Journal of Information Sciences and Computing Technologies(JISCT)
ISSN: 2394-9066

SCITECH
RESEARCH ORGANISATION|

Volume 8, Issue 1
December 05, 2018

Journal of Information Sciences and Computing Technologies
www.scitecresearch.com/journals

A New Hand Based Biometric Modality &An Automated Authentication System

Nirmal Pandey[1], Prof O.P. Verma[2], Dr Amioy Kumar[3]

Abstract.

With increased adoption of smartphones, security has become important like never before. Smartphones store confidential information and carry out sensitive financial transactions. Biometric sensors such as fingerprint scanners are built in to smartphones to cater to security concerns. However, due to limited size of smartphone, miniaturised sensors are used to capture the biometric data from the user. Other hand based biometric modalities like hand veins and finger veins need specialised thermal/IR sensors which add to the overall cost of the system. In this paper, we introduce a new hand based biometric modality called Fistprint. Fistprints can be captured using digital camera available in any smartphone. In this work, our contributions are:i) we propose a new non-touch and non-invasive hand based biometric modality called fistprint. Fistprint contains many distinctive elements such as fist shape, fist size, fingers shape and size, knuckles, finger nails, palm crease/wrinkle lines etc. ii) Prepare fistprint DB for the first time. We collected fistprint information of twenty individuals - both males and females aged from 23 years to 45 years of age. Four images of each hand fist (total 160 images) were taken for this purpose. iii) Propose Fistprint Automatic Authentication SysTem (FAAST). iv) Implement FAAST system on Samsung Galaxy smartphone running Android and server side on a windows machine and validate the effectiveness of the proposed modality.

The experimental results show the effectiveness of fistprint as a biometric with GAR of 97.5 % at 1.0% FAR.

Keywords: *Fistprint; biometric modality; smartphone security; automatic authentication system.*

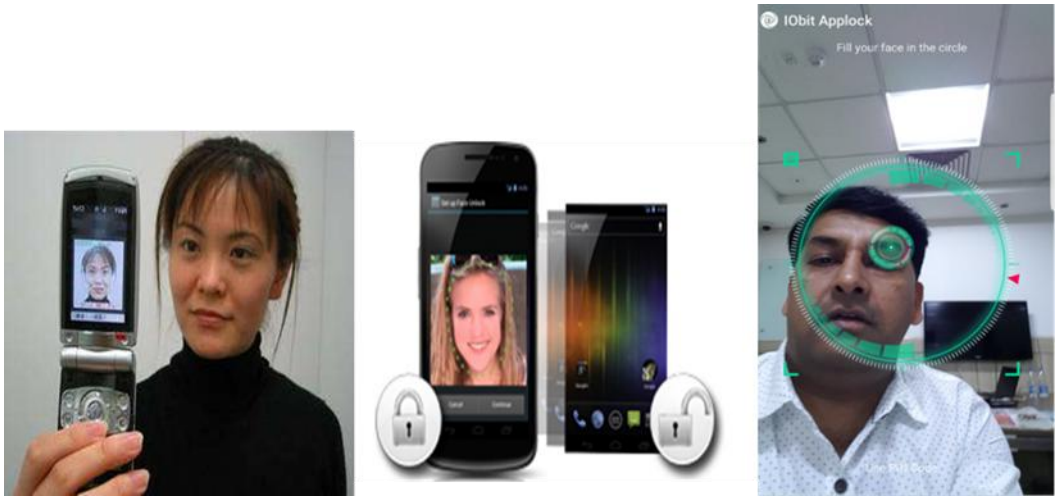
[1]Department of Computer Science & Engineering, Delhi Technological University, New Delhi – 110042
[2]Department of Computer Science & Engineering, Delhi Technological University, New Delhi – 110042
[3]Formerly Guest Faculty (Department of Computer Science & Engineering), Delhi Technological University New Delhi – 110042

I. INTRODUCTION

Biometrics refers to authentication of human beings based on biological features as well as behavioural characteristics [1]. Each of these features or characteristics is called biometric modality. Till recently, traditional identification methods viz. personal identification numbers, passwords, passphrases, hint questions, pattern drawing were very common in smartphones. But all these methods suffer from the weakness of being forgotten or lost. Biometric modalities-based authentication in smartphones is picking up in recent times. Biometric methods have the advantage of being more secure as well as more convenient. Hand based biometric modalities have always been a preferred choice due to non-invasiveness, ease of use and high user acceptance. Fingerprints, palm prints, hand shape, hand appearance, hand geometry, finger knuckles, hand veins and finger veins have been used for authentication purposes.

Due to increased threat to private and confidential data stored in smartphones, OEMs have started integrating biometric enabled security features in smartphones. To the best of our knowledge, OMRON Corporation introduced first facial recognition Biometric for phones[4]. Google introduced face recognition in Nexus Android smartphone produced by Samsung[5]. After that it became a regular feature on most of Android based smartphones. The figure below shows various smartphones with face unlock feature. However, there are several lacunae in the security of the device with face unlock feature. Face unlock features use front camera of the device, which in most of the phones, is of low resolution in comparison to rear camera. Front camera is not able to capture face images with good quality due to low resolution. Moreover, it is also impacted by environmental constraints like low visibility etc. Recently some cases of spoofing smartphone face unlock system has also been reported[6] which makes it less reliable.

[4] https://phys.org/news/2005-03-world-recognition-biometric-mobile.html
[5] http://www.samsung.com/levant/consumer/mobile-devices/smartphones/others/GT-I9250CWATHR/
[6] https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/



a) b) c)

Fig1: Face Unlock Feature (a) OMRON System (b) Google Nexus (c) Samsung Galaxy Note 7 using IOBitApplock[7]

Fingerprint is another biometric which is commonly available in smartphones. Motorola was the first OEM to introduce finger print unlock feature in its Atrix smartphone[8]. This feature was popularised after its introduction in Apple IPhone 5s [25] with the commercial name "Touch ID"[9]. The figure below shows fingerprint system in various smartphones. Fingerprint biometric is very popular and has been accepted by most of the smartphone users. However, fingerprint biometric in smartphones suffer from serious security problems. The main problem with fingerprint scanners is small size of the sensor. Due to this, sensor is not able to take complete scan of the finger. In this process, there is loss of biometric continents in the scanned finger image. This makes it unsuitable for high security applications such as financial transactions.

[7] http://www.iobit.com/en/applock.php
[8] http://www.news18.com/news/india/motorola-atrix-had-a-fingerprint-scanner-two-years-before-iphone-5s-638036.html
[9] https://support.apple.com/en-us/HT201371

a) b)

Fig 2: Fingerprint Unlock Feature (a) Motorola Atrix(b) Samsung Galaxy Note 7

Recently Iris biometric unlock feature has been introduced in smartphones [26] as well as tablets[10]. The figure below depicts Iris unlock feature on Samsung Galaxy Note 7 device. The Iris has large amount of distinctive biometric information that is used to uniquely identify individuals. It is considered to be very safe and secure biometric. However, there are several difficulties faced while putting integrating this biometric on the smartphone platform. Iris biometric needs additional sensors (2 or more) to be added on the front side of the smartphone. This increases the cost of the device. Also, Iris scanning is negatively impacted in bad environmental conditions like low light, or eye disease etc.

Thus there is strong need to have a biometric for smartphones which is cost effective, accurate, easy to use, non-intrusive as well as user friendly. In this work, we present a novel hand based biometric modality called fistprint.

[10] http://www.androidauthority.com/samsung-galaxy-tab-iris-694726/

Fig 3: Iris Unlock Feature Samsung Galaxy Note 7

Fist is formed by curling extended fingers towards palm and clinching the thumb. Clinching of fist in aforementioned fashion exposes some parts of palm as well as dorsal part of hand which contain features that could be used to uniquely identify individuals. The combination of these biometric elements viz. fist shape, fist size, fingers shape and size, knuckles, finger nails, palm crease/wrinkle lines etc. is termed as fistprint. Since this biometric modality is being proposed for the first time, there is no DB available. We present a fistprint DB of 20 subjects (malesas well as females), containing fistprints from left as well as right hand. The fistprint images are taken using Samsung Galaxy Note 3 rear camera.

In this paper, we also present an online automatic authentication system using fistprint biometric modality, Fistprint Automatic Authentication SysTem (FAAST). The client side of this system is implemented on Samsung Galaxy smartphone running Android and server side on a windows machine. Experimental test results are also provided.

Rest of the paper is organized as below. In section II, we present a survey of prior research done related to hand based biometric modalities and systems. Most of these researches show various degrees of accuracy. The details of newly introduced biometric modality i.e. fistprint are presented in Section III. Section IV shows image acquisition and processing and formation of fistprint DB of 20 subjects. FAAST system architecture is given

under Section V. The experimental test results are given under Section VI. Under Section VII, conclusion of the work done is given and scope for future research outlined.

II. STATE OF THE ART AND CONTRIBUTIONS

A. Prior Work

Fingerprints, palm prints, hand shape, hand appearance, hand geometry, finger knuckles, hand veins and finger veins have been used in various biometric authentication systems [2]. Amongst hand driven biometric modalities, fingerprints have been investigated in great detail. A.K. Jain [3] described the way an automatic fingerprint identification system (AFIS) can be implemented and reported the success rate of 99.91%. L. Hong [4] proposed fast fingerprint enhancement algorithm to improve goodness of fingerprint samples. This improved overall accuracy of biometric system by making use of enhanced fingerprint samples. S. Pankanti [5] in his research scientifically established that fingerprints of each individual are unique and distinct.

Palm print authentication systems have been proposed in literature. D. Zhang [6] proposed an online Palm print identification system with ability to process low-resolution Palm print images to achieve effective identification. This system provides FAR of 0.1% and GAR of 97%. J. You[7] proposed a new way to authenticate individuals based on Palm print biometric. A texture-based dynamic selection scheme was proposed that resulted in faster search. They showed that the accuracy of the proposed system was good in 200 test samples vis-à-vis other systems. A. K. Jain [8] presented algorithm to make use of latent palm prints for identification.

A. K. Jain [9] improved hand shape based verification system by pre-aligning hand shapes before extracting the feature set. A.K. Jain [10] proposed a prototype hand geometry based verification system that uses hand geometry as biometric identifier. Their system achieved GAR of 89.68% at FAR of 1.76%.

Chih-Lung Lin [11] proposed a new methodofauthentication making use of thermal images of vein patterns on the dorsal part of palm. They captured the thermal images of the palm-dorsa using IR camera. Their system achieved FRR of2.3% &FAR of 2.3%.

K. Nanda Kumar [12] in his research worked upon normalization and fusion rules using face, finger prints and hand-geometry modalities. GAR of 95% was achieved at FAR of 0.01%.Arun Kumar [13] has considered

dynamic security aspect in multimodal biometric systems. Dynamic security levels were controlled by the addition of cost of false acceptance (CFA) and cost of false rejection (CFR). L. Hong [14] proposed a bimodal system using fingerprint and face. They have fused the Eigen faces and the minutiae features from fingerprints at the decision-level to achieve FRR of 6.6% and FAR of 0.01% in comparison to FRR of 61.2% for face and 10.6% for fingerprint at the same FAR. Frischholz[15] have presented probably the first commercial system BioID using lip movement and face images extracted from the same video sequence. The table 1 summarizes prior works done in the field of hand based biometrics.

Table 1: Summary of prior work

Researcher	Biometric Modalities	Results
Y. Ding, D. Zhuang et al [22]	Unimodal (Hand veins)	Pass rate : 99.1%
Ajay Kumar, Yingbo Zhou [23]	Unimodal (Finger Knuckles)	Pass rate : 98.6% EER : 1.14%
L. Hong and A. K. Jain [14]	Bimodal (Fingerprints and face)	FAR : 0.01% FRR : 6.6%
R. Frischholz and U. Dieckmann [15]	BioID (Face, Voice and Lips)	EER < 1%
J. Fierrez-Aguilar et al [16]	Multimodal (Fingerprint, Face and Signature)	EER : 0.005%
A. Kumar, D. C. M. Wong et al [17]	Bimodal (palmprint and hand geometry)	FAR :0% FRR : 1.41%
Arun Ross, Anil Jain [18]	Multimodal (fingerprint, hand geometry and	FAR : 0.03% FRR : 1.78%
A. K. Jain, K. Nandakumar et al [19]	Multimodal (fingerprint, hand geometry and	FAR : 0.1% FRR : 1.4%
Kalyan Veeramachaneni et al [20]	Adaptive multimodal (Face, voice and Hand geometry)	FAR : 0.0029 FRR : 0.07
Ajay Kumar, Vivek Kanhangad et al [21]	Adaptive multimodal (Palm print, Iris, fingerprint, hand geometry)	Better Fused results

B. Motivations

Biometric modalities based security features are increasingly being added in smartphones to address security concerns of the mobile users [24-26].Fingerprints as well as palm prints, both are touch based. In smartphones due to limited size, fingerprint scanning sensors are very small. Thus these fingerprint sensors are not able to capture full biometric information of the fingers. Therefore, these systems are weakened due to smaller sensor

size available on smartphones. Moreover, the biometric information of more than one finger can't be taken at a time, thus making it cumbersome to collect biometric information of all the fingers of one subject. Palm prints scanning need specialised sensors to capture useful biometric information from the palm. Due to large size of palms, palm scanners are also large in size, which makes these sensors unsuitable for miniaturisation and embedding in to smartphones.

Hand veins and finger veins are other hand based biometric modalities. However, to capture these biometric modalities, specialised IR/thermal sensors are needed. Due to size and weight, these sensors cannot be inbuilt in smartphones. These sensors need to be attached to smartphones externally. This process becomes inconvenient and at the same time adds to the overall cost of the system.

Therefore, we propose in this work a novel hand based biometric modality, called fistprint, which is non-touch based and does not need any specialised sensors for working. Smartphone camera is sufficient to capture fistprint information.

C. Contributions

In this work, our contributions are:

i) We propose a new non-touch, non-invasive hand based biometric modality called fistprint. Fistprint contains many distinctive elements such as fist shape, fist size, fingers shape and size, knuckles, finger nails, palm crease/wrinkle lines etc. Fistprint could be used to uniquely identify individuals.

ii) Since fistprint biometric modality is being proposed for the first time, there is no DB available. We collected fistprint information of twenty individuals - both males and females aged from 23 years to 45 years of age. Four images of each hand fist (total 160 images) were taken for this purpose.

iii) We present an online automatic authentication system using fistprint biometric called Fistprint Automatic Authentication SysTem(FAAST).

iv) We Implemented FAAST system on Samsung Galaxy smartphone running Android and server side on a windows machine and validated the new biometric modality as well as the performance of the automated system.

III. FISTPRINT

Human fist can be formed in multiple ways. For the purpose of capturing fistprint data, the fist is formed by curling the fingers towards palm, exposing knuckles on the dorsal part of hand. The thumb is extended and touches fingers. Forming fist in this fashion exposes finger knuckle patterns, palm crease and wrinkles, nails, fingers (shape and size). The combination of all these elements is termed as fistprint. Fistprint contains large amount of distinctive information and can be used to authenticate individuals. Figure 4 shows fistprints of two individuals (left and right fists). Figure 5 shows fistprint with distinctive elements.

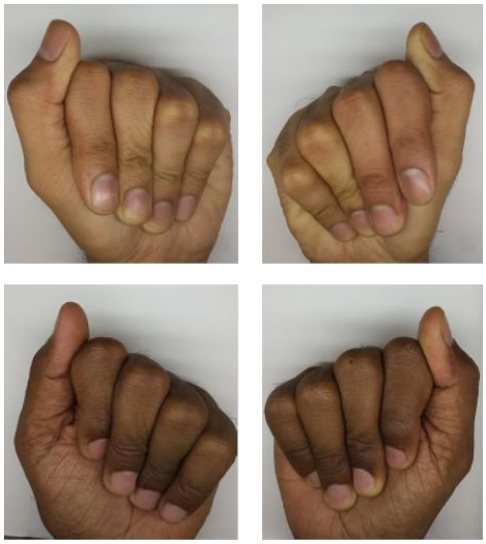


Fig 4: Fistprint Images of two Individuals

(Taken with Samsung Galaxy Note 3 Camera)

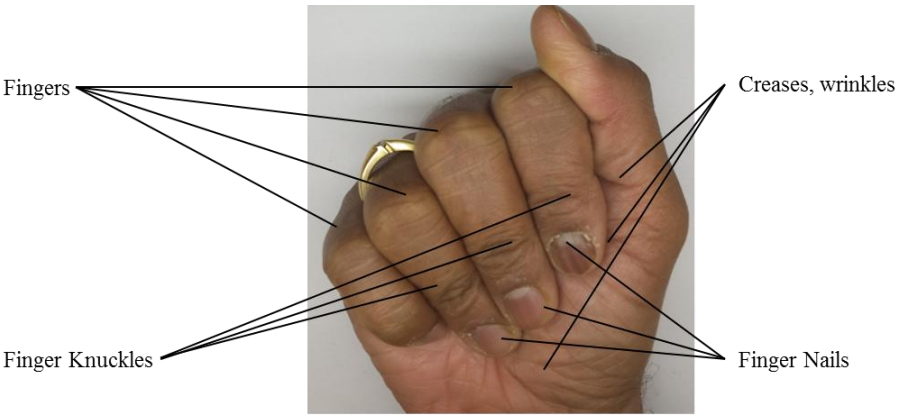


Fig 5: Distinctive features of Fistprint

We propose that fistprint could be suitable biometric. It complies with the following criteria [2]:

- *Universality*: Hands are universal, so are the human fists. Even if fingers of one hand are damaged, fistprint can be taken from other hand. Fistprint identification is also possible even with some damaged fingers.
- *Distinctiveness*: Dorsal parts of fingers and palm, which are used in fistprints, have many lines, wrinkles, texture, shape and size. All these elements make fistprint to be unique to each individual.
- *Permanence*: Growth of human hand stops by the end of teen years. Therefore, fistprints are permanent unless subject goes through some mishap.
- *Circumvention*: As the fistprint is a combination of multiple elements, it is nearly impossible to spoof fistprints.
- *Collectability*: Fistprints can be captured in a non-invasive fashion with a normal camera available in any smartphone. No special sensors are needed for capturing fistprints.
- *Acceptability*: For providing fistprints, the subject is not required to touch any surface. This touchless property of fistprint makes it more non-intrusive. It increases the acceptance of fistprints.
- *Performance*: Due to high amount of distinctive elements, the performance of fistprint based system will be high. We will further corroborate this with experimental test results provided in upcoming sections.

IV. IMAGES ACQUISITION AND PROCESSING

A. Image Acquisition

Fistprint biometric information was acquired with smartphone rear camera. For the purpose of experiment, a total number of 20 persons from various age groups were selected randomly. Along with fistprints, while registering their name and age relatedinformationwere also gathered.

For each candidate, four images of left fist and four images of right fist were collected.Thus a total of 160 images were captured and stored in the data base. All the images were not captured in one sitting; rather these were captured at different points in time. Each image was given a unique filename so that it could be easily identified later for analysis purposes.

B. Image Processing

The captured fistprint images are processed further. Below steps are used. Figure 6 depicts various steps used in image processing of fistprint images.

- *Image Alignment:*There is possibility that captured images could be misaligned. All the images are aligned in such a way that wrist part of the image is parallel to horizontal axis.
- *ROI Extraction:* In this step, fist part of the image is separated from rest of the image.
- *Binarization:* The image is converted to two colors – black and white.
- *Equalization:* Binarized image is processed through histogram equalization to adjust image intensities properly.
- *Filtering:* Equalized image is filtered using Gabor filter. This step helps in keeping features of interest like lines, wrinkles, knuckles, nails etc. in the final image. This serves as the template for classification.

Output of each stage of image processing is shown in figure 7.

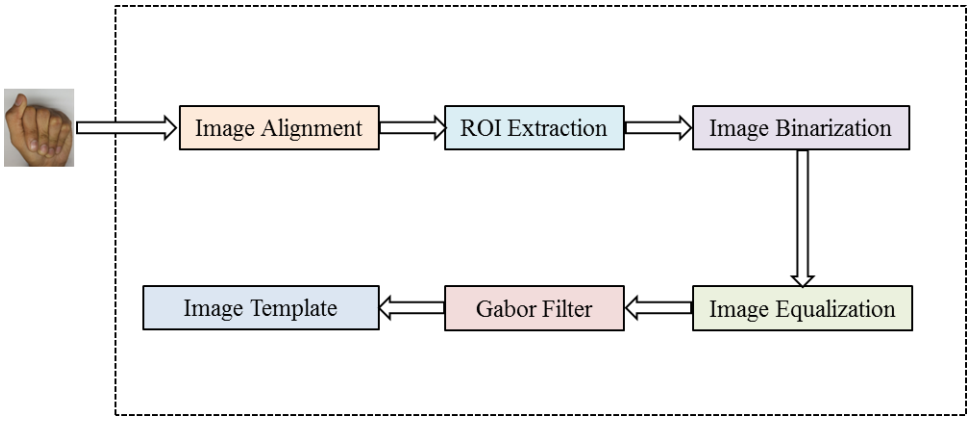


Fig 6: Fistprint Image Processing

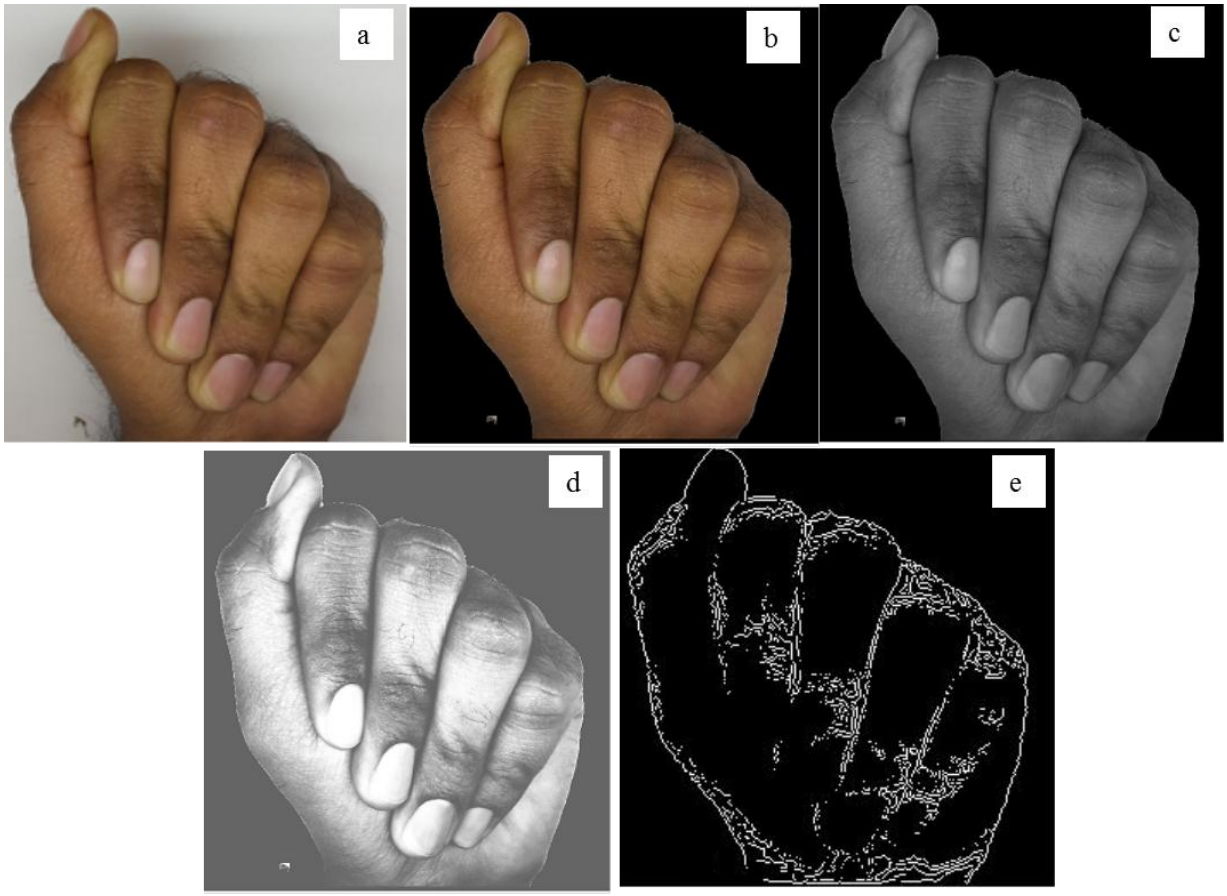


Fig 7: Fistprint Image Processing

(a: Original Image b: ROI Image c: Binarized Image

d: Intensity Equalized Image e: Filtered Image)

V. FISTPRINT AUTOMATIC AUTHENTICATION SYSTEM (FAAST) ARCHITECTURE

FAAST system is depicted in figure 8. The system has two parts – one running on Android [27] device and other running on Windows server. The main components are as follows:

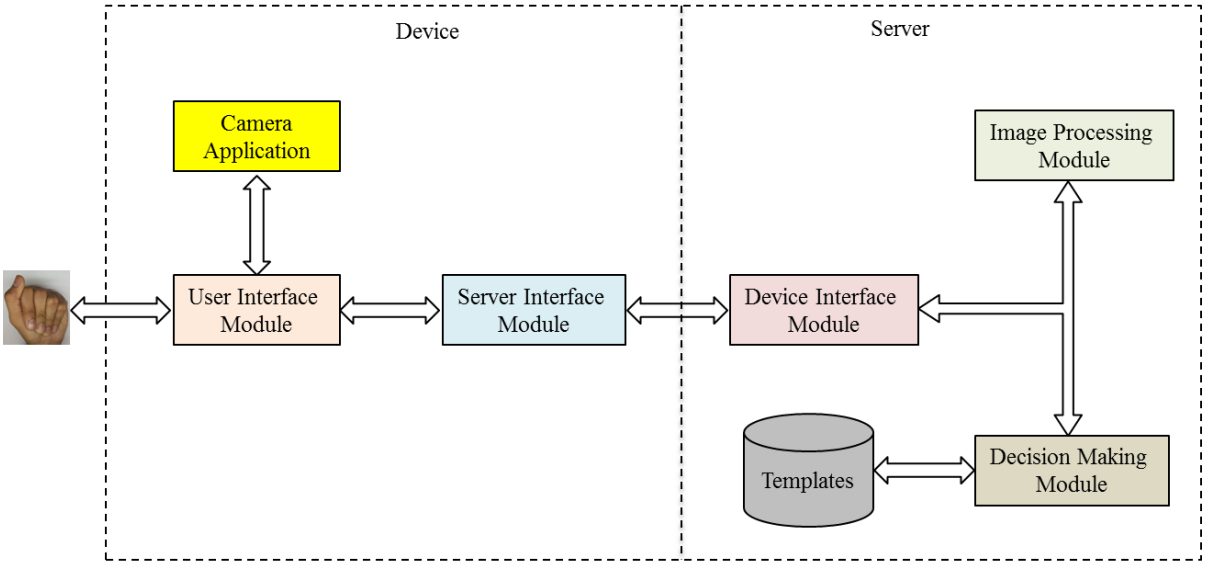


Fig8: FAAST Architecture

A. User Interface (UI) module

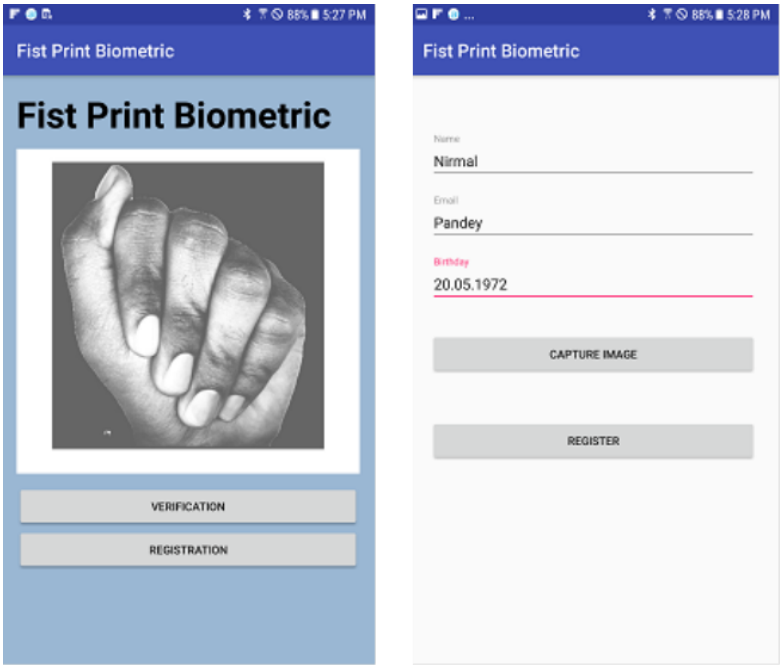
The purpose of User Interface module is to interact with the user of the smartphone. FAAST system operates in two modes – registrationmode and verification mode. The UI module provides UI forms where in user information needed for registration is keyed in during the registration phase. During the verification phase, UI module helps in capturing the fistprint image and displays the final decision of the system (Acceptance or rejection). The figure 9 below depicts actual UI of FAAST system on the device side.

B. Camera Application

Camera application captures the images of fistprint. During the registration as well as verification phase, UI module triggers camera app to capture the image.

C. Server Interface (SI) module

The Server Interface (SI) module on the device handles the full duplex communication between device and the server. It maintains a connection with the server. The captured image by camera app is sent to server over https secure connection.



(Fig9: GUI of FAAST System)

D. Device Interface (DI) module

The purpose of Device Interface (DI) module is to handle the communication between device and the server from the server perspective. It maintains a connection with the device. It receives captured images and registration related information from the device. The acceptance/rejection decision of the system is conveyed to the user from server via DI module. It is resident on the server.All communication between device and the Windows server is carried out using https protocol which adds additional layer of security to the contents being exchanged between device and server.

E. Image Processing Module

The Image Processing module does all the processing like alignment, ROI extraction, equalization and filtering. The filtered image along with registration or verification phase information is sent to Decision making module. This module resides on server.

F. Decision Making Module

During the registration phase, the decision making module stores fistprint templates and other user details in template DB. It also decides on the threshold for making genuine/impostor decisions. During verification phase, the received fistprint biometric information is compared with the stored template of the individual using normalized cross correlationmethod. Based on this value and threshold, genuine/impostor decision is taken and sent to user.

VI. EXPERIMENTAL RESULTS

Fistprint DB was created with 20 users by capturing 4 images each of their left as well as right fist. Thus it had a total of 160 images. So in way experiment was conducted on 40 users. Out of four images of fist belonging to each user, three were used as training images and fourth one was used as test image. For each user, the test image was compared with stored template of that individual and genuine score was calculated. Thus a total of 40 genuine scores were computed during the experiment. The normal distribution curve of the genuine scores is shown in figure 10 below. From the score distribution curve we can see that mean of the genuine scores is 0.11 and standard deviation from the mean is 0.02. Most of the scores lie between 0.09 and 0.13.

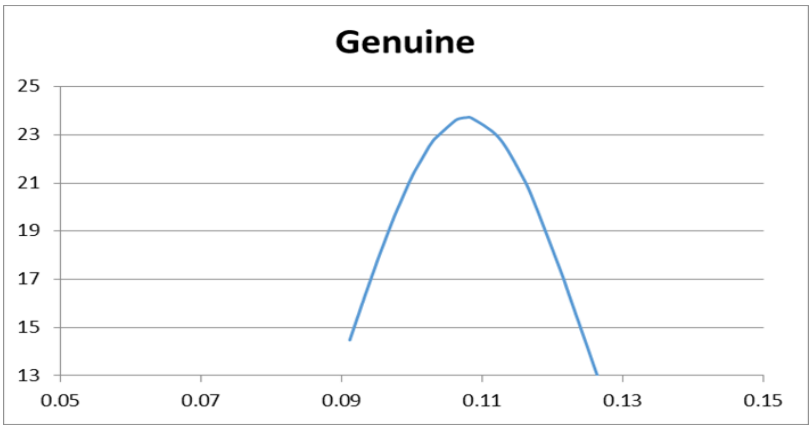


Fig 10: Genuine Scores Distribution

For computing impostor scores, the test image of the 40 registered individuals was compared with the stored templates of remaining 39 users. Thus a total of 40 * 39 = 1560 impostor scores were calculated. The figure 11 below depicts the distribution of impostor scores. From the normal distribution curve of impostor scores we can see that mean of the scores is 0.06 and standard deviation is 0.012. Most of the scores lie between 0.04 and 0.08.

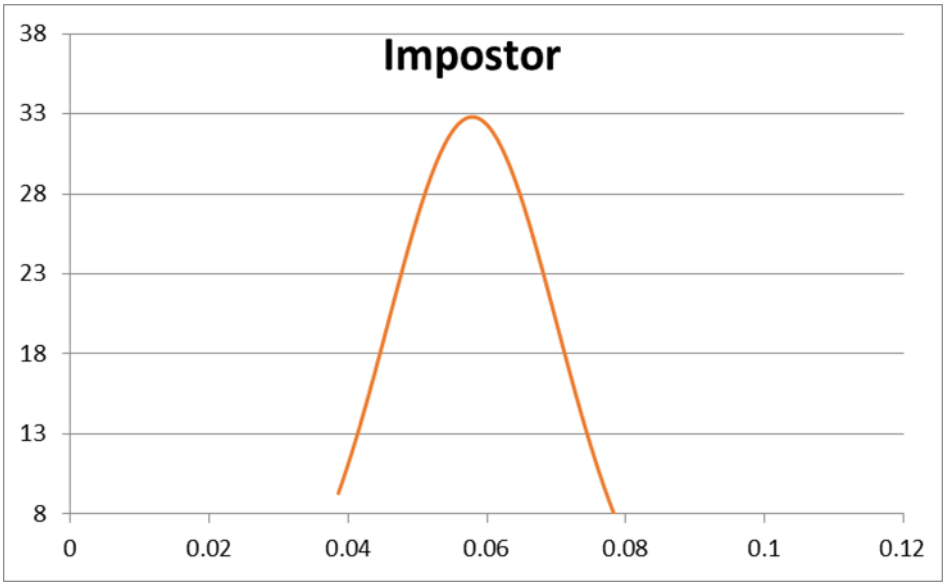


Fig 11: Impostor Scores Distribution

From the experimental data of 40 sets of fistprints, false acceptance rate (FAR) and false rejection rate (FRR) of fistprint biometric was calculated. FAR and FRR distribution of fistprint experiment are shown below.

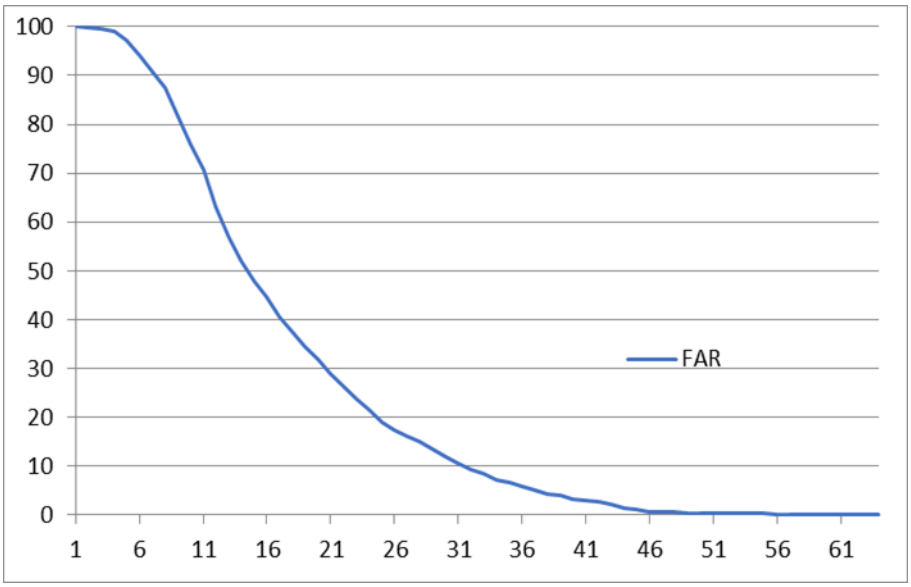


Fig 12: False Acceptance Rate (FAR)

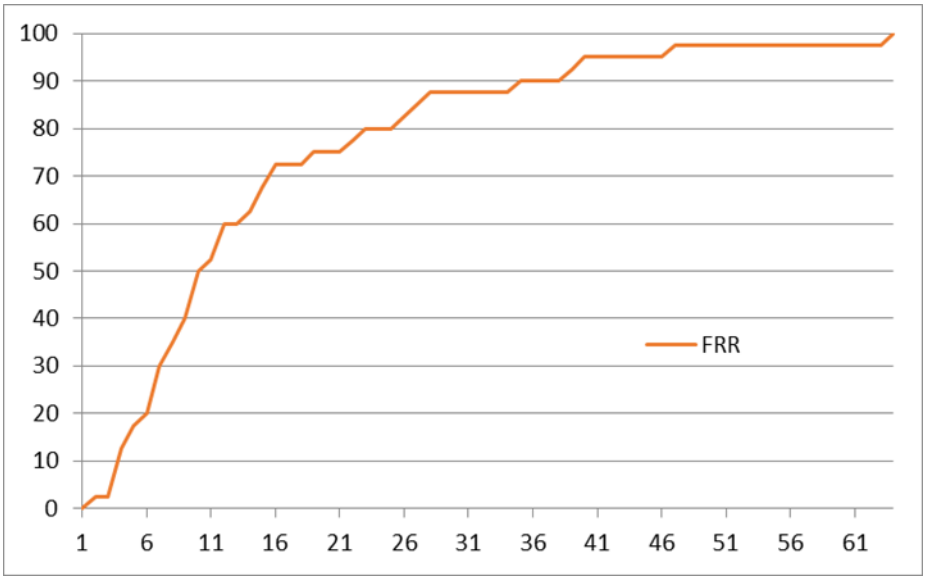


Fig 13: False Rejection Rate (FRR)

ROC curve for fistprint biometric modality is shown in figure 14 below. Fistprint biometric modality shows GAR of 97.5 % at 1.0% FAR and GAR of 87.5% at 0.6% FAR. These results experimentally validate the effectiveness of fistprint as a biometric modality.

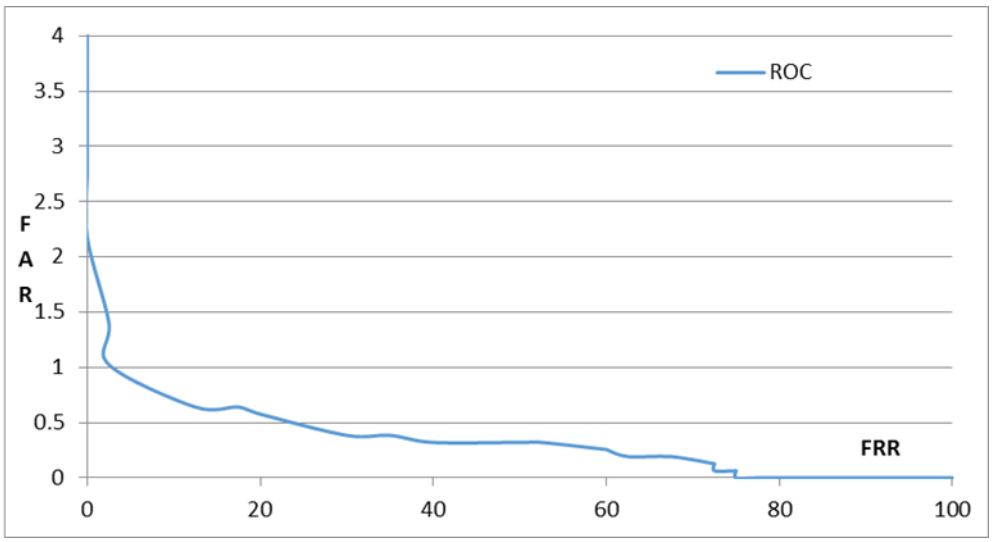


Fig 14: ROC Curve

VII. CONCLUSION AND FUTURE WORK

Security is one of the top concerns of smartphone users nowadays. Keeping user acceptability, non-intrusiveness, cost and performance in mind, we introduced a new hand based biometric modality called

Fistprint(Section III). Since this is a new biometric modality, there is no known fistprint DB available in literature. We collected fistprint information of 20 individuals - both males and females aged from 23 years to 45 years of age. Four images of each hand fist (total 160 images) were taken for this purpose (Section IV). Experimentally we have shown that fistprint as a biometric is successful with GAR of 97.5 % at 1.0% FAR (Section VI).

We also presented an online automatic authentication system using fistprint biometric modality, Fistprint Automatic Authentication SysTem (FAAST) (Section V). The client side of this system was implemented on Samsung Galaxy smartphone running Android and server side on a windows machine. FAAST system worked successfully in online mode.

REFERENCES

[1] A. K. Jain, R. Bolle, and S. Pankanti (Eds), "BIOMETRICS: Personal Identification in Networked Society," *Kluwer Academic Publishers*, 1999.

[2] A.K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[3] A.K. Jain, L. Hong and R. Bolle, "On-line Fingerprint Verification", *IEEE Transactions on PAMI*, Vol. 19, No. 4, pp. 302-314, 1997.

[4] L. Hong, Y. Wan and A.K. Jain, "Fingerprint Image Enhancement: Algorithms and Performance Evaluation", *IEEE Transactions on PAMI* , Vol. 20, No. 8, pp.777-789, August 1998.

[5] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the Individuality of Fingerprints", *IEEE Transactions on PAMI*, Vol. 24, No. 8, pp. 1010-1025, 2002.

[6] D. Zhang, W. K. Kong, J. You, and M. Wong, "Online palmprint identification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 9, pp. 1041–1050, Sep. 2003.

[7] J. You, W. Li, and D. Zhang, "Hierarchical palmprint identification via multiple feature extraction," *Pattern Recognition*, vol. 35, pp. 847-859, 2002.

[8] A. K. Jain and J. Feng, "Latent Palmprint Matching", *IEEE Trans. PAMI* vol. 31, no. 6, pp. 1032-1047, June, 2009.

[9] A. K. Jain and N. Duta, "Deformable matching of hand shapes for verification", *Proc. IEEE International Conference on Image Processing*, October 25-28, Kobe, Japan, 1999.

[10] A.K. Jain, A. Ross and S. Pankanti,"A Prototype Hand Geometry-based Verification System", *2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication (AVBPA)*, Washington D.C., pp. 166-171, March 22-24, 1999.

[11] Chih-Lung Lin, and Kuo-Chin Fan, "Biometric verification using thermal images of palm-dorsa vein patterns", *IEEE transactions on circuits and systems for video technology*, Vol. 14, pp. 199-213, 2004.

[12] K. Nandakumar, "Multibiometric Systems : Fusion strategies and Template Security", *PhD thesis*, Department of Computer Science & Engineering, Michigan State University, East Lansing, USA, 2008.

[13] A. Kumar et al., "Dynamic security management in multi-biometrics," *in Multibiometrics for Human Identification* Eds. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[14] L. Hong and A. K. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, no. 12, pp. 1295–1307, Dec. 1998.

[15] R. Frischholz and U. Dieckmann, "BiolD: A multimodal biometric identification system," *Computer*, vol. 33, no. 2, pp. 64–68, Feb. 2000.

[16] J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, and J. Gonzalez-Rodriguez, "A comparative evaluation of fusion strategies for multimodal biometric verification," in *Proc. 4th Int. Conf. Audio-Video-Based Biometric Person Authentication*, J. Kittler and M. Nixon, Eds., 2003, vol. LNCS 2688, pp. 830–837.

[17] A. Kumar, D. C. M. Wong, H. C.Shen1, and A. K. Jain, "Personal verification using palmprint and hand geometry biometric," in *Proc. 4th Int.Conf. Audio- Video-Based Biometric Person Authentication*, J. Kittler and M. Nixon, Eds., 2003, vol. LNCS 2668, pp. 668–678.

[18] Arun Ross, Anil Jain, "Information Fusion in Biometrics", *Pattern Recognition Letters*, vol. 24 pp. 2115–2125, 2003.

[19] A. K. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern Recognition.*, vol. 38, no. 12, pp. 2270–2285, 2005.

[20] Kalyan Veeramachaneni, Lisa Ann Osadciw, and Pramod K. Varshney, "An Adaptive Multimodal Biometric Management Algorithm", *IEEE Trans. On Systems, Man, and Cybernetics—Part C: Applications and Reviews*, vol. 35, no. 3, August 2005.

[21] Ajay Kumar, Vivek Kanhangad, and David Zhang, "A New Framework for Adaptive Multimodal Biometrics Management", *IEEE Trans. on Information Forensics and Security*, Vol. 5, no. 1, pp. 92-102, March 2010.

[22] Y. Ding, D. Zhuang and K. Wang, "A study of hand vein recognition method," *Proc. IEEE Intl. Conf. Mechatronics & Automation*, Niagara Falls, Canada, pp. 2106 – 2110, Jul. 2005.

[23] Ajay Kumar, Yingbo Zhou, "Personal Identification using Finger Knuckle Orientation Features", *Electronics Letters*, vol. 45, no. 20, September 2009.

[24] Deloitte Global Mobile Consumer Survey2015, available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-global-mobile-executive-summary-2015.pdf

[25] Samsung Galaxy Note 7 with inbuilt Iris scanner. https://news.samsung.com/global/everything-you-need-to-know-about-the-galaxy-note7s-iris-scanner

[26] Apple Introduces fingerprint in iPhones 5S http://www.apple.com/in/pr/library/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World.htmlIf

[27] Google Android Developer Information available at: https://developer.android.com/index.html