[1]Shiva Prasad M S

[2]Ganga Shirisha M S

[3]B Bhaskar Rao

[4]Sanjeevkumar Chetti

[5]Chandrakant Naikodi

A Novel Approach to Integrate Palmprint Recognition and Sequence of Multiple Fingerprints to Authenticate Smartphone

Abstract: - As biometric recognition technologies are accurate and most efficient, they are considered to be essential factorin enhancing security in a variety of smart devices.Fingerprintand palmprint recognition are two of the most prominent biometric procedures by considering its distinctive and reliable properties. This paper proposes a hybrid approach that combines the palmprint and sequence of fingerprint recognition technique to improve accuracy and robustness. We have calculated FAR and FRR values and also computed True Positive and False Positive rates. Accuracy is calculated and consolidated on both of the recognition techniques for different users. Probability of false acceptance and false rejections are computed to find the combinational accuracy of an integrated system. The proposed method shows the encourageable results and hence considered to be one of the best robust security techniques.

Keywords: Palmprint Recognition, Sequence of Multiple Fingerprints, False Accept, False Reject, True Positive, False Positive.

1. Introduction

Biometric based authentication techniques have become increasingly popular because they are both convenient and reasonably secure [1]. Presently fingerprint recognition is widely used due to its usability and ease of access in terms of providing better security [2]. Similar to fingerprint, palmprint also encompass permanent distinguishing characteristics such as high-resolution pores, minutiae points, principal lines and ridge-and-valley patterns [3]. Presently some of the smart device uses fingerprint and palm recognition techniques individually to authenticate the system however if they are used collectively with existing methods it can have various unresolved security problems because there are moreways to capture individual features superstitiously, there is a need to further enhance existing technique.

Fingerprint is recognizedusing four stages: Fingerprint sensing, Feature extraction, Image pattern matching, and Decision making [5]. Fingerprint recognition can be classified into loop, whorl, arch and minutiae points that identifies the uniqueness of an individual [6] however palmprint have several advantages over fingerprint including the ability to recover additional details like main principal lines and wrinkles from images with slightly lower resolution palmprint identification has gained popularity in recent years. Since palmprints include more information than fingerprints do, they can be utilized to create biometric systems that are even more accurate [7]. Palmprint recognition is a biometric technology that identifies individuals based on the unique patterns present on their palms through several steps shown in Fig.1. To begin with, a picture of the palm must be captured. Several kinds of image tools such as cameras, scanners, and specialized palm scanners, can be used for this. Preprocessing is to enhance the quality of the image acquired and makes it suitable for further analysis.

[1] [#1,2]Research Scholar, Department of Studies in Computer Science, Davangere University- 577007 India

[#3]Research Scholar, Cambridge Institute of Technology, Bengaluru-560036

[#4]Principal Director, Ministry of MSME, Government of India, Mumbai, Maharashtra, India

[#5]Professor and Chairman, Department of Studies in Computer Science, Davangere University, Davangere-577007.

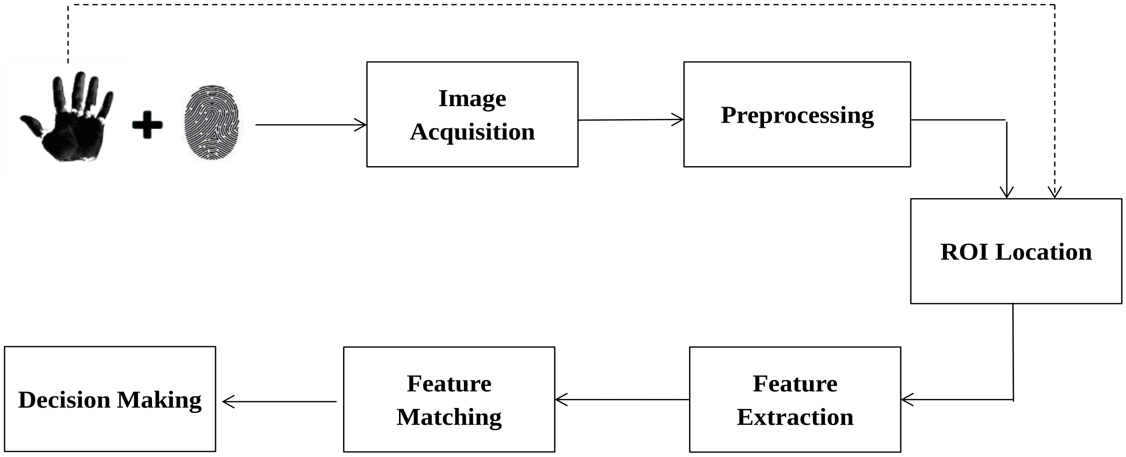


Fig.1. Palmprint and Fingerprint Recognition Process

ROI (Region of Interest) is to locate the precise region of the palm image that has the necessary data for analysis, such as the ridges, lines, and other distinguishing characteristics for identification. Feature extraction gathers all the relevant features from finger and palm, feature matching compares previous templates and decision is made whether finger and palmprint matches with its previous stored features. According to the proposal of this paper every user can register a maximum of 2 palms (left and right) and 10 fingerprints in sequence.

The primary idea is to register multiple fingerprints of a user and to authenticate registered fingerprints in a sequence during validation. The sequence follows the order in which the user register their fingers as shown in Fig.2.

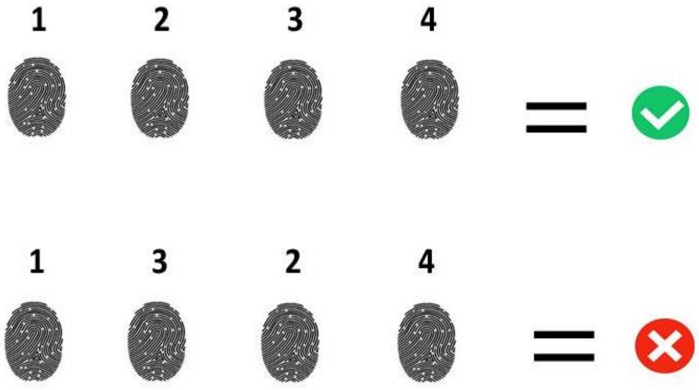


Fig.2. Sequence of Fingerprint Authentication

Each finger is assigned with an unique id value, during the authentication process the user has to provide the same sequence of fingers, supposethe registered order is 1, 2, 3, and 4 then users must authenticate with same sequence of fingers. If any one sequence is missed or placed a wrong finger then authentication will fail as shown in Fig.2. Secondly, in addition to this we are proposing yet another model of palmprint recognition which will be integrated with SMF. Both the palms of a user (left and right) can be registered by assigning palm id i.e. *palm1* and *palm2* and these palms can be placed before or after the SMF authentication system as shown in Fig.3. The testing has been carried out with the palmprint and SMF authentication separately and analyzed the test cases on FAR and FRR for both authentications and found that efficiency is improved significantly.

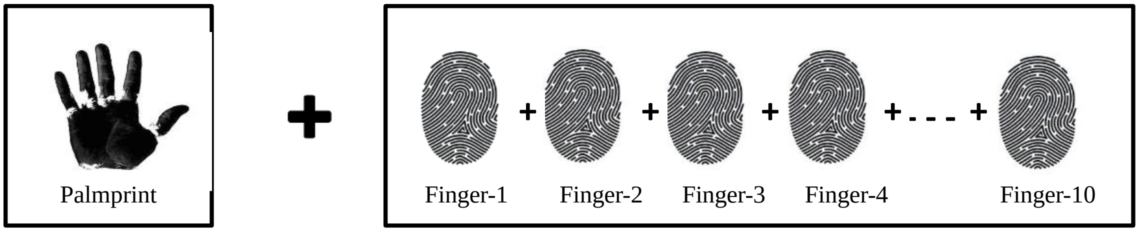


Fig.3. Palmprint and SMF Authentication System

We are presenting an approach that combine Palmprint Recognition (PPR) and Sequence of Multiple Fingerprints (SMF) authentication system [4].Thus by integrating the combined authentication system on any smart device can increase the robustness and security of the system by reducing the chance of brute-force, template, impersonation and several other attacks etc.

2. Literature Review

As part of the literature review, tried to provide all the latest developments and their corresponding future trends, Table 1 highlights the contributions of the different authors.

Sl.no	Reference Paper	Contribution/s	Future Enhancements
1	Shiva Prasad MS et al. [4]	The sequence of Multiple fingerprints creates a robust authentication environment for smartphones.	It can be enhanced with other authentication techniques.
2	Dev.Nath et al. [8]	False Accept Rate (FAR) and False Reject Rate (FRR) are more in single fingerprint authentication that need to be minimized.	The error rates occur quite often and have to be reduced.
3	ZahidAkhtar et al. [12]	Touchstroke, phonemovement,and face patterns can be used for smartphone authentication.	Implicit smartphone Multimodal biometric systems using touch stroke can be implemented on any smartphone.
4	Priesnitz et al [13]	Touch less biometric recognition represents a rapidly growing field of research.	Touches less schemes reveal improved usability and high user acceptance whereas biometric performance remains as challenge.
5	Balakrishnan, S. K et al. [14]	Palmprint recognition can be a promising biometric authentication for any smart system.	Research on palmprint is increasing due to its reliable, stable, distinctive, low cost characteristics.
6	Priesnitz et al. [15]	Our work focuses on contactless biometric authentication system for smartphones.	Contactless scheme performs better than contact based scheme and it can be integrated to smartphone.
7	Adrian-Stefan Ungureanu et al. [16]	Palmprints are under-utilized when compared to other biometrics.	Palmprint cover much larger surface than fingerprint so it will be more robust.

8	Shiva Prasad MS et al. [17]	The accuracy of the SMMF probability on FAR and FRR was 98.13% and 82%, respectively.	SMMF can be integrated to other applications to enhance security as it is simple to program.
9	Poonia et al.[18]	The proposed template is invariant to rotation, translation and distortion.	The performance of the proposed method can be enhanced by fusing the fingerprint and palm print features.
10	Zhao et al. [20]	The palmprint recognition performance will be degraded by the interference factors, i.e., noise, rotations, and shadows.	Multi view palmprint feature learning has been proposed to enhance the feature expression by exploiting multiple characteristics from diverse views.

Table 1: Literature Review

3. Methods and Experiments

Palmprint recognition with smartphone camera has been used to identify ridges, minutiae points and principal lines. An user must register his palm using mobile application [8] to start the authentication process and once the palm is registered, it stores all the palm features in the form of an image and palm can be recognized even with the low-resolution image [2] [3] to get a high resolution images of a palmnew methods need to be used [10]. As we have conducted an experiment on the palmprint recognition model, even at resolution we got good accuracy level. Fig.5 shows palmprint registration and authentication process.

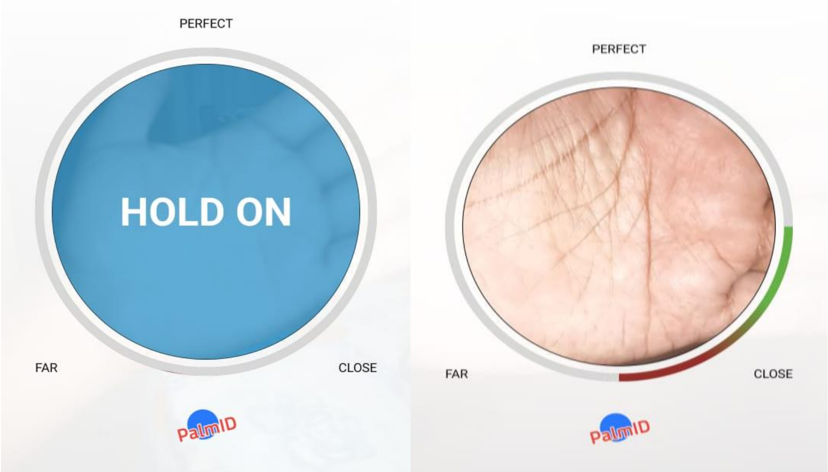


Fig.5 Palmprint Registration and Authentication Process

Palm registration process includes image acquisition, preprocessing and feature extraction. Here image acquisition captures the image of a palm through camera and once the image is captured it is preprocessed to enhance the quality of an image by noise reduction and segmentation to isolate the region of a palm. Distinctive features are extracted from a palm such as ridges, lines, wrinkles and minutiae points. Palm authentication process involves feature representation, comparison or enrollment, matching and decision. Feature representation converts the extracted data suitable for matching and decision process. In comparison and enrollment process, stored templates are compared to identify similarities between the features and for further comparison matching algorithms are used to decide whether the palmprint features are valid or not valid [1] [2] [3] [8] [10]. Palmprint recognition flow process is illustrated in Fig.6.

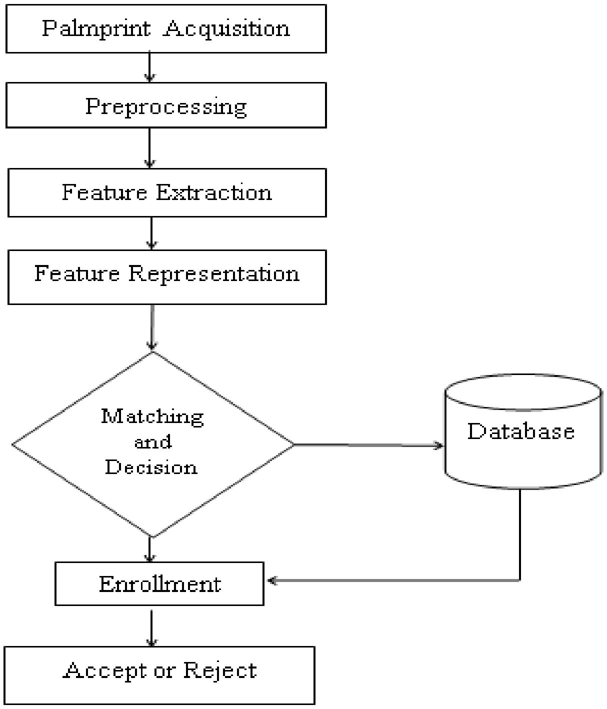
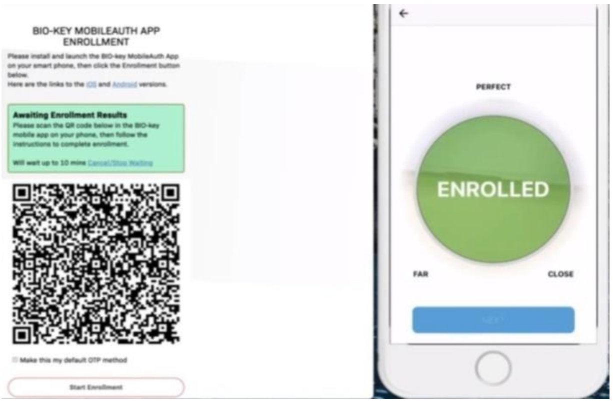


Fig.6 Palmprint Recognition Process

The model has two-step enrollment process, to authenticate the system user must provide login credentials such as username and password on the webpage created, once the login credentials are valid then it notifies the user to scan registered palm using mobile application. Once the user registers login credentials the user needs to register the palm using mobile application that links with webpage through QR code scan as shown in Fig.7.


BIO-KEY MOBILEAUTH APP ENROLLMENT

Please install and launch the BIO-key MobileAuth App on your smart phone, then click the Enrollment button below.
Here are the links to the iOS and Android versions.

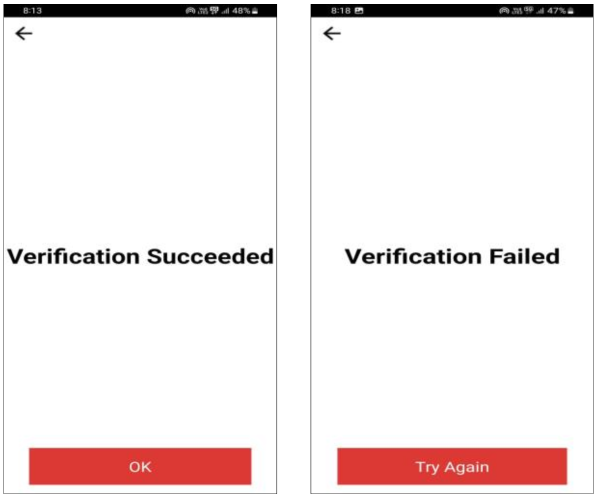
Awaiting Enrollment Results
Please scan the QR code below in the BIO-key mobile app on your phone, then follow the instructions to complete enrollment.

Will wait up to 10 mins Cancel/Stop Waiting

□ Make this my default OTP method

Fig.7 Palmprint Enrollment Process

Once the enrollment process completes, the user must login using two-factor authentication process that includes username-password and the palmprint authentication and the same process is shown in Fig.8.



Verification Succeeded

Verification Failed

Fig.8 Authentication Results

The simulation was designed to sequence the fingerprints using fingerprint sensor and the mobile application was used to recognize the palmprint of a user [8]. The same models were utilized for conducting experiments and analysis. The fingerprint sensing device was able to distinguish multiple fingerprints of a user, at first user needs to register the fingers in the sequence order using the control buttons provided on a device as shown in the Fig.4 and OLED display has set to show the Unique ID (UID) assigned for each finger. The device is capable of storing 127 distinct fingerprints in its memory [9], proposed method requires maximum of 10 fingerprints of a user.

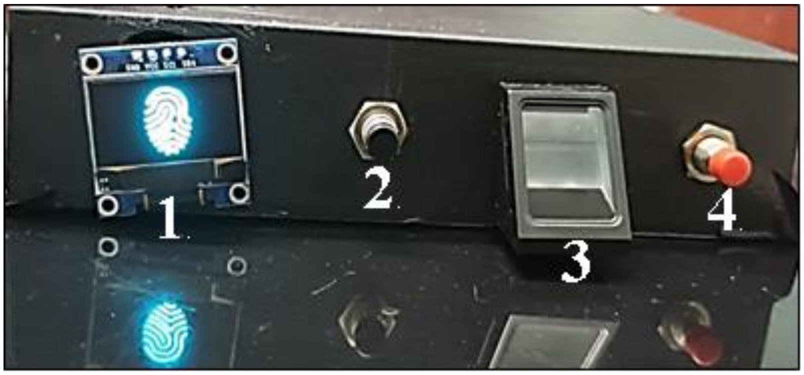


Fig.4. Fingerprint Sensor

Markings of the device as follows: 1.OLED display, 2. Button to increment/decrement ID value, 3.Fingerprint sensor, 3.Button to store the ID value on device. While authenticating, user scans his fingers in the order in which he has registered, while each finger is scanned its corresponding UID is displayed. After scanning all the registered fingers in the sequence and if all the scanned sequential fingerprints are recognized as valid then authentication will be success. The algorithm for SMF is described in Algorithm.

Algorithm: Sequence of Multiple Fingerprints

```
Input: Accept Fingerprints in Sequence
Output: Login Success or Login Failed
1: Initialize a=0,b=0,c=0,d=0
2: if (sequence1 = = template1) #verifying first sequence id
3: then a= a+1
4: else go toStep 19
5: if (sequenc2 = = template2) #verifying second sequence id
```

```
6: then b= b+1
7: else go toStep 19
8: if (sequence3 = = template3) #verifying third sequence id
9: then c=c+1
10: else go toStep 19
11: if(sequence4 = = template4) #verifying fourth sequence id
12: then d=d+1
13: if (d = = 1)
14: convert integer uid to string # as “1”, “2”, “3”, and “4”
15: concatenate uid #ex.”1234”
16: if uid.string = = temp_id.string
17: print “Verification successful”
        Else
18: print “Verification failed”
19: repeat steps 1 to 16 for other sequences if exist
20: end if
```

As both the methodologies are designed and implemented individually, we are proposing a model to integrate both palmprint recognition and SMF authentication system to build a highly robust environment to reduce the possible attacks on individual systems. The Fig.5 shows a proposed integration flow structure of palmprint recognition and SMF authentication system.

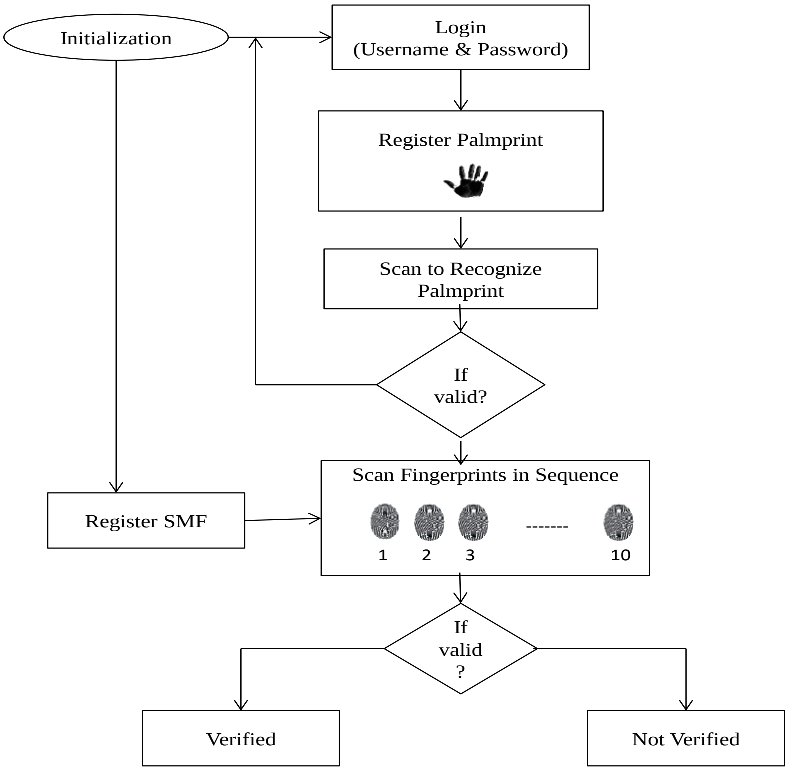


Fig.5 Palmprint Recognition and SMF Authentication

The False Acceptance Rate (FAR) and False Rejection Rate (FRR) for palmprint recognition and fingerprint sequences were extracted as the experiment was carried out separately on palmprint and SMF authentication on the two models. Equations Eq.1 and Eq.2 were used to compute FAR and FRR rates.

$$\text{False Acceptance Rate} = \text{Number of False Accepted} / \text{Total Samples} \quad (1)$$

False Rejection Rate = Number of False Rejected / Total Samples (2)

At first sequence of fingerprints are scanned from 10 different unregistered users, false accepted readings are noted to compute FAR and sequence of fingerprints are scanned from registered user for 10 consecutive times to compute false rejections and readings of computed FAR and FRR rates are provided in Table.2. For the second phase palmprint recognition application was used to compute FRR and FAR. We scanned 5 unregistered users palm to note false acceptance readings and carried the palm scan for 5 times repeatedly on registered user and the readings are recorded in Table.2.

	Palmprint Recognition	**Fingerprint Sequence**			
UID	1	2	3	4	5
FAR	0	0.3	0.2	0.1	0.1
FRR	0.2	0.2	0.4	0.3	0.2

Table 2.Readings obtained from Palmprint and Fingerprint Sequence

ROC (Receiver Operating Characteristic) curve is plotted by computing True Positive Rate (TPR) and False Positive Rate (FPR) refer Eq.3 and Eq.4 with different threshold values at each level of iteration as ROC points are plotted each time True Positive and False Positive values are incremented depending on predicted and actual parameters as on Fig.6. We have examined the authentication process for five days for ten distinct users, recording the true and false rates that are displayed in the table. Based on these data, the accuracy of both authentication models is calculated using four parameters: (True Positive) TP, (True Negative) TN, (False Positive) FP and (False Negative) FN. Fig.7 illustrate how accuracy was shown to increase as users authenticated to the model. Eq.5 is used to calculate the accuracy.

TPR = Total Positive / Number of Positive outcomes (3)

FPR = Total Negative / Number of Negative outcomes (4)

$$Accuracy = \frac{\sum TP + \sum TN}{\sum TP + \sum TN + \sum FP + \sum FN} \quad (5)$$

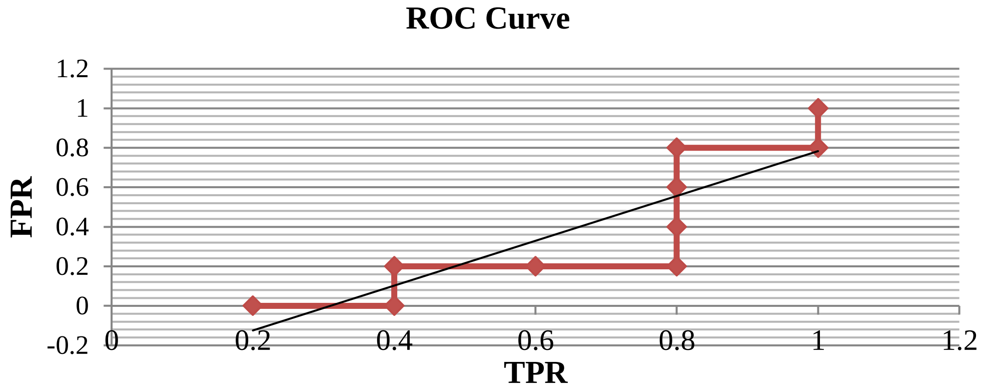


Fig.6 ROC Curve on TPR and FPR values

After analyzing the authentication process for five days for ten distinct users and recording the true and false rates presented in Table.3, the correctness of the authentication model is calculated based on parameters TP, TN, FP, and FN. Accuracy was seen to increase as individuals verified their identity with the model, as seen in Fig.7. The equation Eq.5 is used to calculate the accuracy.

Days	TP	TN	FP	FN	Accuracy (%)
Day 1	09	07	06	2	66.6
Day 2	15	14	05	2	80.55
Day 3	18	11	04	2	82.8
Day 4	22	15	02	1	92.5
Day 5	23	19	01	1	95.45

Table.3 Accuracy of Palmprint and SMF Authentication

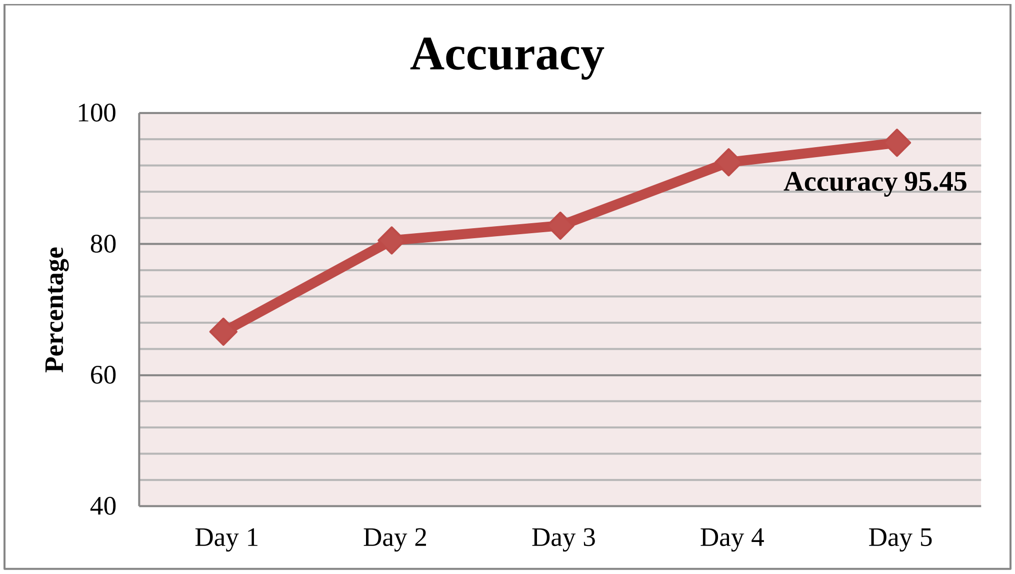


Fig.8 Accuracy of Combined Authentication Model

Equations 6 and 7 can be used to determine the likelihood of FAR and FRR. Combinations denoted as C (n, k) are used to produce a probability solution, where 'n' represents the total number of unauthorized users and 'k' represents the number of users that were mistakenly admitted. The ratio of False Acceptance to misclassifications is known as FA. The likelihood of Correctly Rejecting unauthorized users is known as CR.

$$P(FAR) = \{C(n,k) * P\ (FA)^K * P(CR)^{n-k}\} \tag{6}$$

$$P(FRR) = \{C(n,k) * P\ (FR)^K * P(CA)^{n-k}\} \tag{7}$$

The probabilistic analysis was conducted on 10 different unauthorized users out of which we got 2 misclassifications of falsely accepted users i.e. n is 10 and k is 2. FAR value is calculated to be 0.0387 which means 3.87 % is the chance of the system accepting the unauthorized user as valid and we had 3 misclassification of falsely rejected user i.e. n is 10 and k is 3. FRR value is calculated to be 0.516 which means 5.1% is the chance of the system rejecting the authorized user as invalid during the palmprint recognition process.

4. Conclusion

The integration of palmprint recognition with a sequence of fingerprint recognition presents a promising advancement in biometric security systems. The result of hybrid authentication system provides us better robustness and security as presented in experiments conducted on both the models individually and after accessing results, the paper concludes that integrated system is robust and secure with better accuracy rate of 95.45% as the system is authenticated and probabilistic solution shows 96.13% accuracy on FAR and 94.9% accuracy on FRR findings.

References

[1] Liang, Xu, et al. "Innovative contactless palmprint recognition system based on dual-camera alignment." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 52.10 (2022): 6464-6476.

[2] Young-HooJo., Seong-Yun Jeon., Jong-HyukIm., Mun-Kyu Lee. (2016). Security Analysis and Improvement of Fingerprint Authentication for Smartphones.

[3] Zhang, David, WangmengZuo, and FengYue. "A comparative study of palmprint recognition algorithms." *ACM computing surveys (CSUR)* 44.1 (2012): 1-37.

[4] Shiva Prasad MS.; Chandrakanth Naikodi. "A Novel Approach to Login Smartphones Using Sequence of Multiple Fingerprints for Secured Authentication". 2023. *Journal of Harbin Engineering University ISSN: 1006-7043.*

[5] Chen, Yu, and Yiling He. (2023) BRUTEPRINT: Expose Smartphone Fingerprint Authentication to Brute-force Attack. *arXiv preprint arXiv:2305.10791 (2023).*

[6] Jawarneh, Ibrahim, and NesreenAlsharman. "A mathematical model for arch fingerprint." *arXiv preprint arXiv:2003.00308* (2020).

[7] https://www.sciencedirect.com/topics/engineering/palmprint-recognition.

[8] Dev.Nath.;Saurav Ray.;Sumit Kumar Ghosh. Fingerprint Recognition System: Design & Analysis.2011

[9] https://info.bio-key.com/mobileauth

[10] Industries, Adafruit. Fingerprint Sensor. Fingerprint Sensor: ID 751: Adafruit Industries, Unique & Fun DIY Electronics, and Kits, www.adafruit.com/product/751.

[11] Lu, Guangming, David Zhang, and Kuanquan Wang. "Palmprint recognition using eigenpalms features." *Pattern Recognition Letters* 24.9-10 (2003): 1463-1467.

[12] Akhtar, Zahid, et al. "Multimodal smartphone user authentication using touchstroke, phone-movement and face patterns." *2017 IEEE global conference on signal and information processing (GlobalSIP)*. IEEE, 2017.

[13] Priesnitz, Jannis, et al. "An overview of touchless 2D fingerprint recognition." *EURASIP Journal on Image and Video Processing* 2021 (2021): 1-28.

[14] Balakrishnan, S., K. Venkatesan, and M. Syed ShahulHameed. "An embarking user friendly palmprint biometric recognition system with topnotch security." *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE, 2021.

[15] Priesnitz, Jannis, et al. "Mobile contactless fingerprint recognition: implementation, performance and usability aspects." *Sensors* 22.3 (2022): 792.

[16] Ungureanu, Adrian-Stefan, SaqibSalahuddin, and Peter Corcoran. "Toward unconstrained palmprint recognition on consumer devices: A literature review." *IEEE Access* 8 (2020): 86130-86148.

[17] Shiva Prasad MS.; Chandrakanth Naikodi. "A Novel Approach to Authenticate Smartphones Using Sequence of Multiple Multimedia Features for Robust Authentication". 2023. *Semiconductor Optoelectronics ISSN: 1001-5868.*

[18] Poonia, Poonam, Pawan K. Ajmera, and VijayendraShende. "Palmprint recognition using robust template matching." *Procedia Computer Science* 167 (2020): 727-736.

[19] Zhao, Shuping, LunkeFei, and Jie Wen. "Multiview-learning-based generic palmprint recognition: A literature review." *Mathematics* 11.5 (2023): 1261.