SIFT Based Minutia Descriptors for Fingerprint Combination Protection

Nalini. P
Coimbatore- 641 659, Tamil Nadu, India

Abstract — Biometrics is the technique of evaluating and statistically analyzing biological data that can be used to recognize various biometric features. Therefore, the biometric approach provides higher security. An automated process of identifying an individual based on the individual's biometric features is the biometric approach. Fingerprint-based identification biometric technique is the oldest method which has been successfully used in numerous applications. Each one is known to have distinctive fingerprints.The privacy protection of the fingerprint becomes an important issue with the widespread application of fingerprint techniques in authentication systems. Traditional encryption is not sufficient for fingerprint privacy protection because decryption is required before the fingerprint matching, which exposes the fingerprint to the attacker. Existing method used techniques for protecting fingerprint privacy by combining two different fingerprints into a new identity. However in such a case low quality fingerprint minutiae were not authenticated. To enhance the efficiency and effectiveness of the algorithm for fingerprint verification, SIFT-based Minutiae Descriptor (SMD) is proposed to improve the SIFT algorithm through image processing, descriptor extraction and matcher. This can be done by two step matching process. A two-step fast matcher, named improved All Descriptor-Pair Matching (iADM), is also proposed to implement the 1: N verifications in real-time. Experiment is conducted on MATLAB and it provides better results compared to existing approach.

***Keywords*—**SIFT-based Minutiae Descriptor**,** improved All Descriptor-Pair Matching,Fingerprint.

1. INTRODUCTION

Fingerprint mainly comprises of series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be found by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are a local ridge characteristic that appears at either a ridge bifurcation or a ridge ending.

The biometric device involves a user placing his finger on a platen for the fingerprint to be read. Inorder to generate a template, minutiae are extracted by the vendor’s particular algorithm. Fingerprint biometrics has three main application arenas: large-scale Automated Finger Imaging Systems (AFIS) for law enforcement uses, access control for facilities or computers and fraud prevention in entitlement programs.

Fingerprint recognition has a good balance related to seven pillars of

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

biometrics. Nearly every human being possesses fingerprints (universality) with the exception of hand-related disabilities. Fingerprints are also distinctive and the fingerprint details are permanent, although they may temporarily change due to cuts and bruises on the skin or external conditions (e.g. wet fingers). Live-scan fingerprint sensors can capture high-quality images (collectability) [1]. The deployed fingerprint-based biometric systems offer good performance and fingerprint sensors have become quite small and affordable.

Fingerprints have a stigma of criminality related with them but that is changing with the increased demand of automatic recognition and authentication in a digitally interconnected society (acceptability). By combining the use of multiple fingers, cryptographic techniques and liveness detection, fingerprint systems are becoming quite difficult to circumvent. When only one finger is used however, universal access and permanent availability may be problematic. Moreover, everyday life conditions can also cause deformations of the fingerprint, for instance as a result of doing manual work or playing an instrument. Certain conditions, such as arthritis, affect the ease of use of fingerprint readers. Other conditions such as eczema, may affect the fingerprint itself. It is estimated that circa five per cent of people would not be able to register and deliver a readable fingerprint.

Figure 1: Fingerprint

The two main unique characteristic features of fingerprints are:

• Fingerprints never change: The ridges that are present in hands and feet do not change ever.

• No two fingerprints are alike. The ridges have three characteristics namely ridge endings, bifurcations and dots. A ridge ending is simply the end of a ridge. A dot is a very short ridge that looks like a “dot”. A bifurcation is a Y-shaped split of one ridge into two. These characteristics are not repeated in any two persons.

Fingerprint image acquisition is the most critical step in a fingerprint authentication system since it determines the final fingerprint image quality that has an extreme effect on the overall system performance [2]. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. Patterns are the aggregate characteristics of ridges, and minutia points. The three basic patterns of fingerprint ridges are the arch, loop, and whorl [3]. The ridges enter from one side of the finger which rises in the center forming an arc, and go out to the other side of the finger. The ridges enter from one side of a finger that forms a curve, and go out on that same side.

Ridges form circularly around a central point on the finger.

Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images to be aligned in the same orientation. This algorithm finds a central point in the fingerprint image and centers on that. Template contains size, type and orientation of patterns within the aligned fingerprint image. Person’s fingerprint image is graphically compared with the

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

template to determine the degree to which they match.

The paper can be organized as follows: Paper can be organized as follows: Section III describes about the algorithms used in the proposed methodology. Section IV deals with the results obtained during experiment. The concluding work is presented in section V.

2. RELATED WORKS

A new approach fuses fingerprint and voice data at the template level [4]. Fingerprint and voice modalities are the most practical and commonly accepted biometrics; especially, voice is a familiar way of communicating for humans. The constructed multi-biometric templates are non-unique which reduces privacy concerns. The recital of the biometric system is increased since multiple biometrics is used in verification. Changing the password in text-dependent voice verification systems can provide cancelable biometric templates. It is not possible with physiological biometrics such as fingerprints. Therefore, combining a cancelable biometric with non-cancelable biometrics is advantageous on several counts.

A fingerprint-matching approach is proposed based on standardized fingerprint model to synthesize fingerprint from original templates [5]. Chose one as mean images from the fingerprint templates of finger in the database and Genetic Algorithms is used to find the transformation among them. Subsequently, these transformations are used to synthesize fingerprints by adding ridges and minutiae from original template to mean fingerprint. At last, matching between mean fingerprint and other templates such as FVC2004 DB4 database that contains poor-quality fingerprints is performed to show the capability of the model.

Several methods are demonstrated in this method to generate multiple cancelable identifiers from fingerprint images to overcome these problems [6]. Essentially, a user can be given as many biometric identifiers as needed by issuing a new transformation key. These identifiers can be cancelled and replaced when conciliation. Performance of several algorithms such as polar, cartesian, and surface folding transformations of the minutiae positions are also compared. It is revealed through multiple experiments that revocability is achieved and cross-matching of biometric databases is prevented. It is proved that the transforms are noninvertible by demonstrating that it is computationally as hard to recover the original biometric identifier from a transformed version as by randomly guessing. On conclusion, feature-level cancelable biometric construction is practicable in large biometric deployments based on these empirical results and a theoretical analysis.

A novel two factor authenticator is proposed based on iterated inner products between tokenised pseudo-random number and the user specific fingerprint feature that is generated from the integrated wavelet and Fourier–Mellin transform [7]. Therefore it produces a set of user specific compact code that coined as BioHashing which is highly tolerant of data capture offsets with same user fingerprint data resulting in highly correlated bitstrings. Furthermore, there is no deterministic way to get the user specific code without having both token with random data and user fingerprint feature. Thus it would protect us for instance against biometric fabrication by changing the user specific credential is simpler than changing the token containing the indiscriminate records. The BioHashing has significant functional advantages over solely biometrics (zero equal error rate point and clean separation of the genuine and imposter populations, thus allowing

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

elimination of false accept rates without suffering from increased occurrence of false reject rates).

A minutia matching is the most popular approach to fingerprint verification. A novel fingerprint feature named the Adjacent Feature Vector (AFV) is proposed for fingerprint matching [8]. It consists of four adjacent relative orientations and six ridge counts of a minutia. The optimal matching score is computed in three stages for the specified fingerprint image: minutiae candidate pairs searching based on AFVs, coordinate transform for image rotation and translation and transformed minutiae matching to get matching score. The tested results show that this method provides a good trade-off between speed and accuracy.

The problem of retrieving candidate lists for matching partial fingerprints is investigated by exploiting global topological features [9]. Distinctively, an analytical approach is proposed for reconstructing the global topology representation from a partial fingerprint. Initially, an inverse orientation model is presented for describing the reconstruction problem. Afterwards, a general expression is provided for all valid solutions to the inverse model. It permits us to preserve data fidelity in the existing segments while exploring missing structures in the unknown parts. Further algorithms are developed for estimating the missing orientation structures based on some a priori knowledge of ridge topology features. The experimental results showed that model-based approach can effectively reduce the number of candidates for pair-wised fingerprint matching, thereby considerably improve the system retrieval performance for partial fingerprint identification.

3. METHODOLOGY

Fingerprint privacy is protected by a SIFT based minutiae extraction by combining two different fingerprints and reconstructing the fingerprints into a new identity. Two fingerprints are captured from two dissimilar fingers in the enrollment. The minutiae position is extracted from one fingerprint and orientation is extracted from the other fingerprint. Reference points are extracted for both fingerprints. A combined minutiae template is generated and stored in a database based on this extracted information and coding strategies. The system requires two query fingerprints from the same two fingers which were used in the enrollment for authentication purpose. The orientation and SIFT based minutiae extraction is to be done. SIFT based minutiae extraction consists of three steps of processing which includes preprocessing, descriptor extraction and all descriptor pair matching. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against a combined minutiae template. The extracted information of two different fingerprints can be matched against the database fingerprint images.

The algorithm used to protect fingerprint combination is described below.

- **Reference Point Detection**

Given a fingerprints, the main steps of the reference point's detection are summarized as follows:

- Compute the orientation O from the fingerprints. Obtain the orientation Z in complex domain described as follows

- Calculate a certainty map of reference points

Where * is the convolution operator and $_{ref}$ is the conjugate of

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

which is the kernel for reference point's detection.

- Calculate an improved certainty map

Where Arg (z) returns the principal value of the argument of z

- Locate a reference point satisfying the two criterions: amplitude of of the point s a local maximum, and the local maximum should be over a fixed threshold T.

A reference point at the corresponding angle can be estimated as)

- Repeat step 4 until all reference points are located.
- If no reference point is found for the fingerprint in steps 4 and 5 (e.g., an arch fingerprint), locate a reference point with the maximum certainty value in the whole fingerprint image.

- **Minutiae Position Extraction**

- Fingerprint Ridge Thinning

Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide and uses an iterative parallel thinning algorithm. This algorithm marks down redundant pixels in each small image window (3x3) in every scan of the full fingerprint image. And finally removes all those marked pixels after several scans. While testing, such an iterative parallel thinning algorithm has bad efficiency although it can get an ideal thinned ridge map after enough scans, a one-in-all method to extract thinned ridges from gray-level fingerprint images directly. These method traces along the ridges having maximum gray intensity value. Though, binarization is implicitly enforced since only pixels with maximum gray intensity value are remained. Thinned ridge map is then filtered by other three Morphological operations to remove some isolated points, H breaks and spikes.

- Minutiae Marking

After the fingerprint ridge thinning, spotting minutia points is relatively easy. However it is still not a trivial task as most literatures declared because at least one special case evokes my caution during the minutiae marking stage.

Usually, for each 3x3 window, the central pixel is a ridge branch [Figure 2(a)] if the central pixel is 1 and has exactly 3 one-value neighbors. The central pixel is a ridge ending [Figure 2(b)] if the central pixel is 1 and has only 1 one-value neighbor.

0	1	0	0	0	0	0	1	0
0	1	0	0	1	0	0	1	1
1	0	1	0	0	1	1	0	0
(a) Bifurcation			(b) Termination			(c) Triple counting branch		

Figure 2: Minutiae Marking

It illustrates a special case that a genuine branch is triple counted. Assume both the uppermost pixel with value 1 and the rightmost pixel with value 1 have another neighbor outside the 3x3 window, therefore the two pixels will be marked as branches too. Although actually one branch is located in the small region. Hence a check routine requiring that none of the neighbors of a branch are branches is added.

At this stage, the average inter-ridge width D is estimated. The average inter-ridge width refers to the average distance between two neighboring ridges. The approach to approximate the D value is easy. Scan a row of the thinned ridge image and sum up all pixels in the row whose value is one. Next divide the row length with the above summation to get an inter-ridge width. Such kind of row scan is performed upon several other rows and column scans are also conducted for more accuracy. Finally all the inter-ridge widths are averaged to get the D.

All thinned ridges in the fingerprint image together with the minutia marking

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

are labeled with a unique ID for further operation.

- **Combined Minutiae Template Generation**

The combined minutiae template generated by is not appropriate for generating a combined fingerprint. To create a real-look alike fingerprint image from a set of minutiae points, further apply a noising and rendering step after adopting the work where the following 7 stages are carried through as illustrated below.

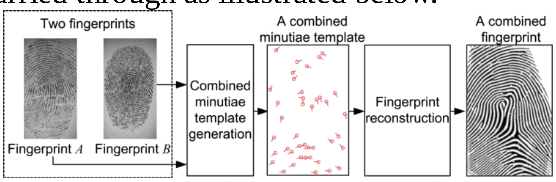


Figure 3: Generating a combined fingerprint for two different fingerprints

- Estimate an orientation field from the set of minutiae points by adopting the orientation reconstruction algorithm [3].
- Generate a binary ridge pattern based on and a predefined fingerprint ridge frequency using Gabor filtering.
- Estimate the phase image of the binary ridge pattern
- Reconstruct the continuous phase image by removing the spirals in the phase image
- Combine the continuous phase image and the spiral phase image (calculated from the minutiae points), generating a reconstructed phase image.
- Refine the reconstructed phase image by removing the spurious minutiae points to produce a refined phase image r
- Apply a noising and rendering step on r so as to create a real-look alike fingerprint image.

- **Two Stage Matching**

Two stage fingerprint matching includes query minutiae determination and matching score calculation

- Query Minutiae Determination

Query minutiae determination is an important step in fingerprint matching. The local features are extracted from the minutiae point. The distance and direction calculation is carried out between the two nearest features extracted.

- Matching Score Calculation

For the combined minutiae templates that are generated, perform modulo for all the minutiae directions [10]. After modulo operation, use a minutiae matching algorithm to calculate a matching score between the query minutiae and the original minutiae features extracted.

- **SIFT Based Minutiae Descriptor**
- Fingerprint Image Preprocessing

The SIFT descriptor becomes unstable in the presence of variations in finger pressure or differences in skin characteristics [5]. Therefore, the gray-scale fingerprint images without pre-processing are not proper for original SIFT extraction. Figure 4 shows the image processing flow employed in FISiA. Filters are used to process the original fingerprint image to derive an enhanced gray image. It can be partitioned into the following major stages: highpass filter, ridge direction detection, lowpass filter, and ridge enhancement.

- Descriptors Extraction

Binarization and thinning are performed initially. Minutiae are detected from the thinned image. The type of minutiae can also be classified into ridge bifurcation and ridge ending [11].

Ridge bifurcation minutia is a point where a ridge splits from a single path to two paths, while a ridge ending minutia is a point where a ridge terminate. The minutia m is defined by

which includes its x and y coordinates and the direction by tracing.

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

The SIFT descriptor are calculated based on the processed image .The skeleton image should not be used to extract minutiae because the texture information needed by the SIFT operator are removed in the skeleton image. A SIFT descriptor is proposed by computing the gradient magnitude and orientation (as shown on the left of Figure 5) at each point in a region around the sampling point. These samples are then accumulated into orientation histograms summarizing the contents over the sub-regions (as shown on the right of Figure 5). The recommended descriptor consists of the SIFT descriptor of the minutia and SIFT descriptors at several sampling points around the minutia.

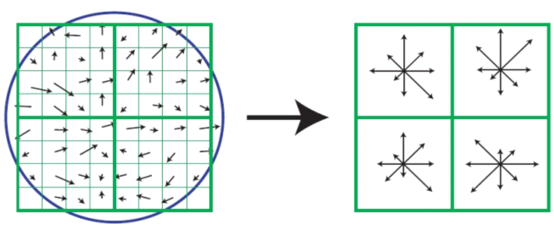


Figure 4: SIFT Descriptor

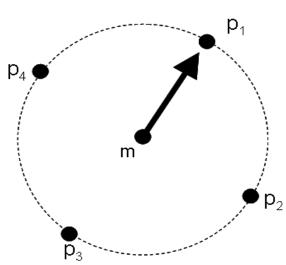


Figure 5: SIFT-based Minutia Descriptor (SMD)

- Improved All Descriptor-Pair Matching

Using the proposed SIFT-based minutia descriptor (SMD), a two-step fast matching method, named improved All Descriptor-Pair Matching (IADM) was developed. The optimized ADM is the improved All Descriptor-Pair Matching (IADM), which is two-step fast matching method consisting of global search and local search.

In the first step, the optimized ADM is performed only based on the SIFT descriptor of minutiae positions. In other words, only the S (m) of D (m) is used in the equation. As the result of this step, the peak of the Hough Transform which shows the best alignment transformation (Δx, Δy, Δθ) is obtained.

This is the result of the rough alignment transformation which will be used for local search. Since the SIFT descriptor of minutiae positions is only N/5 where N is the number of SIFT points, the computation of Euclidean Distance is (N 2 /25) times. Actually, a more efficient way can be applied. Rather than using 2-D accumulator array, BX and BY, two 1-D accumulator arrays are used as the histogram arrays for each corresponding axis of the displacement vector. These histograms accumulate scores for each axis Δx and Δy as shown in Figure 6. Then the center of the distribution score and can be obtained by analyzing these histograms. The best rotation Δθ can also be obtained by repeating all possible rotation steps by Optimized ADM. The easiest way is to extract the locations with the maximum value of each histogram. The method of employing two 1-D arrays has two advantages. It is able to decrease the time for searching peak from the accumulator array. In addition, the memory requirement can also be decreased. The local search is applied in the second step. Only the SIFT descriptor of sampling points around minutiae are used for local matching. The

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

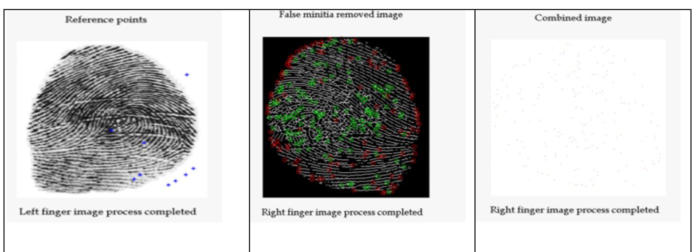
matching is performed by employing the Hough Transform for all closest pairs calculated by Euclidean Distance in this local area by the same way. A small 2-D accumulator array C, with (,) as the center, is utilized to accumulate the score.

4. EXPERIMENTAL RESULTS

The experiment is conducted on the first two impressions of the FVC2002 DB2 database that contains 200 fingerprints from 100 fingers with 2 impressions per finger using MATLAB software.

The experimental results obtained by processing fingerprint image using proposed techniques are shown as follows:

Fingerprint Feature Images	**Combined Fingerprint image**
1-10	1.87
11-20	1.83
21-30	1.80
31-40	1.79



(a) Reference point detection	(b) False Minutiae Removal	(c) Combined image processing

Figure 6: Different types of new identity generated from two different fingerprints.

Reference points are obtained by processing left fingerprint of an image. In right fingerprint image, false minutiae are removed. Finally both fingerprint images are combined to create a new identity which should not be easily hacked by others.

The ultimate measure of utility of a biometric system for a particular application is recognition rate. This can be described by two values.

- False Acceptance Rate (FAR): The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percentage of invalid inputs which are incorrectly accepted.
- False Rejection Rate (FRR): The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percentage of valid inputs which are incorrectly rejected.

FAR and FRR are trade off against one another. That is, a system can usually be adjusted to vary these two results for a particular application. However, decreasing, one increases the other and vice versa.

- **FRR Comparison of Combined Fingerprint image**

- Table 1 shows the FRR comparison of the combined fingerprint image. From the database, 40 test fingerprint feature images are taken up for the evaluation of this experiment. The FRR ratio is obtained in terms of 10 samples from 1 to 40.

TABLE 1: FALSE REJECTION RATE (FRR) (%) COMPARISON

It is clearly observed that the FRR obtained for the first 10 sample fingerprint images is 1.87%. Thus, the FRR obtained by the proposed method is lesser than that of existing method which is 6%.

- **FAR Comparison of Combined Fingerprint image**

Table 2 shows the FAR comparison of the combined fingerprint image.The same procedure followed for the FRR comparison is used in this section.

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

TABLE 2: FALSE REJECTION RATE (FRR) (%) COMPARISON

Fingerprint Feature Images	Combined Fingerprint image
1-10	0.050
11-20	0.054
21-30	0.067
31-40	0.070

It is clearly observed that the FAR obtained for the first 10 sample fingerprint images is 0.050%. Thus, the FRR obtained by the proposed method is lesser than that of existing method which is 0.1%.

- **Accuracy Calculation**

The average FAR and FRR for the 40 test biometric images is calculated. Then, accuracy is obtained by the following formula

Table 3 shows the accuracy evaluation of the combined fingerprint image. It is observed from the table that the proposed system provides better accuracy when compared with the existing work. Average accuracy obtained by our fingerprint combination method is 98.06 %.

TABLE 3: ACCURACY EVALUATION OF THE COMBINED FINGERPRINT IMAGE

Fingerprint Feature Images	FRR	FAR	Accuracy
1-10	1.17	0.050	98.05
11-20	1.13	0.054	98.054
21-30	1.10	0.067	98.067
31-40	1.09	0.070	98.07

Thus the proposed method achieves better results even for fingerprints with lots of cuts and less overlapping areas.

5. CONCLUSION

Protection of fingerprint combination using combined fingerprint template and fingerprint reconstruction is presented. Fingerprints are captured along with its orientation and minutiae points and reference points. A combined minutiae template was created from those fingerprints to generate a new identity. A combined minutiae template containing only a partial minutiae feature of each of the two fingerprints was generated and stored in a database. The combined minutiae template was similar to an original minutiae template. Fingerprint reconstruction was employed to create a single fingerprint from the combined fingerprints. By reconstruction a real-look alike fingerprint was obtained from the combined minutiae template. Finally a two stage fingerprint matching was done to match the query fingerprint against the reconstructed fingerprint. A fingerprint identification algorithm using SIFT-based Minutia Descriptor (SMD) and improved All Descriptor-Pair Matching (IADM) can deal not only with normal fingerprints, but also specific fingerprints with lots of cuts and less overlapping areas. Fingerprint identification algorithm makes the descriptor more robust to variations in finger pressure or differences in skin characteristics. In future, the minutiae extraction from fingerprints will be done using SIFT based minutiae descriptors.

- REFERENCES

[1]Yong-Liang Zhang, Gang Xiao, Yan-Miao Li, Hong-Tao Wu and Ya-Ping Huang, “Slap Fingerprint Segmentation for Live-Scan Devices Ten-Print Cards”, 20th International Conference on Pattern Recognition (ICPR), Pp. 1180 – 1183, 2010.

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

[2]B. J. A. Teoh, C. L. D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," Pattern Recognition, Vol. 37, No. 11, Pp. 2245–2255, 2004.

[3]W. J. Scheirer and T.E. Boult, "Cracking fuzzy vaults and biometric encryption", In Proceedings of Biometrics Symp., Pp. 34–39, September 2007.

[4]Eren Camlikaya, Alisher Kholmatov and Berrin Yanikoglu, "Multi-biometric Templates Using Fingerprint and Voice", Proceedings of SPIE, Vol. 6944, 2008.

[5] Le Hoang Thai and Ha Nhat Tam, "Fingerprint recognition using standardized fingerprint model", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010.

[6] N.K. Ratha, N.Y. Hawthorne, S. Chikkerur, J.H. Connell and R.M. Bolle, "Generating Cancelable Fingerprint Templates", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 4, Pp. 561 – 572, April 2007 .

[7] Andrew Teoh Beng Jin, David Ngo Chek Ling and Alwyn Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number", Pattern Recognition, Vol. 37, No. 11, Pp. 2245–2255, November 2004.

[8] X. Tong, J. Huang, X. Tang and D. Shi, "Fingerprint Minutiae Matching Using Adjacent Feature Vector", Pattern Recognition Letters, Vol. 26, No. 9, Pp. 1337–1345, July 2005.

[9]Yi Wang and Jiankun Hu, "Global Ridge Orientation Modeling for Partial Fingerprint Identification", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 33, No. 1, Pp. 72-87, January 2011.

[10] B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy", In Proceedings of ICPR- BCTP Workshop, Cambridge, U.K., 2004.

[11] Ru Zhou , Dexing Zhong , and Jiuqiang Han "Fingerprint Identification Using SIFT-Based Minutia Descriptors and Improved All Descriptor-Pair Matching" Sensors, Vol.27, 2013.

[12] G. Feng, K. Dong, D. Hu & D. Zhang, When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy, ICBA, pp. 701- 707, 2004.

[13] S. C. Dass, K. Nandakumar & A. K. Jain, A principal approach to score level fusion in Multimodal Biometrics system, Proceedings of ABVPA, 2005.

[14] Rikin, A.S.; Li, D.; Isshiki, T.; Kunieda, H. A fingerprint matching using minutia ridge shape for low cost match-on-card systems. IEICE Trans. Fundam. **2005**, E88-A, 1305-1312.

[15] Chen, J.; Moon, Y.S. Using SIFT features in palmprint authentication. In Proceedings of the 19th International Conference on Pattern Recognition, ICPR 2008, Tampa, FL, USA, 8-11 December 2008; pp. 1-4.

[16] Zhou, R.; Sin, S.W.; Li, D. Isshiki, T.; Kunieda, H. Adaptive SIFT Based Algorithm for Specific Fingerprint Verification. In Proceedings of 2011 International Conference on Hand-Based Biometrics (ICHB), Hong Kong, China, 17-18 November 2011; pp. 1-6.

Nalini. P received B.E degree in Computer Science from Nehru Institute of Engineering & Technology in 2012 and M.E degree in Computer Science from Park College of Engineering & Technology in 2014. I have research interests in image processing. I have presented the paper in national and international conferences.

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR