Detection of PARD Attack using Key based Biometric Authentication System and Fingerprint Impression

Lovelesh Khard
Computer Science and Engineering UIT, RGPV
Bhopal,India

Uday Chourasia
Assistant Professor, Depart. of CSE UIT, RGPV
Bhopal,India

Raju Baraskar
Assistant Professor, Depart. of CSE UIT, RGPV
Bhopal,India

ABSTRACT
Biometric verification assumes a noteworthy part in security as these are by nature interesting for each human. Be that as it may, the security is traded off when the example coordinating framework is not exact. Verification framework like unique finger impression acknowledgment is most ordinarily utilized biometric validation framework. In this paper overview is done on unique mark acknowledgment strategies. What's more, extraordinary methodologies are examined as far as precision and execution. As unique finger impression may likewise contain clamor; so picture de-noising systems are additionally concentrated Cross edge recurrence examination of finger impression pictures is performed by method for factual measures and weighted mean stage is ascertained. These distinctive components alongside edge unwavering quality or edge focus recurrence are given as contributions to a fluffy c-implies classifier.

Keywords
Component; formatting; style; styling; insert (key words)

1. INTRODUCTION
Fingerprint is the most interesting and oldest human identity used for recognition of individual. In the early twentieth century, fingerprint was formally accepted as valid signs of identity by law-enforcement agencies. On the basis of this the automatic fingerprint recognition system for authentication and identification ie Basically there are two types of fingerprint Recognition System AFAS (Automatic Fingerprint Authentication System), AFIS(Automatic Fingerprint Identification/Verification System) developed by the scientist and developers recently.

These framework simply utilized as a part of different application and frameworks where the confirmation and ID of person required, similar to Defense, law, wrongdoing, Banking, correspondence and so on. Unique finger impression acknowledgment framework depends on two essential premises Persistence: The fundamental attributes of unique finger impression don't change with time i.e. protect its qualities and shape structure birth to death, and Individuality, the finger impression is novel to a person. Image enhancement techniques are usually applied to remote sensing data to improve the appearance of an image for human visual analysis. Enhancement methods range from simple contrast stretch techniques to filtering and image transforms. Image enhancement techniques, although normally not required for automated analysis techniques, have regained a significant interest in recent years. Applications such as virtual environments or battlefield simulations require specific enhancement techniques to create ‘genuine living environments or to process images in near real time. Biometric systems are separated into two classes i.e. Physiological (fingerprints, face, iris, DNA, retina, voice, hand geometry, palm print, retinal output and so on.) and Behavioral (step, signature and so on). These physiological or behavioral Characteristics are utilized for human distinguishing proof on the premise of their comprehensiveness, uniqueness, lastingness and collection ability.

Most are known to possess distinctive, immutable fingerprints.

Figure 1 Secugen Hamster plus fingerprint Scanner

2. RELATED PREVIOUS WORK
Raju Rajkuma et al., 2011 [7] studied on directional filter, which describes the splitting of the input image into eight parts and rebuilding in to image after image enhancement.

Anush Sankaran et al.,2013 [8] defined as Clarity of a latent impression is characterized as the perceptibility of unique mark highlights while quality was characterized as the sum of features causal towards matching. Automated estimation of clarity and quality at local regions in a latent fingerprint is a study challenge and had received limited attention in the literature.

Daniel Peralta et al., 2015[9] Fingerprint recognition had found a reliable application for verification or identification of 32 people in biometrics. Worldwide, fingerprints can be viewed as respected traits due to several 33 perceptions observed by the experts; such as the distinctiveness and the permanence on 34 humans and the performance in real applications. Among the main stages of fingerprint 35 recognition, the automatic matching phase has established much attention from the early 36 years up to nowadays. This paper was devoted to review and categorize the vast number 37 of fingerprint matching methods proposed in the specialized literature. In particular, they 38 focus on local minutiae-based matching algorithms, which provide good performance with 39 an excellent trade-off between efficacy and efficiency.

Emanuela Marasco et al. 2014 [10] various issues identified with the presentation of unique mark acknowledgment frameworks to assaults had been high-lit in the biometrics true

to life. One such vulnerability involves the utilization of counterfeit fingers, where materials, for example, playdoh, silicone, and gel were designed with unique finger impression edges. Analysts had shown that some business unique mark acknowledgment frameworks can be misdirected when these simulated fingers are set on the sensor, i.e., the framework effectively forms the subsequent unique mark pictures in this manner concurring a foe to parody the fingerprints of aanother person. However, in the meantime, a few countermeasures that different between live fingerprints and parody antiques had been contemplated. While some of these hostile to ridiculing plans were equipment based, a few programming based methodologies had been proposed too. In this paper, they survey the works and present the cutting edge in unique mark hostile to caricaturing.

Rijo Jackson Tom et al., 2013 [11] aanalyses their association with gender of an individual using frequency domain technique and a pattern appreciation technique. The combined dispensation has provided better results. This paper aims in using 2D- Discrete Wavelet and Principal Component Analysis combined to classify gender using an obtained fingerprint.

Shahyar Karimi et.al., 2008 [12] existing as method for latent fingerprint image segmentation and enhancement was presented. In distinction with most state-of-the-art methods, our approach does not rely on the information of local gradients, which are sensitive to structured and formless background noise. Thus, the planned method was robust against gradient deviances. It also provides robust estimates to Orientations and frequencies of fingerprints in a local region to allow actual Gabor filtering for fingerprint ridge/valley pattern enhancement.

B.G. Sherlock et al., 1998 [13] method of improving fingerprint images was described, based upon non-stationary turning Fourier domain filtering. Fingerprints were first curved using a directional filter whose orientation was everywhere matched to the local ridge orientation. Thresholding then yields the enhanced image. Various popularizations lead to efficient application on general-purpose digital computers.

3. PROPOSED WORK

Our Research Methodology is purely laboratorial, where Researcher can experiment on fingerprint Image for enhancement that will provide us the quality image for recognition system. The enhancement process will work out as follows:

1) Physical Fingerprint required as input.

2) Input is processed by using various image processing tools and databases which is collected from various persons (The Fingerprint Verification Competition (FVC)2004 to 2007 fingerprint samples along with real samples will observe The basic fundamental steps of these systems are:

- Image acquisition
- Pre-processing segmentation
- Enhancement
- Feature extraction, matching along with classification through databases. Enhancement by the Help of Special Domain and Frequency Domain with different methods discussed in outline of study we will enhance the image for better quality.

3.1 Finger Print Sensing Technologies

Fingerprint sensor innovation has been being developed for a considerable length of time. Unique mark sensors come in different shapes and sizes, however for the most part fall into two classifications; territory output (or touch) sensor and swipe sensor. With a touch sensor, the client places and holds the finger on the sensor surface and impression exchanged from the stack of the last joint of finger or thumb. Touch sensors are utilized for the most part as a part of altered frameworks as a result of their size and shape [3]. These square-formed touch sensors are physically bigger (in stature and width) than swipe sensors and are utilized for instance, in migration access control applications. With a swipe sensor (a tight line of sensors), the client slides a finger vertically over the surface. These sensors are ideally utilized as a part of versatile customer electronics because of their size and shape [4,5].

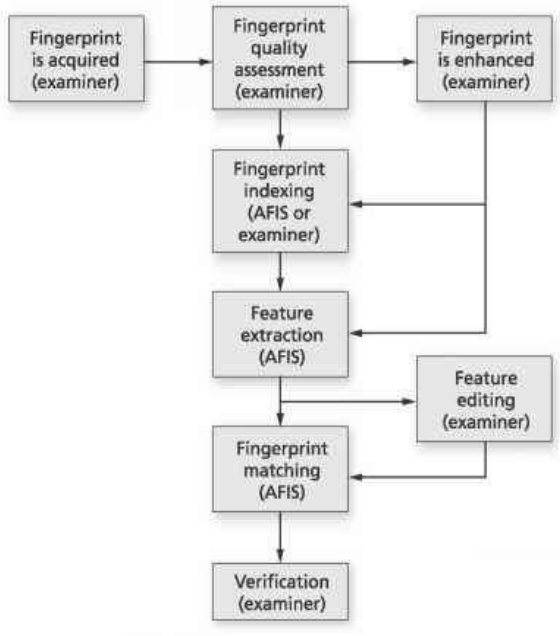


Figure 2-Fingerprint Sensor Technology

Automated fingerprint identification system (AFIS) flow chart data), and comparison evaluation (the machine evaluates the quality of the "match"). The AFIS may be set to accept or reject a certain threshold of comparison quality. In this way the examiner can increase or reduce the number of possible matches the machine offers.

3.2 Fingerprint based biometrics

A biometric system is embedded in the authentication process of an identity management system. Its result is used to decide if the individual that has delivered the biometric data shall be recognized by the identity management system. The flow of the data in the Fig. 3 is as follows:

Take fingerprint impression as input. Extraction of Minutiae points from fingerprint is done in four parts:

- HistoFMedian method is used to enhance the fingerprint image.

- Binarization is applied on the enhanced image.

- Region of Interest is extracted by using morphological operations.
- Using Thinning algorithm features are extracted from digitized data.

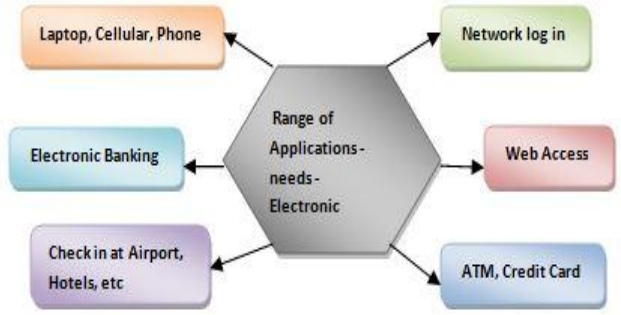


Figure-3 a range of electronic access applications that require automatic recognition

At the same time an attack named PARD attack hit the secured system but as the features are encoded with the key so it will be detected by the matcher.

- On the extracted features now apply key KFV to encode the feature vector.
- A Matcher is a comparison process that evaluates the similarity between the reference templates residing in the database and the captured data sample and that result in a similarity score.
- Assume that the data available in Fingerprint database is also encrypted with the same i.e by key KFV at the time of enrollment of the person.
- If the authentication process authenticates the person who want to use the application device, the secret features will be extracted now and will be available to the application devices, otherwise the authentication process will not allow the person to use the data.
- The key will not get released just after extraction of the features because of the security issues, in fact key will be released on the same side of the application device, otherwise meanwhile an attack can hit on the secret data.
- We present a new fingerprint image enhancement algorithm based on contextual filtering in the Fourier domain. The proposed algorithm is able to simultaneously estimate the local ridge orientation and ridge frequency information using Short Time Fourier Analysis. The algorithm is also able to successfully segment the fingerprint images. The following are some of the advantages of the proposed approach.

- The proposed approach obviates the need for multiple algorithms to compute the intrinsic images and replaces it with a single unified approach.
- This is also a more formal approach for analysing the non-stationary fingerprint image than the local/windowed processing found in literature.
- The algorithm simultaneously computes the orientation image, frequency image and the region mask as a result of the short time Fourier analysis. However, in most of the existing algorithms the frequency image and the region mask depend critically on the accuracy of the orientation estimation.
- The estimate is probabilistic and does not suffer from outliers unlike most maximal response approaches found in literature.
- The algorithm utilized complete contextual information including instantaneous frequency, orientation and even orientation coherence/reliability**.**

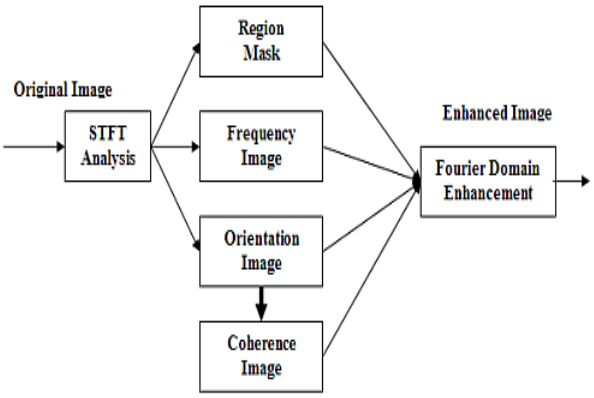


Figure-5 Overview of the proposed approach

Table-1 Summary of previous work

Features	Han, Y., Ryu et al.[1]	Zwiesele et al.[2]	Espinoza et al.[3]	Matsumoto et al.[4]	Galbally et al.[5]
Security	Moderately high	High	high	Medium	Comparative high
Authentication	Yes	Yes	No	Yes	No
Attack Prevention	PARD Attack	Hill climbing attack	PARFD Attack	Brute force Attack	faux feature Attack
Space Complexity	Highly	Highly	Comperitively high	Highly	Medium

Implementation of algorithm	Thinning Algorithm	Finger Print Key Generation Algorithm	BioCrypto Key Generation Algorithm	BioCrypto Key Generation Algorithm	fingerprint matching algorithms
Used technique	Biometric system recognisation	Biometric identification system	Figure print sensor technology	Finger print Impression	Finger print sensing
Efficiency/Reliability	High	Moderate	Medium	Comparative high	High
Speed (Processing)	Moderate speed	Less speed	High speed	High speed	Comparative high
Cost	Less	Average	High	High	High

4. RESULTS AND ANALYSIS

The algorithm proposes to match two fingerprints provided that their minutiae points are identified already. In order to test and verify our algorithm, we used the algorithm proposed by Sharat et all in [23], to extract minutiae points from a given fingerprint image. In short, [23] does fingerprint image enhancement based on STFT (Short Time Fourier Transform) analysis to improve the overall clarity of a fingerprint image and also provides it in a binary format. We use [23] to obtain the enhanced binary image, after which we thin down the binary image down to a width of one pixel so as to retrieve minutiae points from the image. What we have now is a pair of fingerprint images with their minutiae points identified.

involves two phases in order to produce a matching score. In the first phase, the methodology used to obtain the common minutiae point set (minutiae points present in both the base and the input image) is explained. In the second phase, the technique to perform actual matching based on the common minutiae point set is detailed. Figure 3 explains how the minutiae points are obtained using [23].

We conducted tests on Databases 1 and 2 from the FVC 2000 datasets. Database 1 contains images obtained from a low cost optical scanner while Database 2 contains images obtained from a low cost capacitive scanner. Three tests were performed on the databases.

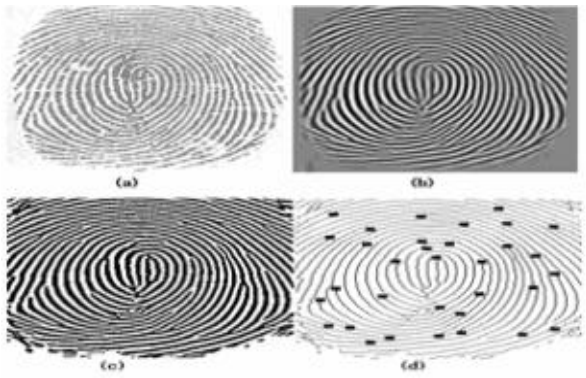
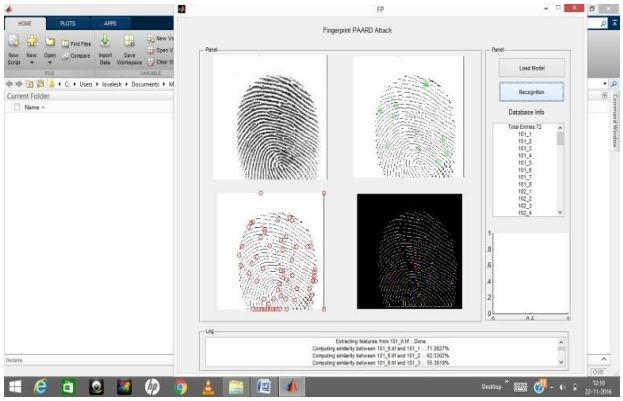


Fig 3: (a) Original image (b) Enhanced image (c) Enhanced Binary image (d) Thinned image

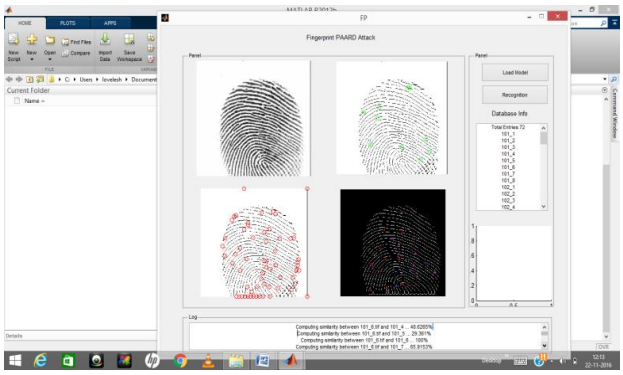
(1) To find the algorithm's efficiency when base and the input images are obtained from the same sensor.

(2) To find the efficiency when the base and input images originated from different sensors. The above two tests are based on Genuine Accept Rates and False Reject Rates.

(3) To find the False Accept Rate. Case 1: Database 1 contains 8 images [8 instances of the same finger] each of 10 different persons.



So there are totally 80 images. For each person, 56 test cases were formulated. That is, out of the 8 instances, one instance would be set as the base image and would be tested against the remaining 7 images, which were considered to be input images. So there would be 7 test cases for one instance of one user. Hence, there would be 8 * 7 = 56 test cases for one person. And there would be 10 * 56 = 560 test cases in total for database 1. We express the efficiency of the algorithm in the following way: Efficiency in % = Number of Positive Matches / Total Number of Test cases. We got the following results for Database 1: Efficiency = 539 / 560 = 96.25 %. Hence the Genuine Accept Rate = 96.25 % and the False Reject Rate = 3.75 %. Similarly there are 560 test cases for database 2. Efficiency in this case = 541 / 560 = 96.61%. Genuine Accept Rate = 96.61%, False Reject Rate = 3.39%. The cumulative results can be given as the following: Efficiency = (539) + (541) / (560) + (560).



5. CONCLUSION

In this paper a overview is done on unique mark acknowledgment systems. Diverse methodologies are considered in wording of performance parameters like PSNR, accuracy and smoothness. So, de-noising techniques are likewise contemplated. The issue of anticipation from those assaults can be taken care of in future likewise work should be possible in the course to find better changes utilized as a part of the framework for security, i.e more discriminable fingerprint components can be intended to enhance the security. It is found that first preprocessing of the fingerprint should be done and then smoothening and de-noising should be done. Then matching should be performed. The literature survey on different existing latent fingerprint methods was includes done in this paper. We have described the contextual in the field, including some situations about feature extraction and pre-processing techniques. Then, we have calculated the main properties of the Latent methods, as well as the information. The effect of incorporating clarity in quality assessment is studied. It is diagrammatically shown that improvement assists in better estimation of quality thus resulting in improved performance.

6. REFERENCES

[1] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, 2003.

[2] R. Derakhshani, S.A.C. Schuckers, L.A. Hornak, and L.O. Gorman, “Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners”, Pattern Recognition, vol. 36, pp. 383-396, 2003.

[3] N.K. Ratha, J.H. Connell, and R.M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems”, IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.

[4] S. Pankanti and M.M. Yeung, “Verification watermarks on fingerprint recognition and retrieval”, Proc. SPIE EI,vol. 3657, pp. 66-78, 1999.

[5] A.K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, “FingerCode: A filterbank for fingerprint representation and matching”, Proc. IEEE Conf. on Computer Vision and Pattern Recognition, vol. 2, pp. 187-193, 1999.

[6] A.K. Jain, L. Hong, S. Pankanti, and R. Bolle, “An identity authentication system using fingerprints”, Proc. IEEE, vol. 85, no. 9, Sept. 1997, pp. 1365-1388.

[7] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial 'gummy' fingers on fingerprint systems," in Proceedings of SPIE, Jan 2002, vol. 4677

[8] Reza Derakshani, Stephanie Schuckers, Larry Hornak, and Lawrence Gorman, "Determination of vitality from a noninvasive biomedical measurement for use in fingerprint scanners,"Pattern Recognition Journal, vol. 36, no. 2, 2003

[9] A Jain, L Hong, and R Bolle, "On-line fingeroint verification,"IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no.4, pp. 302-314, 1997.

[10]A Jain, L Hong, and R Bolle, "On-line fingeroint verification,"IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 4, pp. 302-314, 1997.

[11] M.Bellare, D. Pointcheval, and P. Rogaway, “Authenticated Key Exchange Secure Against Dictionary Attacks,” Advances in Cryptolog Eurocrypt ’00, 2000 pp. 139-155.