacturers to install more secure authentication methods than the simple conventional personal-identification-number-based method. To satisfy these demands, some contemporary mobile devices adapt the fingerprint-verification function. These devices embed extra sensors to capture fingerprint images at low costs. However, additional sensor increases the cost of the mobile device because new product design and platform development are additionally required. To reduce the costs, built-in cameras can be used to obtain the fingerprint images. This approach is very attractive because additional hardware costs are unnecessary, and modern cameras that are built in mobile devices can already provide high-resolution and close-up images. Once a built-in camera is used as the input device, the acquisition of suitable images for fingerprint verification is the fundamental step. The prevailing techniques of user authentication, which involve the use of either and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations. User IDs and passwords can be changed as often as required. Yet, the user only has a limited number of biometric features (one face, ten fingers, and two eyes).And which cannot be copied. Additionally, a biometric property of an individual can be lost only in case of serious accident. The aim of this dissertation is to develop a secure architecture for mobile network using inbuilt camera. First, study several biometric identification techniques are reviewed and the security challenges with each technique is investigated. Then a generic securely

approach for mobile devices using biometrics is proposed and evaluated. This project is implemented by using android, and open CV library so that it will work on all android operating systems mobile version 2.2 to advance version this will work with
all camera starting from 2megapixel it does not need a very high resolution camera.

Figure1:Atrix4G with fingerprint scanner.

The objective of this dissertation is to develop a secure architecture for mobile network and system involving biometric information. First, several biometric identification techniques are reviewed and the security challenges with each technique is investigated. Then a generic securely approach for mobile devices using biometrics is proposed and evaluated.

Android OS:

Figure 1: android

Android is a Linux-based operating system designed primarily for touch-screen mobile devices such as Smartphone's and tablet computers. Initially developed by Android, Inc., which Google backed financially and later bought in 2005, Android was unveiled in 2007 along with the founding of the Open Handset Alliance: a consortium of hardware, software, and telecommunication companies devoted to advancing open standards for mobile devices. The first Android-powered phone was sold in October 2008. Android is open source and Google releases the code under the Apache License. This open-source code and permissive licensing allows the software to be freely modified and distributed by device manufacturers, wireless carriers and enthusiast developers. Additionally, Android has a large community of developers writing applications ("apps") that extend the functionality of devices, written primarily in a customized version of the Java programming language. In October 2012, there were approximately 700,000 apps available for Android, and the estimated number of applications downloaded from Google Play, Android's primary app store, was 25 billion. A developer survey conducted in April–May 2013 found that Android is the most popular platform for developers, used by 71% of the mobile developer population. These factors have contributed towards making Android the world's most widely used Smartphone platform, overtaking Symbian in the fourth quarter of 2010, and the software of choice for technology companies who require a low-cost, customizable, lightweight operating system for high tech devices without developing one from scratch. As a result, despite being primarily designed for phones and tablets, it has seen additional applications on televisions, games consoles, digital cameras and other electronics. Android's open nature has further encouraged a large community of developers and enthusiasts to use the open-source code as a foundation for community-driven projects, which add new features for advanced users or bring Android to devices which were officially, released running other operating systems.

Open CV:

Open CV (Open Source Computer Vision Library) is a library of programming functions mainly aimed at real-time computer vision, developed by Intel, and now supported by Willow Garage and Itseez. The library is cross-platform. It focuses mainly on real-time image processing. If the library finds Intel's Integrated Performance Primitives on the system, it will use these proprietary optimized routines to accelerate itself. Open CV is written in C++ and its primary interface is in C++, but it still retains a less comprehensive though extensive older C interface. There are now full interfaces in Python, Java and MATLAB/OCTAVE (as of version 2.5). The API for these interfaces can be found in the online documentation.

II. Review Of literature

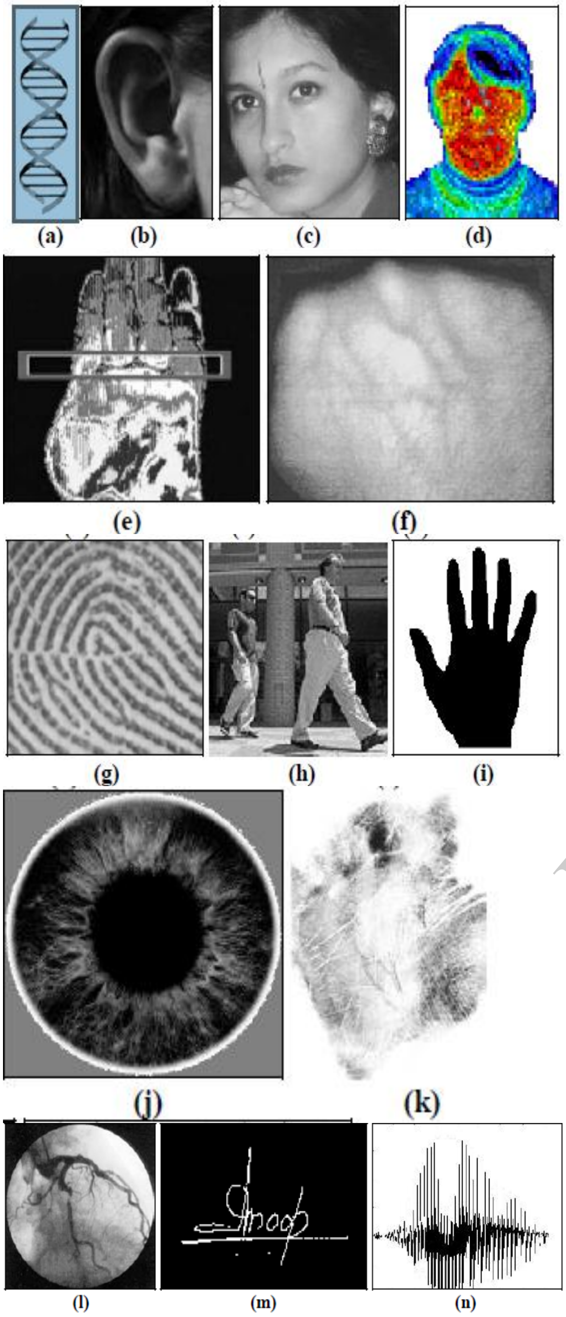


Figure 4. Examples of biometric characteristics: a) DNA, b) ear, c) face, d) facial thermo gram, e) hand thermo gram, f)hand vein, g) fingerprint, h) gait, i) hand geometry, j) iris, k) palm print, l) retina, m) signature, and n) voice.

Different numbers of biometric signatures are present and are used in different devices. Biometric has its strength and weakness and the choice is depend on the user, no biometric is "best". The match between a specific biometric and an application is determined depending upon on the operation of the application.[1] Different biometric signatures are shown in fig4.The use of biometrics to secure mobile devices has been explored in recent years, especially after emergence of smart phones with higher processing capabilities. Majority of the phones available in market do not have any dedicated component for recording biometric data. The camera, microphone and touch screen are mainly used as interfaces to collect biometric data. In 2011, Motorola released Atrix 4G smart phone which includes a dedicated fingerprint reader. It is also possible to enhance fingerprint images and ***the old Fujitsu F505i [7].***from mobile phone cameras and extract fingerprint features for scanning and verification purposes [2].Like palm print, where the lines of the palm are analyzed for identification, finger lines also have the potential for persona l identification for mobile phones. Face recognition techniques have also been applied to identify individuals using mobile phone cameras [3]. As most smart phones and tablets are now equipped with medium to high resolution cameras, face recognition can be performed from pictures taken with moderate lighting conditions. Eye features, such as iris scan, pupil, eye shape and distance between eyes, can be used to more precisely identify individuals [4]. In addition, teeth shape authentication can make the recognition performance more accurate where individual and overall teeth shapes are analyzed to perform matching [5].Voice or speech recognition using microphone can also be used for user authentication in order to access mobile devices [6]. In this case, the smart phone user would be asked to speak a set of words or sentences and thus the response are recorded to retrieve voice samples. For authentication purpose, the user might be asked to speak a selected sentence or words, where from voice traits, such as pitch magnitudes, tones, breaks and vibration frequencies, can be verified. Authentication using voice may fail to identify individuals due to factors such as flue, cold or emotional states. It can also be noted that perpetrators can use recorded voice and try to gain access as the legitimate user. Behavioral traits, such as keystroke dynamics, are another set of features that can be used to authenticate users [7]. When smart phone and tablet users type various words in their phone using keypad or touch screen, time between key strokes are recorded and analyzed. Hence a typing pattern of different words is derived which can then be utilized to verify the identity of a person [8].

III. Proposed architecture

An overview of the proposed system architecture for mobile security is shown in the block diagram of Fig.3 Skin color segmentation: In isolating skin color region normalized RGB, HIS and YCrCb color space transformations are commonly used. Based on the color component values, each pixel is classified as skin or non-skin. In this architecture RGB matching algorithm is used the number of pixels used to represent the finger in mobile phone photos dominates the pixels used to represent other part of the body. Therefore these approaches are likely to give good results on handsets. To reduce the effects of illumination variations scale-by-max color balancing is done. Many complex methods have been used in the literature to do the processing of images in extreme illumination conditions. One of the simplest methods to implement on a mobile phone could be do the calculations in RGB space

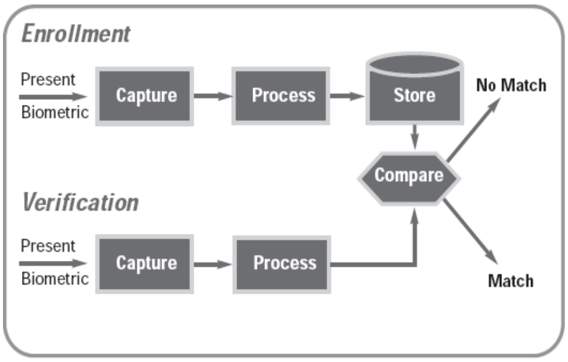


Figure5: An overview of the proposed mobile device security architecture

Algorithm:

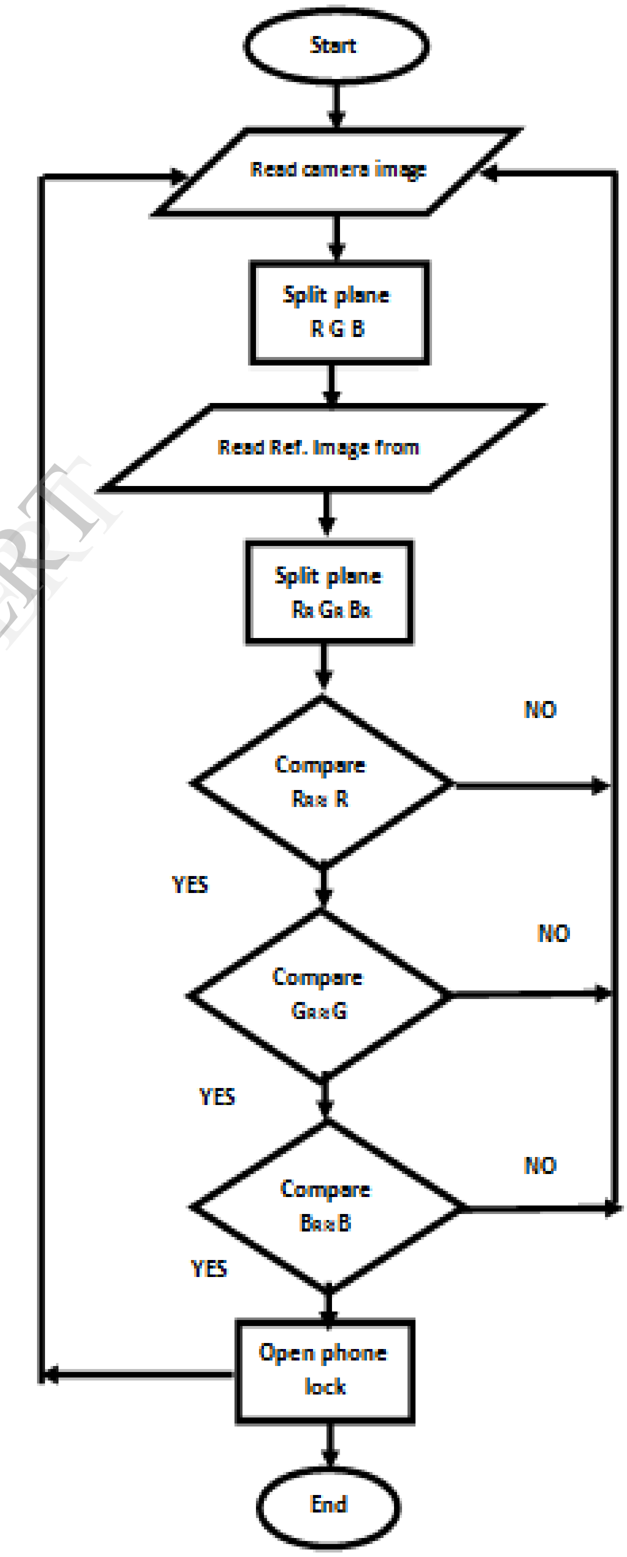
1) Read the image from the camera. It should necessarily be in Bitmap format.
2) Split the current image into three bit planes, namely R G B.
3) Read the reference image from the database.
4) Split the reference image into three bit planes, namely R G B.
5) Compare the R plane of the reference image with the R plane of current image
    - If the Euclidian distance between the planes is within the threshold, continue.
    - If the Euclidian distance between the planes does not lie within the threshold, go to step 10

6) Compare the G plane of the reference image with the G plane of the current image
    - If the Euclidian distance between the planes is within the threshold, continue.
    - If the Euclidian distance between the planes does not lie within the threshold, go to step 10

7) Compare the R plane of the reference image with the R plane of the current image
    - If the Euclidian distance between the planes is within the threshold, continue.
    - If the Euclidian distance between the planes does not lie within the threshold, go to step 10

8) Compare the B plane of the reference image with the B plane of the current image
    - If the Euclidian distance between the planes is within
    - If the Euclidian distance between the planes does not lie within the threshold, go to step 10

9) The images have successfully matched.
10) Stop.



Result and Discussion:

Now days tshe Smartphone’s stored our important information. Our aim if the costly mobile device is stolen by theft it should not be usable for the theft. This is very innovative idea to authenticate mobile devices using biometric. It is much secured and difficult to steal as biometric is unique. In this project we are taking no of samples and by using RGB algorithm the samples are matched with the samples stored in database. Initially 77%-78% accuracy is possible with RGB algorithm. In future we will use different image processing algorithm like KMEANS, edge detection.

Correct fingerprint:

	No of samples	Correctly Detected	Accuracy
Person1	100	82	82%
Person2	100	72	72%
Person3	100	79	79%

Wrong fingerprint:

	No of samples	Wrongly Detected	Accuracy
Person1	100	33	77%
Person2	100	32	78%
Person3	100	34	76%

Conclusion:

This is very innovative idea to authenticate mobile devices using biometric. It is very secured and difficult to steal. In this project a robust system is developed for mobile devices security. This implemented architecture can be used in all android mobile. Even if the accuracy of the biometric techniques is not perfect yet making a secure biometric systems is, however, not as easy as it might appear. The word biometrics is very often used as a synonym for the perfect security without need of dedicated scanner and the security is increased against intrusion theft and manipulation of devices.

References:

[1] A. Jain, A. Ross, S. Prabhakar, "An introduction to biometric," *IEEE Transaction On Circuits and System for Video Technology*, vol. 14, no. 1, pp. 4 – 20, 2004.

[2] D. Lee, K. Choi, H. Choi and J. Kim, "Recognizable-image selection for fingerprint recognition with a mobile-device camera," *IEEE Systems, Man, and Cybernetics Society*, vol. 38, issue 1, pp. 233 – 243, February 2008.

[3] K. Choi, K. Toh and H. Byun, "Realtime training on mobile devices for face recognition applications," *Pattern Recogn*, vol. 44, no. 2, pp. 386 – 400, February, 2011.

[4] K. Park, H. Park, B. Kang, E. Lee and D. Jeong. "A study on iris localization and recognition on mobile phones," *EURASIP J. Adv. Signal Process*, vol. 2008, January 2008.

[5] D. Kim, K. Chung and K. Hong, "Person authentication using face, teeth and voice modalities for mobile device security," *IEEE Transaction on Consumer Electronics*, vol. 56, no. 6, pp. 2678 – 2685, November 2010.

[6] G. Crescenzo, M. Cochinwala and H. Shim, "Modeling cryptographic properties of voice and voice-based entity authentication," *Proceedings of the 2007 ACM workshop on Digital identity management (DIM '07)*, New York, NY, USA, pp. 53 – 61, November, 2007.

[7] A. Peacock, X. Ke, and M. Wilkerson, “Typing patterns: a key to user identification,” *IEEE Security & Privacy*, pp. 40 – 43, 2004.

[8] E. Maiorana, P. Campisi, N. González-Carballo and A. Neri, "Keystroke dynamics authentication for mobile phones," *Proceedings of the 2011 ACM Symposium on Applied Computing (SAC '11)*, pp. 21 – 26, March, 2011