IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 11, Issue 4, Ver. I (Jul.-Aug .2016), PP 13-16
www.iosrjournals.org

Securing Online Transaction using Fingerprint Authentication with Embedded Cameras

Miss. Gayatri Kulkarni[1], Mrs. Deepali Raut-Dhole[2]
[1](M.E E&TC, A'Nagar, Maharashtra, India,gayatri.kulkarni1990@gmail.com)
[2](M.Tech DECS, Pune, Maharashtra, India,raut.deepa3@gmail.com)

Abstract: *Now a day's mobile phone became smart phone with lot of features. Smart phone comes with high resolution cameras and support high speed internet. This tends to increase the use of online transactions. But these is secured only by ID no. & password, this is not so secured. Biometric characteristics like fingerprint are changes person to person. So to increase the security of online transactions we use Fingerprint recognition with credit card/debit card transaction. Smart phone with high pixel camera function are capable of capturing image & processing task. In this proposed system cell phones cameras capturing fingerprint images as biometric traits. No need of extra module for fingerprint recognition.*

Keywords: *Smart phone, Embedded Camera, Fingerprint recognition, online transaction.*

I Introduction

Everyday a lot of new mobile phones called as smart phones come in a market with various features like embedded cameras, Fast processors, pocket high speed Internet & many more. By using embedded camera we can take photos & shoot videos. Some of embedded cameras have high resolution & high picture quality images more than 5 Mega-Pixels. Due to high speed internet almost all banking technology has changed to online. So the traditional way of shopping is changed to Internet shopping also we can pay the various bills, transfer the money by using online transactions. But security of online transactions is a big issue. Now days this system is secured only by credit card/debit card no/ ID no, CVC no. & OTP (one time password) which is send on registered mobile no. Moreover, the services which can be accessed via smart phones (e.g., m-banking and m-commerce etc.) represent a major value. Therefore, the danger of a mobile device ending up in the wrong hands presents a serious threat to information security and user privacy. According to the latest research from Halifax Home Insurance claims, 390 million British pounds a year is lost in Britain due to the theft of smart phones. With the average handset costing more than 100 British pounds, it is perhaps not surprising that there are more than 2 million stolen in the UK [1] & India every year.

Biometric characteristics like fingerprint, voice pattern, iris etc cannot be stolen or forgotten & also biometric characteristics are unique & remain same even fingerprints of twins are different. So it's most promising technology for authentication. Approximately from 14th century fingerprints were stamping on paper using ink for identification of person. Now days they are captured as live-scan digital images acquired by directly sensing the fingerprint surface with an electronic fingerprint scanner. The fingerprint pattern displays different features at different levels. Some smart phone has inbuilt fingerprint scanner. But they are very costly. Many fingerprint recognition algorithms perform well on databases that had been collected with high-resolution cameras and in highly controlled situations [2].

In this paper we present fingerprint recognition as means of verifying the identity of the user using embedded camera. We use Fingerprint of user as a password for online transactions. The image of fingerprint is captured by using embedded camera of smart phone. Mostly more than 5 Mega-pixel cameras are used for capturing the image of fingerprint traits. This image is compared with the database. If the image is matched with the database then user can do the online transactions. This is the most secure and easy method. The main purpose of this paper is to lower down the user effort while keeping the error rates in an acceptable and practical range. Therefore, this proposal is a realistic approach to be implemented in mobile devices for user authentication.

II Fingerprint Recognition

Fingerprint recognition is the most matured approach among all the biometric techniques. With its success of use in different applications, it is today used in many access controls applications as each individual has a unique fingerprint. The hand skin or the finger skin consists of the so called friction ridges with pores. The ridges are already created in the ninth week of an individual's fetal development life [3], and remains the same all life long, only growing up to adult size, but if severe injuries occur the skin may be reconstructed the same as before. Researchers have found out that identical twins have fingerprints that are quite different and that in the forensic community it is believed that no two people have the same fingerprint [4].

Many capture device technologies have been developed over the last decades replacing the old ink imaging process. The old process was based on sensing ridges on an individual's finger with ink, where newer technologies uses a scanner placing the surface of the finger onto this device. Such technologies are referred to as live-scan and based on four techniques [5]:

Frustrated total internal reflection (FTR) and optical methods is a first live scan technology. Figure 1 illustrates how the reflected signal is acquired by a camera from the underside of a prism when a finger touches the top of the prism. The typical image acquisition surface of 1 inch by 1 inch is converted to 500 dots per inch (DPI) using either charge coupled device (CCD) or complementary metal oxide semiconductor (CMOS) camera.

In CMOS Capacitance, The ridges and valleys create different charge accumulations, when a finger hits a CMOS chip grid. This charge is converted to an intensity value of a pixel using various competing techniques such as alternating current (AC), direct current (DC) and radio frequency (RF). The typical image acquisition surface of 0.5 inch by 0.5 inch is converted to 500 dots per inch (DPI). The resultant images also have a propensity to be affected by the skin dryness and wetness.

Another method is Ultrasound Sensing. The thermal sensor is developed by using pyro-electric material, which measures temperature changes due to the ridge-valley structure as the finger is swiped over the scanner and produces an image. In this case the skin is a better thermal conductor than air and thus contact with the ridges causes a noticeable temperature drop on a heated surface. This technology is claimed to overcome the dryness and wetness of the skin issues of optical scanners. But the resulting images are not affluent in gray value images. The thermal sensor is becoming more popular today, because they are small and of low cost. Swipe sensors based on optical and CMOS technology are also available as commercial products.

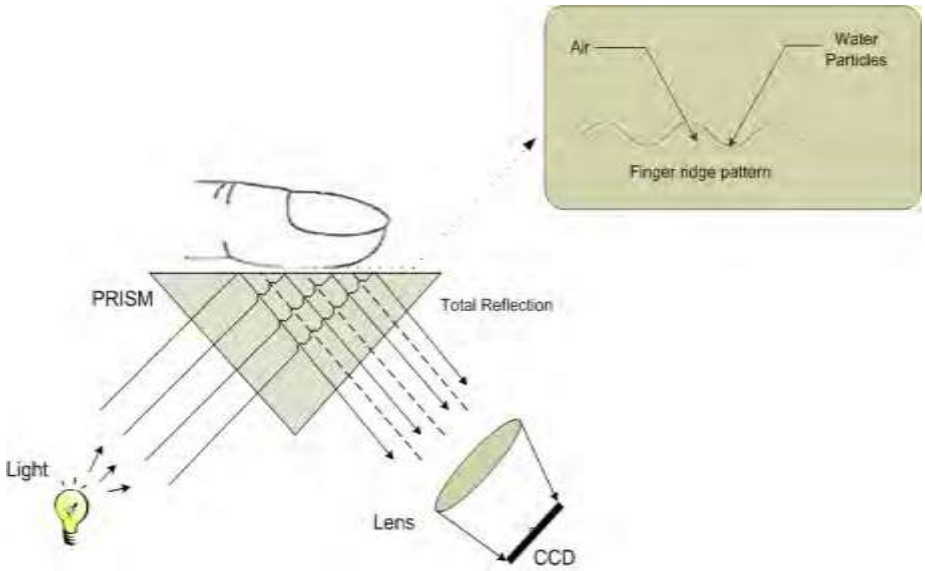

Fig 1. Optical fingerprint sensing by frustrated total internal reflection

III Data collection

3.1 Data collection steps

There is no any standard database is available for fingerprint images captured by digital camera so we have to constructed own database. The constructed independent database consists of 1320 fingerprint images. These images stem from 220 finger instances, where each instance was captured 6 times. The minimum specifications required for embedded camera of smart phones are: - 5 mega pixel, high resolution (2592x1944), high speed cameras with LED flash and autofocus. The images are stored in the internal memory of the phones and all the images were collected in the cameras "Burst Mode". Existing smart phone cameras are not designed for biometric use and accurate focusing will always be a challenge for fingerprint image capturing. We address these potential challenges in this paper in a simplified way to investigate whether smart phone camera can generate good quality samples and corresponding good biometric performance in a relative stable data collection environment.

1.2 Evolution

The user's fingerprint image captured by using embedded camera of smart phone is our biometric sample. Next step is to extract the sample. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. We use minutia points for extraction of sample. The extracted

minutia points are used for comparison between stored database & user. The result of the comparison is called the similarity score S, where a low value of S indicates little similarity, while a high value indicates high similarity. The last step is to compare the similarity score S to a predefined system threshold T, and output a decision based on both values. In case the similarity score is above the threshold (S > T) then the user is accepted as genuine, while a similarity score below the threshold (S < T) indicates an impostor who is rejected by the system. Obviously the biometric features of the user must initially be stored in the database before any comparison of a probe feature vector can take place. This is done during the enrolment phase. During the enrolment biometric samples are captured from the biometric characteristic, after which it is processed and features are extracted. The extracted data is now stored in a database and linked to the identity of the user who enrolled. The stored data in the database is referred to as the reference template of the user. In case of fingerprint biometrics it is a common approach to derive the features from multiple captured samples and generate a single minutiae template.

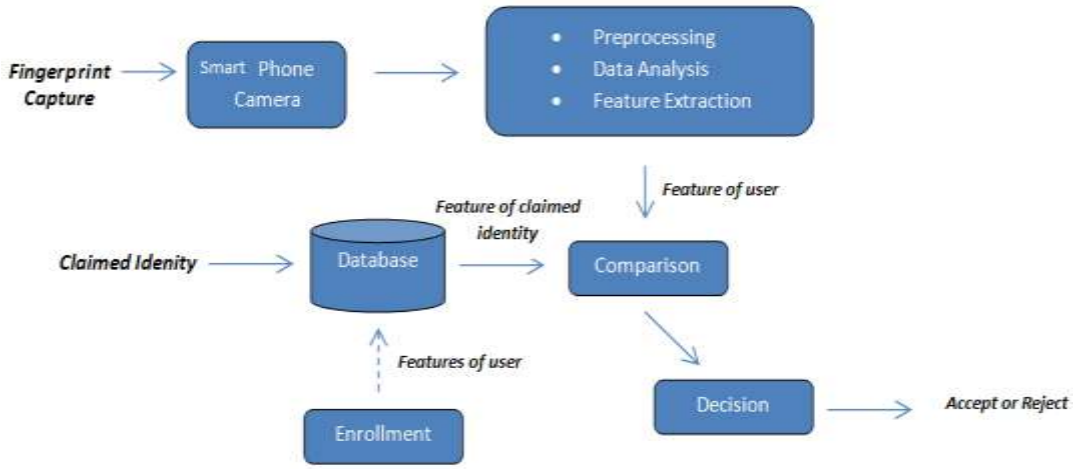

Fig 2: Verification process of System

In order to measure the sensor performance we have applied the Neurotechnology, Verifinger 6.0 Extended SDK commercial minutia extractor for the feature extraction. The SDK includes functionality to extract a set of minutiae data from an individual fingerprint image and to compute a comparison-score by comparing one set of minutiae data with another. Both SDKs support open and interoperable systems as the generated minutiae templates can be stored according to the ISO or ANSI interchange standard [6].

IV Flow of system

The following steps are followed when we are doing online transactions by using finger print recognition.

1. Open the particular website or App for e-banking or e-shopping.
2. Choose the particular option or request an order.
3. Then enter credit card/debit card no.
4. If credit card no/debit card no. matches then enter pin no. and captured the image of particular fingerprint.
5. Verify the pin no. & fingerprint image with the database. If it matches then only you can do the online transactions.

V Conclusion

Securing online transactions has been wide research area because now day's cyber crimes are increased. Third party can hack your bank account and removed your all money from your account. If smart phone is lost or stolen in an unattended moment then sensitive information is accessible from the mobile device but also transactions on the stock market and other critical services, which grant access to financial assets. So we have introduced a solution to check user's identity based on biometric characteristics i.e fingerprint authentication by using embedded camera of smart phone. In this system no any extra hardware is required to scan fingerprint. So this proposed system is very easy and provides high security as well as safety to user.

For a stable fingerprint recognition application to be performed in a smart phone we have to considered some factors while taking image of fingerprint like plain background of image, geometric distortion, LED flash & image quality assessment. This system when fully deployed will definitely reduce the rate of fraudulent activities on online transactions.

Acknowledgements

We would like to thank our family & friends for their unending support and wisdom urged us to pursue new ideas with their support and guidance.

References

[1] Mobile phone theft increasing across the uk. http://www.insure4u.info/home-insurancemobile/mobile-phone-theft-increasing-across-theuk.html. [Online; accessed 30-March-2011].
[2] Nist image group's fingerprint research. http://www.itl.nist.gov/iad/894.03/fing/fing.html.[Online; accessed 13-February-2011].
[3] Fetal development http://www.pregnancy.org/fetaldevelopment.[Online; accessed 13-February-2011].
[4] Sharath Pankanti, Salil Prabhakar, and Anil K. Jain. On the individuality of fingerprints. IEEE Trans. Pattern Anal. Mach. Intell., 24:1010–1025, August 2002.
[5] Ruud Bolle, Jonathan Connell, Sharanth chandra Pankanti, Nalini Ratha, and Andrew Senior. Guide to Biometrics. SpringerVerlag, 2003.
[6] Fingerprint Recognition with Embedded cameras on mobile phones by Mohammad Omar Derawi, Bian Yang, Christoph Busch. https://www.researchgate.net/publication/256010598, January 2012.