An Efficient Secure Biometric System with Non-Invertible Gabor Transform

Radha Narayanan[1] and Kathikeyan Subramanian[2]

**[1] Department of Computer Science, Karpagam University
Coimbatore,641 021,Tamil Nadu**

**[2] Department of Information Technology,College of Applied Sciences,
Sohar, Sultanate of Oman**

Abstract

Biometric scheme are being widely employed because their security merits over the earlier authentication system based on records that can be easily lost, guessed or forged. High scale employments and the related template storage have increased the requirement to guard the biometric data stored in the system. Theft of biometric information is a negotiation of the user's privacy. In Addition, the stolen biometric information can be used to access other biometric systems that have the similar feature provided for the user. Several alternative functions have been identified in literature for creating revocable or non-invertible biometric templates. Although, their security examination either disregards the distribution of biometric features or uses inefficient feature matching. This generally shows the way to unrealistic approximation of security. In this paper a novel approach for the Non-Invertible biometric system is proposed to secure the biometric template. Security of a feature transformation method can be assessed according to the two main factors: i) non-invertibility, and ii) diversity. Non-invertibility represents the complexity in obtaining the original biometric when the secure template is provided and diversity represents the complexity in guessing one secure template when a different secure template created from the identical biometric is provided. The proposed Non-invertible Gabor transform possess both the non invertible and diversity features which enhances the security of the system to a large extent. The proposed approach is very much resistant to minor translation error and rotation distortion. The experimental result shows the better performance of the proposed technique compared to the existing system.

Keywords: *Non-Invertible Gabor Transform, Minutiae, Minucode*

1. Introduction

consistent identity management technique is widely required in order to contest the increased growth in identity theft and to satisfy the increased security needs in a many applications ranging from international border crossings to securing data in databases. Finding the uniqueness of a person is an important process in any identity managing system. Proxy representations of uniqueness like passwords and ID cards are not adequate for trustworthy identity determination since they can be effortlessly misplaced, shared or stolen. Biometric recognition [11, 12] is the science of establishing the identity of an individual with the help of the anatomical and behavioral features. Commonly used biometric features are fingerprint, face, iris, hand geometry, voice, palmprint, handwritten signatures and gait. Biometric features [8] have a number of attractive properties with respect to their use as an authentication token [16], viz., reliability, convenience, universality etc. These features have lead to the wide usage of biometric authentication technique. But there are still some subjects regarding the security of biometric recognition systems that required to be addressed for ensuring the integrity and public acceptance of these systems.

There are five main elements in a general biometric authentication system such as sensor, feature extractor, template database, matcher and decision module. Sensor is the interface between the user and the authentication system and it is used to scan the biometric feature of the individual. Feature extraction phase processes the scanned biometric trait to dig out the significant data (feature set) that is helpful in differentiation of various users. Sometimes the feature extractor is performed after the quality assessment phase that judges whether the scanned biometric trait is of adequate quality for future processing. When the enrollment phase is performed, the extracted feature set is stored in a database as a template (X_T) [6] along with the user's individuality data. As the template database can be physically distributed and enclose millions of records, preserving its security is not a minor work. The matcher module is generally an executable program that accepts two biometric feature sets X_T and X_Q (from template and query, respectively) as inputs and outputs a match score (S) which represents the matching between the two sets. At last, the decision phase suggests the identity conclusion and reply to the query.

Because of the fast growth in sensing and computing techniques, biometric systems have evolved to be reasonable and are effortlessly embedded in a various consumer devices and making this technology weaker for the malicious designs of terrorists and thefts. To avoid any possible security breaks, vulnerabilities of the biometric system must be found and addressed thoroughly. Several studies have analyzed possible security violations in a biometric system and existing techniques to handle those violations. Recognized techniques of vulnerability analysis like attack trees have also been helpful in examining how biometric system security can be compromised.

This paper provides better solution to this problem. In this paper, initially the features are extracted from the fingerprint. Then the secure template is obtained from these features with the help of non-invertible transform called Non-Invertible Gabor Transform [9, 10]. Finally the anonymous matching is performed to identify the authenticated user.

2. Related Work

An Efficient Approach for Non-Invertible Cryptographic Key Generation from Cancelable Fingerprint Biometrics is proposed by Lalithamani *et al.,* [1]. The main drawback of the conventional cryptographic algorithms is the preservation of their key's secrecy. Incorporating the users' biometric features in the generation of strong and repeatable cryptographic keys has gained huge popularity among researchers. The randomness of the user's biometric features, incorporated into the generated cryptographic key, makes the key in order that it cannot be cracked by the attacker lacking noteworthy information of the user's biometrics. However, if a person's biometric is once missed, it will be helpful for the attackers everlastingly as it is naturally belong to the user. To deal with this problem, cancelable biometrics can be used as an effective answer for canceling and re-issuing biometric templates. Here, this paper presents an innovative and efficient technique to create a non-invertible cryptographic key from cancelable fingerprint templates. In the beginning, a one-way transformation is applied on the minutiae points obtained from the fingerprints to accomplish a set of transformed points. Consequently the transformed points are made use of to produce cancelable templates [14, 15]. The cancelable fingerprint templates [7] are then used to create a unique non-invertible key.

Chulhan *et al.,* [2] presents an Alignment-Free Cancelable Fingerprint Templates based on Local Minutiae Information. For every minutia, a rotation and translation invariant value is calculated from the orientation data of neighboring local regions around the minutia [13]. The invariant value is utilized as the input to two changing functions that output two values for the translational and rotational movements of the original minutia correspondingly, in the cancelable template. If a template is compromised, it is modified by a new template generated by various changing functions. The presented technique conserves the original geometric relationships among the enrolled and query templates after their transformation. As a result the transformed templates can be used to identify a person without requiring alignment of the input fingerprint images.

Takahashi *et al.,* [3] put forth a new technique for creating cancelable fingerprint templates with verifiable security based on the well-known chip matching algorithm for fingerprint verification and correlation-invariant random filtering for transforming templates. Ratha *et al.,* [4] demonstrate different techniques to create multiple cancelable identifiers from fingerprint images. A client is given as much biometric identifiers as required by issuing a new transformation key. The identifiers can be cancelled and replaced when cracked by attackers. The performance of various techniques like Cartesian, polar, and surface folding transformations of the minutiae positions are compared.

Huijuan *et al.,* [5] proposed a non-invertible transform approach to perpendicularly project the distances between a pair of minutiae to a circle to create the features. To attain better result, other local features like relative angles between the minutiae pair, and global features like orientation, ridge frequency and total number of minutiae of the randomly sampled blocks around each minutia are also used. The cancelable templates are eventually created by the proposed ldquobin-based quantization (BQ)rdquo. Both feature extraction and cancelable template generation are administrated by a secret key to assure revocability and security.

3. Methodology

This section provides the detailed description of the proposed technique based on the system model shown in Figure1. The proposed Biomapping technique consists of three fundamental procedures: fingerprint feature extraction, noninvertible transform and anonymous matching.

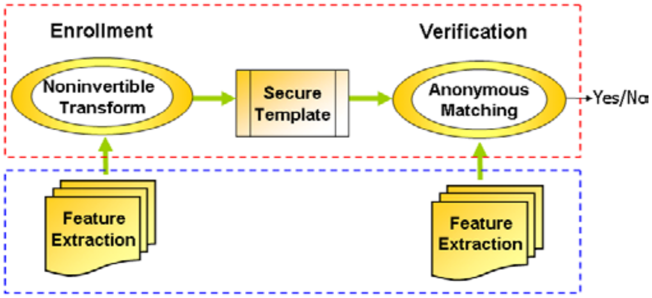
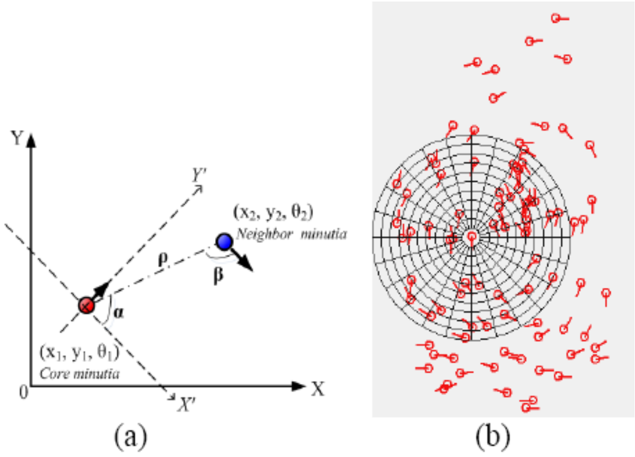


Fig. 1System model for privacy-preserving Biometric Recognition

3.1 Fingerprint feature extraction algorithm

The majority of the existing techniques are based on reference core points of a fingerprint, but, exact evaluation continues to be a complex difficulty and mistakes in the reference core points may led to false reject. To overcome this problem, a minutiae-centered region encoding, MinuCode is used to neglect the reference core point determination and handle with the noise of fingerprint biometrics. The location and orientation attributes of a minutia are used together and these attributes are considered as a 3-tuple (x, y, θ).

Initially, a circular region R is built around every minutia with the similar radius. For every region, the center minutia is taken as the core minutia, and the other minutiae as the neighbor minutiae. Then every neighbor minutia will be transformed into the polar coordinate scheme in accordance with the respective core minutia, and is mentioned as a new 3-tuple (ρ, α, β), where ρ and α represents the radial distance and radial angle respectively, and β indicates the orientation of the neighbor minutia in accordance with the core minutia, α, β∈ [1,360]. An example is provided in Figure 2 (a).



(a) (b)

Fig. 2 Illustration for minutiae-centered region encoding, MinuCode

Next, a tessellation quantification is performed on every one of the neighbor minutiae by tessellate the region of interest middle at the core minutia. After that the 3-tuple (ρ, α, β) in the polar coordinate will be quantified into a rougher 3-tuple T (b, a, o).

$$\begin{cases} b = \left\lfloor \frac{\rho}{db} \right\rfloor \\ a = \left\lfloor \frac{\alpha}{da} \right\rfloor \\ o = \left\lfloor \frac{\beta}{do} \right\rfloor \end{cases} \quad (1)$$

Where $\lfloor / \rfloor$ is an operator to compute the quotient.

In the above equation, the parameter db represents the bandwidth of the region tessellation, da represents the distortion tolerable difference of radial angle, and do represents the distortion tolerable difference of the orientation of the neighbor minutia in accordance with the core minutia. Figure 2(b) illustrates an example of tessellation quantification in a fingerprint. The ith neighbor minutia in accordance with the core minutia in the special region is therefore indicated as the 3-tuple $T_i=(b_i, a_i, o_i)$. If there are m neighbor minutiae in a region R, then, R can be indicated as a set of T:

$$M = < T_1, T_2 \dots . T_m > \quad (2)$$

where the set M is called MinuCode.

Then, if there are N minutiae in a fingerprint, the original fingerprint template can be a gathering of MinuCodes $\{M_1, M_2, \dots, M_N\}$. This gathering is the outcome of the feature extraction process.

3.2 Non-Invertible Transform Algorithms

This approach integrates the feature extraction and the noninvertible transform. This approach uses the Non-invertible Gabor transform.

3.3 Non-Invertible Construction using Non-Invertible Gabor Transform

The feature extraction points of the fingerprint obtained are used for the Non-Invertible construction of the Gabor transform.

The MinuCodes $\{M_1, M_2 \dots M_N\}$ obtained are supplied to the non invertible Gabor transform in which the translation and modulation operations are performed initially.

The primary building blocks of the Gabor representation are the so-called Gabor systems. To describe a Gabor system, let a > 0 and b > 0 be such that ab = q/p with p and q relatively prime, and let T_{ak} and M_{bl}, for k, l ∈ $\mathbb{Z}$, be the translation and modulation operators represented by

$$T_{ak} f(t) = f(t - ak) \quad (3)$$

$$M_{bl} f(t) = e^{2\pi iblt} f(t) \quad (4)$$

For $s \in L^2(\mathbb{R})$, the Gabor system $\mathcal{G}(s,a,b)$ is a collection of$\{M_{bl}T_{ak}s(t);(k,l) \in \mathbb{Z}^2$. The composition

$$M_{bl}T_{ak}f(t) = e^{2\pi ibl t}f(t-ak) \qquad (5)$$

Which is a unitary operator, is called a time-frequency shift operator. Several technical details in time-frequency analysis are connected to the commutation law of the translation and modulation operators, namely

$$M_{bl}T_{ak} = e^{2\pi iabkl}T_{ak}M_{bl} \qquad (6)$$

When p = 1, the time-frequency shift operators commute, i.e. $M_{bl}T_{ak} = T_{ak}M_{bl}$, since $e^{2\pi iabkl} = 1$ for all K, l ∈ $\mathbb{Z}$. One outcome of the commutation rule that is used in the exposition is the relation

$$< f, M_{bl-bn}T_{ak-am}f > = e^{2\pi iab(l-n)m} < M_{bn}T_{am}f, M_{bl}T_{ak}f > \qquad (7)$$

When p = 1 this becomes

$$< f, M_{bl-bn}T_{ak-am}f > =< M_{bn}T_{am}f, M_{bl}T_{ak}f > \qquad (8)$$

For s ∈ $L^2(\mathbb{R})$, the collection $\mathcal{G}(s,a,b)$is a Riesz basis for its closed linear span if there exist bounds A > 0 and B < 1 such that

$$A\|c\|_{\ell^2}^2 \le \left\| \sum_{k,l\in\mathbb{Z}} c_{k,l}M_{bl}T_{ak}s \right\|^2 \le B\|c\|_{\ell^2}^2 \quad c \in \ell^2 \qquad (9)$$

and is a frame when

$$A\|f\|^2 \le \sum_{k,l\in\mathbb{Z}} |< f, M_{bl}T_{ak}s|^2 \le B\|f\|^2 \quad for\ all \quad f \in \overline{span}\ \{M_{bl}T_{ak}s\} \qquad (10)$$

A required condition for $\mathcal{G}(s,a,b)$to comprise a frame for $L^2(\mathbb{R})$ is that ab≤1. In addition if $\mathcal{G}(s,a,b)$is a frame, then it is a Riesz basis for $L^2(\mathbb{R})$ if and only if ab = 1. This paper focus on the regime ab≥1, where $\mathcal{G}(s,a,b)$does not necessarily span $L^2(\mathbb{R})$.

With a Gabor system $\mathcal{G}(s,a,b)$ this paper associate a synthesis operator (or reconstruction operator) $S : \ell^2(\mathbb{Z}^2)$ →$L^2(\mathbb{R})$, defined as

$$S_c = \sum_{k,l\in\mathbb{Z}} c_{k,l}M_{bl}T_{ak}s \qquad (11)$$

$$S_c = \sum_{k,l\in\mathbb{Z}} c_{k,l}M_{bl}T_{ak}s(t) \qquad for\ every\ c \in l^2(\mathbb{Z}^2) \qquad (12)$$

The conjugate $S^*: L^2(\mathbb{R}) \to l^2(\mathbb{Z}^2)$ of S is known as the analysis operator (or sampling operator), and is given by

$$S^*f = \{\langle f, M_{bl}T_{ak}\, s\rangle\} \qquad for\ every\ f \in L^2(\mathbb{R}) \qquad (13)$$

The Gabor representation of a feature contains the set of coefficients $\{C_{k,l}\}_{k,l\in\mathbb{Z}}$ acquired by inner products with the elements of some Gabor system $\mathcal{G}(s,a,b)$.

$$C_{k,l} = \langle f, M_{bl}T_{ak}S\rangle \qquad (14)$$

This procedure can be indicated as an analysis filter-bank. Therefore, s(t) is referred to as the analysis window of the transform. If $\mathcal{G}(s,a,b)$constitutes a frame or Riesz basis for $L^2(\mathbb{R})$, then there exists a function $v(t) \in L^2(\mathbb{R})$such that any $f(t) \in L^2(\mathbb{R})$ can be reconstructed from the coefficients $\{C_{k,l}\}_{k,l\in\mathbb{Z}}$ using the formula

$$f(t) = \sum_{k,l\in\mathbb{Z}} C_{k,l}\, M_{bl}\, T_{ak}v(t) \qquad (15)$$

In this paper, Gabor system is consider that do not essentially span $L^2(\mathbb{R})$ but rather only a (Gabor) subspace. A Gabor space is the set V of all feature that can be represented with some norm-bounded sequence $c_{k,l}$. As perfect recovery cannot be assured for each signal in $L^2(\mathbb{R})$in these cases, the choice of selecting the analysis and synthesis windows based on the implementation constraints. Conversely, for the purpose of analysis and synthesis processes to be stable, it is assured that the systems $\mathcal{G}(s,a,b)$and $\mathcal{G}(v,a,b)$form frames or Riesz bases for their span.

For tractability, it is assumed that, a and b are positive constants such that ab = q/p, where p and q are relatively prime. In addition, only Gabor spaces are considered whose generators are obtained from the so-called Feichtinger algebra S_0, which is defined by

$$S_0 = \left\{ f \in L^2(\mathbb{R}) \middle| \|f\|S_0 := \int |\langle f, M_\omega T_x\psi\rangle| dx\, d\omega < \infty \right\} \qquad (16)$$

where $\psi(t)$ represents the Gaussian window. An important possessions of S_0 is that if v(t) and s(t) are elements from S_0 then $\{\langle v, M_{bl}T_{ak}s\rangle\}_{k,l\in\mathbb{Z}}$ is an $\ell^1(\mathbb{Z}^2)$ sequence. Examples of functions in S_0 are the Gaussian and B-splines of strictly positive order. The Feichtinger algebra is an tremendously helpful space of good window functions in the sense of time-frequency localization.

The final secure template of a fingerprint will be a collection of transformed MinuCodes {M'$_1$, M'$_2$,…, M'$_N$}. N is the number of minutiae in the fingerprint.

3.4 Anonymous matching algorithm

The minutia point arrangement process can be divided into two phase. Initially, Biomapping handles the alignment errors in the minutia location and orientation with the help of minutiae-centered quotient computation and tessellation quantification: provided a transformed MinuCode from the secure template and an original MinuCode from query fingerprint, two neighbor minutiae are considered to be matched only if the MinuCode identified after Non-Invertible Gabor Transform are identical.

In the next phase, the threshold mechanisms are used to deal with the replacement errors that carry with the elimination and adding of a few minutiae. Two thresholds tm and tp are used for the anonymous matching: two regions are similar if there are minimum of tm equal neighbor minutiae. At last, two fingerprints are considered to be matched if there are at least tp equal regions.

4. Experimental Result

The experimental result for the proposed biometric system is presented in this section. The experiments are conducted with the help of public domain FVC2002-DB2 database. The database contains 100 fingers, each one has 8 impressions. The first two impressions of every finger are used in this experimentation. As a result, the number of genuine attempts is 100, and the number of the impostor attempts is 9900.

Table 1: FRR and FAR Resulted for the Existing and Proposed Biometric System

Region	Existing		Proposed	
Threshold (tp)	FRR	FAR	FRR	FAR
0	0	98.3	0	80.6
5	4.2	20.5	0	5.2
10	12.1	10.2	4.5	0
15	28.9	4.2	10.2	0
20	40.3	1.1	20.5	0
25	52.1	0	30.9	0
30	60.7	0	38.1	0
35	74.5	0	42.6	0
40	80.3	0	49.9	0
45	88.1	0	55.2	0

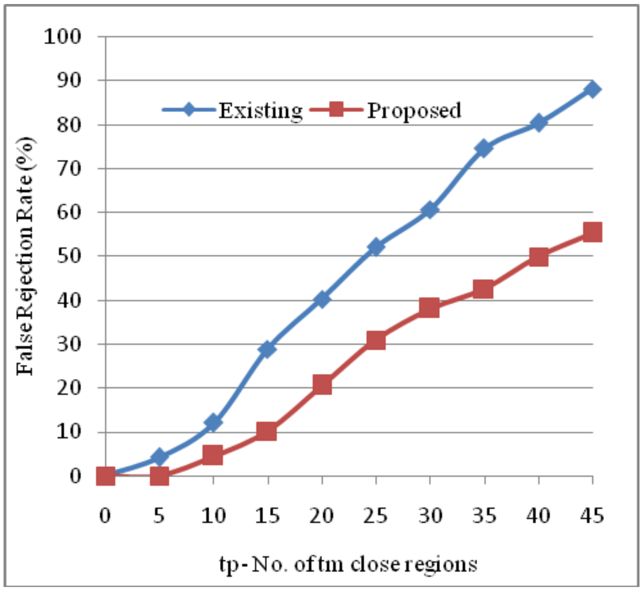


Fig. 3 False Rejection Rate for Different Threshold

Table 1 provides the obtained False Rejection Rate (FRR) and False Acceptance Rate (FAR) for the various region thresholds. It can be clearly observed from the table that initially for the region threshold of 0, the FRR is 0 for both techniques. When the threshold value is increased, the FRR will gradually increase. When the threshold is 15, FRR is 28.9 for the existing method, whereas it is only 10.2 for the proposed technique. When the threshold is set as 45, FRR is 88.1 for the existing method, whereas it is only 55.2 for the proposed technique which is a huge difference. When FAR is considered, the proposed technique will have 0 FAR when the threshold is set above 10, whereas for the existing technique the threshold should be set above 20.

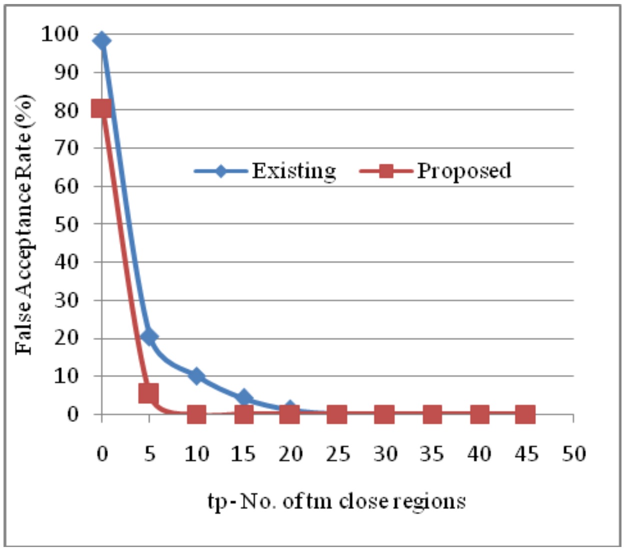


Fig. 4 False Acceptance Rate for Different Threshold

Fig. 3 and Fig. 4 shows the variations in FRR and FAR for various region thresholds respectively. It can be clearly observed that the proposed technique will result in lesser FRR and FAR when compared to the existing biometric system.

5. Conclusion

Biometrics provides easy usability over earlier token and password based authentication techniques, but raises privacy and security concerns. The earlier authentication techniques like credit cards and passwords can be revoked or substituted if it is not handled properly but biometrics is everlastingly linked with a user and cannot be substituted. Cancelable biometrics is helpful to overcome this by generating revocable biometric templates. In this paper, the secure template is obtained from these features with the help of non-invertible transform called Non-Invertible Gabor Transform. The experimental result shows that the proposed biometric system results in better FRR and FAR which in turn indicates the better accuracy and security than the existing biometric system.

This biometric system thus provides a good improvement over the other techniques which are based purely on biometric feature extraction and complex classifier. This approach can be enhanced to higher level in order to further improve the security. This work can be extended in future by using the highly secure non invertible transform such as Baker Non-Invertible Transform. The usage of this Baker Non-Invertible Transform will result in strong mixing of feature points and it will be very hard to break by the attackers and thus it can provide better security.

Moreover, the future enhancement will address the practical issues of the latency for recognition and the size of the secure template.

References

[1] Chulhan Lee, Jeung-Yoon Choi, Kar-Ann Toh and Sangyoun Lee, "Alignment-Free Cancelable Fingerprint Templates Based on Local Minutiae Information", IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, Vol. 37, No. 4, 2007.

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

[3] Jain, A.K., Nandakumar, K. and Nagar, A., "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, Special Issue on ASPPRMB, Vol. 2008, Pp.1-17, 2008.

[4] Andrew Teoh, B.J. and David Ngo, C.L., “Cancellable Biometrics Featuring with Tokenised Random Number”, Pattern Recognition Letter, Vol. 26, No. 10, Pp. 1454–1460, 2005.

[5] Daugman, J.G., “Complete Discrete 2D Gabor Transform by Neural Networks for Image Analysis and Compression”, IEEE Transaction on Acoustic Speech and Signal Processing, Vol. 36, No. 7, Pp. 1169-1179, 1988.

[6] Dunn, D., Higgins, W. E., “Optimal Gabor Filters for Texture Segmentation,” IEEE Transaction on Image Processing, Vol. 4, No. 7, Jul. 1995.

[7] Jain, A.K., Ross, A. and Pankanti S., “Biometrics: A Tool for Information Security,” IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, 2006.

[8] Ross, A.K., Shah, J. and Jain, A.K., “From Templates to Images: Reconstructing Fingerprints from Minutiae Points,” IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 4, Pp. 544–560, 2007.

[9] Cappelli, R., Lumini, A., Maio, D. and Maltoni, D., “Fingerprint Image Reconstruction from Standard Templates,” IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 9, Pp. 1489–1503, 2007.

[10] Lalithamani, N. and Soman, K.P., "An Efficient Approach for Non-Invertible Cryptographic Key Generation from Cancelable Fingerprint Biometrics", International Conference on Advances in Recent Technologies in Communication and Computing, Pp. 47-52, 2009.

[11] Takahashi, K. and Hitachi, S.H.,"Generating Provably Secure Cancelable Fingerprint Templates based on Correlation-Invariant Random Filtering", IEEE 3rd International Conference on Theory, Applications, and Systems, Pp. 1-6, 2009.

[12] Huijuan Yang, Xudong Jiang and Kot, A.C., "Generating Secure Cancelable Fingerprint Templates Using Local and Global Features", 2nd IEEE International Conference on Computer Science and Information Technology, Pp. 645-649, 2009.

[13] Weicheng, S., Surette, M. and Khanna, R., “Evaluation of Automated Biometrics-Based Identification and Verification Systems”, Proceedings of the IEEE, Vol. 85, No.9, Pp. 1464-1478, 1997.

[14] Jain, A.K., Ross, A. and Uludag, U., “Biometric Template Security: Challenges and Solutions,” Proceedings of European Signal Processing Conference (EUSIPCO), 2005.

[15]Boult, T.E., Scheirer, W.J. and Woodworth, R., “Fingerprint Revocable Biotokens: Accuracy and Security Analysis,” Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Pp. 1–8, 2007.

[16]Ratha, N.K., Connell. J.H. and Bolle, R.M., “An Analysis of Minutiae Matching Strength,” Proceedings of Third International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), 2001, Pp. 223–228, 2001.

First Author

Mrs.N.Radha received M.Sc(Computer Science) in Madurai Kamaraj University and completed M.Phil (Computer Science in bharathiar University,India. Currently she is pursuing her Ph.D. (Computer Science) in Karpagam University, India. She had 14 years of teaching experience. At present she is working in PSGR Krishnammal College for women. She presented papers in Various International and National Journals. Her areas of interests are Information security, Biometric security and oops. She has published more than 10 papers in various National and International Journals.

Second Author:

Dr.Karthikeyan completed M.Sc (Computer Science) in Bharathidasan university in the year 1996.He has done M.Phil(Computer Science) in Bharathiar University in the year 2003 and he completed Ph.D (Computer science) in Alagappa university in the year 2008.He has 15 years of teaching experience hold various positions . Now he is working as an Assistant Professor in College of Applied Sciences, Sultanate of Oman. His areas of interests are Cryptography and Network Security - Security Protocols, Key Management and Encryption Techniques. He is Guiding 16 M.phil scholars and 6 Ph.D scholars. He has published and presented more than 50 papers in various National, International and conference and journals. He served as Reviewer, editor in Chief, Associate editor, Technical editor, Editorial Board member and Guest editor in various National and International Journals. He got senior Membership in IACSIT, Singapore and ACEEE, India. He got membership in CSTA, New York, USA and in International Association of Engineers – Computer Science/Wireless Networks, Canada/Spain.