Survey on Fingerprint Recognition System using Image Preprocessing and De-noising

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

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

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

ABSTRACT
Biometric authentication plays a major role in security as these are by nature unique for every human. But the security is compromised when the pattern matching system is not accurate. Authentication system like fingerprint recognition is most commonly used biometric authentication system. In this paper survey is done on fingerprint recognition techniques. And different approaches are studied in terms of accuracy and performance. As fingerprint may also contain noise; so image de-noising techniques are also studied Cross ridge frequency analysis of fingerprint images is performed by means of statistical measures and weighted mean phase is calculated. These different features along with ridge reliability or ridge centre frequency are given as inputs to a fuzzy c-means classifier..

Keywords
PSNR, de-noising, Biometric authentication, STFT, SWT, DIP

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 1.1: Secugen Hamster plus Fingerprint Scanner

2. PERFORMANCE PARAMETERS AND TECHNIQUES
If PSNR (Peak Signal to Noise Ratio) value decreases quality of Image Increases and Vice versa with respect to the different image enhancement technique will give the Different values for PSNR.

SWT Approach –The Stationary Wavelet Transform was proposed to make the decomposition time invariant. In order to preserve the invariance by translation, the down sampling operation must be suppressed and the decomposition obtained in redundant form, which is to be referred as Stationary Wavelet Transform, results with some texture descriptor based on the intensity histogram:

a) Mean (M): It measures the average intensity of given image

b) Standard Deviation (σ): It measures the average contrast of the image.

c) Smoothness (S): It measures the relative smoothness of the intensity in a region. S is 0 for a region of constant intensity and approaches 1 for regions with large excursions in the values of its intensity levels. The variance used in this measure is normalized to the range 0 to 1.

d) Uniformity (U): It measures uniformity. It is maximum when all gray levels are equal (maximally uniform).

e) It is observed that there is variation in Image smoothness between before and after enhancement

STFT. is a well-known technique in signal processing to analyze non-stationary signals. The algorithm estimates all the intrinsic properties of the fingerprints such as the foreground region mask, local ridge orientation and local ridge frequency. Furthermore a probabilistic approach of robustly estimating these parameters. This experiments have been compare with the proposed method to other filtering approaches in literature have shown that this technique performs favorably. Fingerprints are one in all the foremost mature biometric technologies and also are thought-about legitimate proofs of proof in courts of law everywhere the planet. Fingerprints are, therefore, employed in forensic divisions worldwide for criminal investigations.

3. 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 [3, 4].

3.1 Fingerprint based biometrics

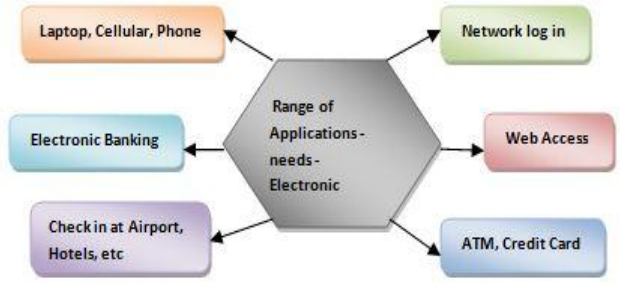

Figure-3.1: A range of electronic access applications that require automatic recognition

The figure-2 depicts numerous electronic access applications in widespread use that need automatic recognition. If the fingerprint recognition may be aa part of a security concept, one needs to expect specialized attacks. The appliance determines quality and amount of the safety demand. Every application state of affairs the expected attacks and their likelihood needs to be determined to be ready to determine that is that the expense for counter measures against each reasonably attacks. Attacks like Brute force, faux feature attacks, Replay attacks, Latent print attacks, worm attacks, Dead feature attacks, Hill climbing attacks, Software leaks and Use of force attacks are most typical and vital to biometric security parts. It depends on the particular application, against that attacks security measures are necessary.

4. LITERATURE SURVEY

In [1] Chaohong Wu, Zhixin Shi and Venu Govindaraju describes an integration model for fingerprint image enhancement. The gap with some length between the two ends of broken ridges is effectively joined. One filled gap can remove two false ending minutiae the smudges of small size and medium size in the valleys are cleaned out. The holes in the ridges are completely removed. Ridge boundaries become much smoother. However, some problems need to be solved. This algorithm fails when image regions are contaminated with heavy noises and orientation field in these regions can hardly be estimated. Therefore, segmentation of these unrecoverable regions from the original image is necessary. Through the clustering of image quality characteristics, the performance of the proposed method was evaluated by using the block directional difference and the Quality Index of the extracted minutiae. The results show that the proposed method is able to improve both block directional difference and quality index, and the time required is in a reasonable range. But image characteristic factors for the identification system in real worlds are still required to be improved. The research is going on with respective to the method but the result is still not to be up to the level of matching the fingerprint.

In [2] authors suggest that, the novel features for minutiae verification in fingerprint images provides accuracy superior to anything other dim scale approaches specified in writing. The methodologies are computationally productive and can likewise be utilized to plan details indicator that can specifically work on the dim scale pictures. Be that as it may, intertwining the choice of the two classifiers and studying the effects of minutiae verification on matching performance are still required to improved Image and that can be possible with the help of enhancement.

The strategies in light of direct dark scale improvement perform superior to anything approaches which require binarization and diminishing as middle of the road steps. The normal blunder rate, regarding dropped, traded and false particulars, as created by binarization methodology, is impressively lower than the errors produced by approaches. The modified Gabor filter performs better especially for poor quality images with corrupted ridges and blocks with singular points. The need for estimation of local frequency information, as conducted by Gabor-based filter, is eliminated by using unique anisotropic filter. The enhancement scheme which is used still requires speed and efficiency as well. In this paper, we analyze these attacks in the realm of a fingerprint-based biometric system. Fingerprint-based systems are among the most frequently deployed biometric systems, due to their accuracy, size, cost, performance and proven track record. Hence, we choose to use a fingerprint-based system in this study.

The paper introduces by Hong et al. entitle with a new approach for fingerprint

In [3], on behalf of Pattern Recognition Society suggest the most generally refered to unique mark improvement strategy taking into account the convolution of the picture with Gabor channels tuned to the nearby edge introduction and edge recurrence. The principle phases of this calculation incorporate standardization, edge introduction estimation, edge recurrence estimation and filtering. The initial phase in this methodology includes the standardization of the unique mark picture for which it has a pre specified mean and change. Because of defects in the unique mark picture catch

process, for example, non-uniform ink power or non-uniform contact with the finger impression catch gadget, a finger impression picture may show bended levels of variety in dark level qualities along the edges and valleys. Hence, standardization is utilized to lessen the impact of these variations which facilitates the subsequent.

In [4], Umut Uludag, Anil K. Jain. Attacks on Biometric Systems: A Case Study in Fingerprints tested several fingerprint sensors to check whether they accept an artificially created (dummy) finger instead of a real finger. The authors describe methods to create dummy fingers with and without the cooperation of the real owner of the biometric (say, Alice). When the owner cooperates (namely, Alice is helping the attackers), obviously, the quality of the produced dummy fingers can be higher than those produced without cooperation (namely, Alice is a victim of the attackers).

In (5) Afzel Noore , Richa Singh , Mayank Vatsa , Max M. Houck ."Enhancing security of fingerprints through contextual biometric watermarking" This paper presents a novel digital watermarking technique using face and demographic text data as multiple watermarks for verifying the chain of custody and protecting the integrity of a fingerprint image. The watermarks are embedded in selected texture regions of a fingerprint image using discrete wavelet transform. Experimental results show that modifications in these locations are visually imperceptible and maintain the minutiae details. The integrity of the fingerprint image is verified through the high matching scores obtained from an automatic fingerprint identification system. There is also a high degree of visual correlation between the embedded images, and the extracted images from the watermarked fingerprint.

The degree of similarity is computed using pixel-based metrics and human visual system metrics. The results also show that the proposed watermarked fingerprint and the extracted images are resilient to common attacks such as compression, filtering, and noise. In this paper, a contextual fingerprint image watermarking algorithm is proposed. Two watermarks, a facial image and the corresponding demographic text data of an individual are embedded into selected texture regions of fingerprint image using discrete wavelet transform. The watermarked fingerprint provides added protection from tampering and the fingerprint matching ability is not affected even when subjected to common attacks.

In (6) Stephen M. Matyas Jr.1 and Jeff Stapleton2A Biometric Standard for Information Management and Security . Biometric systems are being widely developed and deployed to provide greater security to users and there is an increased awareness of the value of biometric systems. Biometric systems are being developed and deployed; users are gaining experience and confidence in biometric systems and are beginning to reap the benefits of this technology. Users and developers of this technology have also recognized the need for a biometric standard and work on a defining standard is currently underway. The standard establishes an appropriate biometric model and the associated security requirements that will allow different biometric solutions to co-exist in the marketplace.

The standard views biometric systems within a global user community and it assures that the security of any one biometric system will be unaffected by the security of any other biometric system. Biometrics are fast emerging as a reliable automated method of establishing the identity of a living person, such as an ATM customer or computer user. Examples of biometrics include finger, voice, iris, face and hand.The single data representation of a biometric characteristic or measurement, captured or scanned by a biometric device is called a biometric sample.The information extracted from one or more biometric samples is used to create a biometric template.

In(7)AdityaAbhyankar,Stephani Schuckers. Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques.It has been demonstrated that simple and inexpensive techniques are sufficient to spoof fingerprint scanners. Previously, effective use of physiological phenomenon of perspiration is shown as a countermeasure against such attacks. These techniques require more than one image for performing the liveness check and hence may not be suited for on-line processing. In this work, a liveness measure based on single image is developed. The inherent texture and density differences between 'live' and 'not live' fingerprint images are exploited. Multire solution texture analysis techniques are used to minimize the energy associated with phase and orientation maps. Cross ridge frequency analysis of fingerprint images is performed by means of statistical measures and weighted mean phase is calculated. These different features along with ridge reliability or ridge center frequency are given as inputs to a fuzzy c-means classifier.

The proposed algorithm was applied to a dataset of approximately 58 live, 50 spoof and 28 cadaver fingerprint images, from three different types of scanners. An error rate of 1.4% is achieved. The algorithm provides a faster technique for doing a liveness test which relies on only one fingerprint image.

In(8) Hisham Al-Assam*, Sabah Jassim "Security evaluation of biometric keys" Biometric cryptosystems combine biometrics with cryptography by producing Biometric Cryptographic Keys (BCKs) to provide stronger security mechanisms while protecting against identity theft. The process of generating/binding biometric keys consists of a number of steps starting with a feature extraction procedure, the complexity of which depends on the specific biometric trait/scheme, followed often by user selected transformation to allow for revocability, and an error correction scheme to tolerate reasonable amount of intra-class variation. Each of these steps has its own effect on the security of the generated/bound key. Proper security evaluation must include thorough analysis of the security effect of each of these steps. We propose a comprehensive approach to BCK's security evaluation that takes into consideration each of the steps involved in their construction. We first review existing BCKs and highlight that the analysis of their security is either insufficient or not provided. In addition to evaluating the correctness (i.e. error rates), and the generated/bound key size, we evaluate the randomness of biometric features employed in the process of key generation.

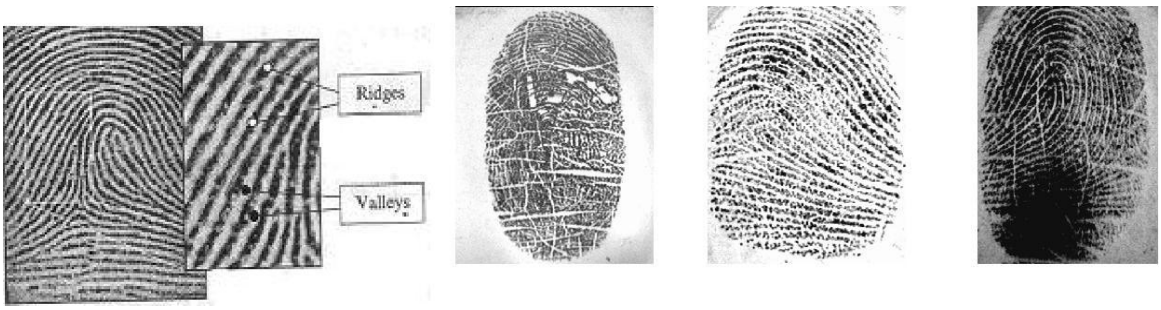

Figure-3

(a) Show the ridges and valleys (b) cuts in fingerprint (c) low contrast (d) different pressure on devices

Table 4.1. 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	Moderatily high	high	high	Medium	Comperitive 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	BioCryptKey Generation Algorithm	BioCryptKey Generation Algorithm	fingerprint matching algorithms
Used technique	Biomtic system recognisation	Biometrc identification system	Figure print sensor technoly	Fingue print Impression	Fingure print sensing
Efficiency/Reliability	High	Moderate	Medium	Comperitive high	High
Speed (Processing)	Moderate speed	Less speed	High speed	High speed	Comperitive high
Cost	Less	Average	High	High	High

5. CONCLUSION

In this paper a survey is done on fingerprint recognition techniques. Different approaches are studied in terms of performance parameters like PSNR, accuracy and smoothness. So, de-noising techniques are also studied. The issue of prevention from those attacks can be handled in future also work can be done in the direction to find better transformations used in the system for security, i.e more discriminable fingerprint features can be designed to improve 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.

6. REFERENCES

[1] Han Y, Ryu C, Moon J, Kim H, Choi H. A study on evaluating the uniqueness of fingerprints using statistical analysis. InInternational Conference on Information Security and Cryptology 2004 Dec 2 (pp. 467-477).

[2] Zwiesele A, Munde A, Busch C, Daum H. BioIS study. Comparative study of biometric identification systems. InSecurity Technology, 2000. Proceedings. IEEE 34th Annual 2000 International Carnahan Conference on 2000 (pp. 60-63).

[3] Espinoza M, Champod C, Margot P. Vulnerabilities of fingerprint reader to fake fingerprints attacks. Forensic science international. 2011 Jan 30;204(1):41-9.

[4] Espinoza M, Champod C. Risk evaluation for spoofing against a sensor supplied with liveness detection. Forensic science international. 2011 Jan 30;204(1):162-8.

[5] Galbally J, Fierrez J, Alonso-Fernandez F, Martinez-Diaz M. Evaluation of direct attacks to fingerprint verification systems. Telecommunication Systems. 2011 Aug 1;47(3-4):243-54.

[6] Kang H, Lee B, Kim H, Shin D, Kim J. A study on performance evaluation of the liveness detection for various fingerprint sensor modules. InInternational Conference on Knowledge-Based and Intelligent Information and Engineering Systems 2003 Sep 3 (pp. 1245-1253).

[7] Van der Putte T, Keuning J. Biometrical fingerprint recognition: don't get your fingers burned. InSmart Card Research and Advanced Applications 2000 (pp. 289-303).

[8] Matsumoto T, Matsumoto H, Yamada K, Hoshino S. Impact of artificial gummy fingers on fingerprint systems. InElectronic Imaging 2002 2002 Apr 18 (pp. 275-289).

[9] Wiehe A, Søndrol T, Olsen OK, Skarderud F. Attacking fingerprint sensors. Gjøvik University College. 2004 Dec.

[10] Memon S, Sepasian M, Balachandran W. Review of Fingerprint Sensing Technologies. Proc. INMIC. 2008 Dec 23;8.

[11]Salil Prabhakar, Anil Jain, and Sharath Pankanti. Learning fingerprint minutiae location and type Number 8, pages 1847–1857, 2003.

[12]Salil Prabhakar, Anil Jain, J. Wang, Sharath Pankanti, and Ruud Bolle. Minutiae verification and classification for fingerprint maching.In international conference on pattern .volunme 1 2000

[13] Che-Yen Wen and Chiu-Chung Yu. Fingerprint enhancement using am-fm reaction diffusion systems. *Journal of Forensic Science*, 48(5), 2003.

[14] K. Nilsson and J. Bigun. Localization of corresponding points in fingerprints by complex filtering. *Pattern Recognition Letters*, 24, 2003.

[15] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial gummy fingers on fingerprint systems. In *Proceedings of SPIE,Optical Security and Counterfeit Deterrence Techniques IV*, volume 8577, 2002

16] D. Maio, D. Maltoni, A. K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer Verlag, 2003

[17] T. Jea, V. K. Chavan, V. Govindaraju, and J. K. Schneider. Security and matching of partial fingerprint recognition systems. In *Proceeding of SPIE*, number 5404, pages 39–50, 2004.[20] Anil Jain, Salil Prabhakar, Lin Hong, and Sharath Pankanti. Filterbank-based fingerprint matching. In *Transactions on Image Processing*, volume 9, pages 846–859, May 2000.

[18] Jinwei Gu and Jie Zhou. A novel model for orientation field of fingerprints. In *IEEE Computer Society Conference On Computer Vision and Pattern Recognition*, 2003

[19] M. D. Garris, C. I. Watson, R. M. McCabe, and C. L. Wilson. Users guide to nist fingerprint image software (nfis). Technical Report NISTIR 6813, National Institute of StandardsandTechnology,2002.

[20]S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric recognition: Security and privacy concerns. *IEEE Security and Privacy Magazine*, 1(2):33–42, 2003.

[21] P. Ramo, M. Tico, V. Onnia, and J. Saarinen. Optimized singular point detection algorithm for fingerprint images. *IEEE Transactions on Image Processing*, 3:242–245, 2001.