`

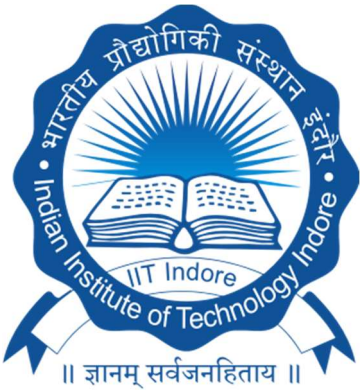
B. TECH. PROJECT REPORT

On

Cancelable Fingerprint Biometrics

BY

Piyush Verma



DISCIPLINE OF COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY INDORE

December 2016

`

CANCELABLE FINGERPRINT BIOMETRICS

A PROJECT REPORT

Submitted in partial fulfillment of the requirements for the award of the degrees

of
BACHELOR OF TECHNOLOGY
in

COMPUTER SCIENCE AND ENGINEERING

Submitted by:
Piyush Verma

Guided by:
Dr. Somnath Dey, Assistant Professor

`

INDIAN INSTITUTE OF TECHNOLOGY INDORE
December 2016
CANDIDATE'S DECLARATION

I hereby declare that the project entitled **"Cancellable Fingerprint Biometrics"** submitted in partial fulfillment for the award of the degree of Bachelor of Technology in 'Computer Science And Technology' completed under the supervision of **Dr. Somnath Dey, Assistant Professor ,** IIT Indore is an authentic work.

Further, I declare that I have not submitted this work for the award of any other degree elsewhere.

Signature and name of the student(s) with date

CERTIFICATE by BTP Guide(s)

It is certified that the above statement made by the students is correct to the best of my/our knowledge.

Signature of BTP Guide(s) with dates and their designation

`

Preface

This report on “Cancellable Biometrics" is prepared under the guidance of Dr. Somnath Dey.

This report intends to give a detailed design and analysis of a cancellable biometric protection technique, specifically a cancelable fingerprint protection technique called Protected-MCC. Furthermore, this report attempts to clearly explain the enhancements applied to the existing technique to reduce the complexity of the technique and compares the result to some well-known techniques in the literature.

Piyush Verma
B.Tech. IV Year
Discipline of Computer Science and Technology
IIT Indore

`

Acknowledgements

I thank Dr. Somnath Dey for his kind support and valuable guidance. It is his help and support, due to which I became able to complete the design and technical report. I also thank Mr. Rudresh Dwivedi for helping me on the concerned topics.

Without their support, this report would not have been possible.

Piyush Verma
B.Tech. IV Year
Discipline of Computer Science and Technology
IIT Indore

`

List of Figures

List of Tables

`

Table of Contents

`

1. Abstract

A person's physiological or behavioral characteristics, known as biometrics, are important and vital methods that can be used for identification and verification. Although several fingerprint template protection methods have been proposed in the literature, the problem is still unsolved, since enforcing non-reversibility tends to produce an excessive drop in accuracy. In this report, a novel protection technique for Minutia Cylinder-Code (MCC) which is a well-known local minutiae representation, called P-MCC is implemented and tested on a FVC2002 DB1 dataset. Experimental evaluation have shown that the method fulfills the requirements of a cancelable biometric construct; it is non-invertible, revocable which MCC failed to deliver. Moreover, the method outperforms the state-of-the-art methods, and also the original approach in terms of accuracy as well as protection against attacks.

`

2. Introduction

A person's physiological or behavioral characteristics, known as biometrics, are important and vital methods that can be used for identification and verification. *Biometric recognition* (or simply biometrics) refers to the use of distinctive *anatomical* (e.g., fingerprints, face, iris) and *behavioral* (e.g., speech) characteristics, called *biometric identifiers* or *traits* or *characteristics* for automatically recognizing individuals [1]. Biometrics is becoming an essential component of effective person identification because biometric identifiers cannot be shared or misplaced, and they are intrinsically linked to the individual's identity. Therefore biometric based identification forms a very powerful tool for identity management with tremendous potential consequences, both positive and negative. Consequently, biometrics is not only a fascinating pattern recognition research problem but, if carefully used, is an enabling technology with the potential to make our society safer, reduce fraud and provide user convenience (user-friendly man–machine interface). Biometrics-based authentication systems offer obvious usability advantages over traditional password and token-based authentication schemes. However, biometrics raises several privacy concerns. A biometric trait is permanently associated with a user and cannot be changed. Hence, if a biometric identifier is compromised, it is lost forever and possibly for every application where the biometric is used. Moreover, if the same biometric is used in multiple applications, a user can potentially be tracked from one application to the next by cross-matching biometric databases. Hence, template protection techniques have gained increasing interest in the biometric community.

`

In general, template protection methods are designed to guarantee:

i. **Irreversibility:** the infeasibility to reconstruct the original pattern from the protected template,
ii. **Diversity:** the property to derive different protected templates from the original protected template,
iii. **Accuracy:** the preservation of the recognition accuracy when the matching is carried out on protected templates, and
iv. **Revocability:** the possibility to revoke a compromised template and reissue a new one based on the same biometric data.

Fingerprint recognition is one of the most popular biometric techniques used in automatic personal identification and verification. Most fingerprint matching systems are based on four types of fingerprint representation schemes: (a) grayscale image, (b) phase image, (c) skeleton image, and (d) minutiae (Figure 1). The minutiae-based representation has become the most widely adopted fingerprint representation scheme.

(a) Grayscale image (b) Phase image (c) Skeleton image (d) Minutiae

Figure 1: Fingerprint representation scheme [2]

`

Minutiae constitute the two most prominent local ridge characteristics, **ridge ending**: the point where a ridge ends abruptly and **ridge bifurcation**: the point where a ridge forks or diverges into branch ridges (Figure 2).

(a) Ridge bifurcation (b) Ridge ending

Figure 2: Two commonly used fingerprint features[3]

Each of the *ridge endings* and *ridge bifurcations* types of minutiae has three attributes, namely, the x-coordinate, the y-coordinate, and the local ridge direction *(θ)* (Figure3).

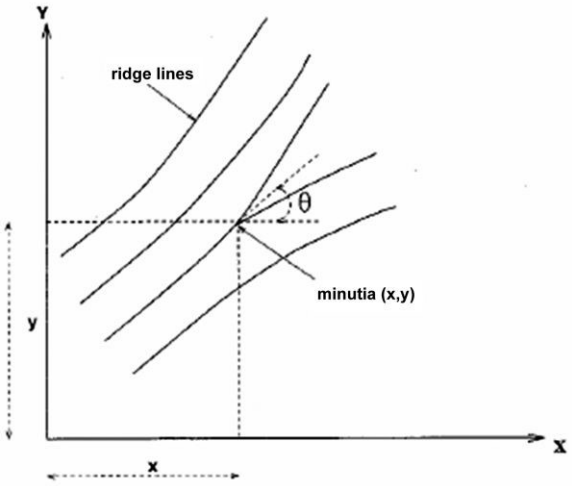


Figure 3: Components of a minutiae feature[4]

`

But Fingerprint Matching is considered an extremely difficult problem facing issues like displacement, rotation, distortion, noise (dirt on the sensor), pressure and skin conditions like dryness, disease, sweat, dirt, grease, humidity at the time of fingerprint acquisition that is used for matching. The major approaches for fingerprint matching are: the ***Correlation-based*** matching that superimposes images and compares pixels, the ***Ridge Feature-based*** matching that compares the structures of the ridges and the features extracted from them like local orientation and frequency, ridge shape, texture information etc. and the **most widely used** approach, the ***Minutiae-based*** matching that compares the extracted minutiae. The approach described in this report, P-MCC also uses a minutiae-only local representation called Minutiae Cylinder Code (MCC) and the subsequent matching is done by features derived from the minutiae points.

3. Literature Review.

There are several protection techniques present in the literature but the problem of achieving high accuracy with a sophisticated protection scheme is still unsolved with each of these techniques having their respective advantages and drawbacks.

Kumar Et al. **[5]** proposed a mapping strategy for combining multiple hash functions based on certain triplets or k-plets features. In the case of triplets, such features could be angles formed by the triplets, their sides or a combination of altitude and base. The triplets were then binned on basis of one of these features and map specific hash function to each bin. Therefore each bin acted as the key for the choice of the hash function. Hence for the mapping of a bin to a specific hash function, a random seed is utilized. However, a high EER is a major limitation of this method.

`

Zhe and Jin **[6]** proposed a scheme where a minutia vicinity set was first constructed and each of the minutiae vicinity was then decomposed into four minutia triplets. Then, a set of randomized geometric invariant features were derived from the minutia triplets and stored as a template. In particular, for a set of N fingerprint minutia, $\{m_i \mid i = 1, \ldots, N\}$, a minutia vicinity V_i is defined as m_i together with 3 nearest (measured in terms of Euclidean distance) neighboring minutiae c_{i1}, c_{i2}, c_{i3}, i.e. $V_i = \{m_i, c_{i1}, c_{i2}, c_{i3} \mid i = 1, \ldots, N\}$. Each of the minutia vicinity was decomposed into four minutia triplets $\{T_{ir} \mid i = 1, \ldots, N, r = 1, 2, 3, 4\}$

Hence, a feature vector, u_r which consists of nine features could be formed as follows:

$$u_r = (s_1, \alpha_1, \Delta o_1, s_2, \alpha_2, \Delta o_2, s_3, \alpha_3, \Delta o_3)$$

where r = 1,…,4 ; $\Delta o_1 = |o_1 - o_2|$; $\Delta o_2 = |o_2 - o_3|$; $\Delta o_3 = |o_3 - o_1|$ and s1, s2 and s3 denote the length of the three sides in pixel; α1, α2 and α3 represent the internal angles measured in degree; Δo denotes the relative orientation between two adjacent minutiae and o_1, o_2, o_3 are the orientation for minutiae m_1, m_2, m_3 respectively. In order to achieve revocability, they adopted a biometric salting technique by adding a user-specific random matrix, R which was stored in the token. In the event of a template being lost or compromised, the new one could be re-issued by using different random matrix. However, the MVD features are highly likely to reveal the minutia vicinity, e.g., four minutiae triangles after decomposition **[7]** which makes it a weak protection template.

Krivokuća Et al. **[8]** proposed a fingerprint construct consisting of a single pattern created from a small subset of minutiae from the corresponding minutiae template. A pattern consisted of a few minutiae connected in a particular order via straight lines. There were two constraints on the types of patterns that might be formed. Firstly, each node must have exactly one line entering it and one line exiting from it, such that the latter line immediately follows the former line. Secondly, the pattern must form a closed shape, which means that the last line must finish at the first node. A pattern that consisted of N minutiae was referred to as an N-node pattern, and was described by two sets of features: local features and global features. The local feature set characterized the shape of the pattern, while the global feature set represented both the location and orientation of the pattern relative to the fingerprint core. The local features included:

`

- l_{ij}: The length of the connection line from minutia m_i to minutia m_j, which is the Euclidean distance between the locations of mi and mj. (i = 1, 2, …, N and j = 2, …, N, 1).
- α_{ij} and β_{ij}: Let φ_{ij} denote the angle of the connection line from minutia mi to minutia mj. Further, let θ_i and θ_j represent the orientations of minutiae mi and mj, respectively. (φ_{ij}, θ_i and θ_j all increase in the clockwise direction from the horizontal and lie in the range [0°, 360°)). Then, α_{ij} is the angle difference between φ_{ij} and θ_i, and β_{ij} is the angle difference between φ_{ij} and θ_j.

Global features of the pattern included the coordinates depicting the location of the pattern centroid relative to the core: (x, y) and the pattern orientation ω. The major drawback of this approach was its fairly high computational complexity in global consolidation.

Ahmad and Han **[9]** devised another cancelable fingerprint template scheme based on local features. The proposed scheme utilized the minutiae information only and the minutiae were transformed using Cartesian and Polar Transformations. As it did not utilize any singular point, each minutia point was used as the reference to the transformation which was performed in both Cartesian and polar coordinate systems. This transformation could be denoted as:

$$BS_p = f_2\left(f_1\left(BS_{up}\right)\right)$$

where BS_p, f_1 and f_2 are the transformed (protected) fingerprint template, transformation function in Cartesian and polar coordinate spaces, respectively. This function needs a set of keys κ, which comprise κrot and $\{\kappa rad, \kappa\alpha, \kappa\beta\}$ for Cartesian and Polar transformations, respectively. All of those keys can be derived from hashed pass phrases, so, it is most possibly random. In the verification step, the fingerprint query is extracted and transformed in the same way as what has been done to the fingerprint template. The algorithm in **[10]** was used for matching (verification).The non-reversibility in this technique was by the secrecy of the key rather than by the transformation itself.

`

4. Motivations and Objectives.

Although several fingerprint template protection methods have been proposed in the literature, the problem is still unsolved. Matching fingerprints based only on local minutiae arrangements relaxes global spatial relationships, which are highly distinctive, and therefore reduces the amount of information available for discriminating fingerprints. Few approaches which require the global minutiae matching algorithms are computationally demanding and lack robustness with respect to nonlinear fingerprint distortion. Also, most of the proposed non-invertible transforms have a fairly low non-reversibility degree; in fact, only a few minutiae (about 8%) have their neighbors perturbed by these transformations **[1]**. In conclusion, although the approach achieves a high matching accuracy, the level of non-reversibility provided is quite limited. Enforcing non-reversibility tends to produce an excessive drop in accuracy. Furthermore, unlike fingerprint verification, whose performance is assessed today with public benchmarks and protocols, the performance of template protection approaches is often evaluated in heterogeneous scenarios, thus making it very difficult to compare existing techniques.

Hence, a minutiae-only local representation aimed at combining the use of both local and global similarities for matching is required. Most of the fingerprint matching algorithms recently proposed exploit several extra features besides minutiae; minutiae-only templates also allow us to compress into a few hundred bytes the salient fingerprint information, thus enabling their storage on inexpensive smart cards. There is a need for accurate and interoperable minutiae-only algorithms. Here, the main objective is to generate a Protected Fingerprint Verification Template that uses a Transformation Function using the minutiae-only MCC Representation **[11]**.

`

5. Proposed Technique

Minutia Cylinder-Code Representation (MCC) is one of the most effective local minutia descriptors for fingerprint recognition. The template protection scheme described in this report has been specifically designed to benefit from the MCC representation by further adding to the security of the MCC template.

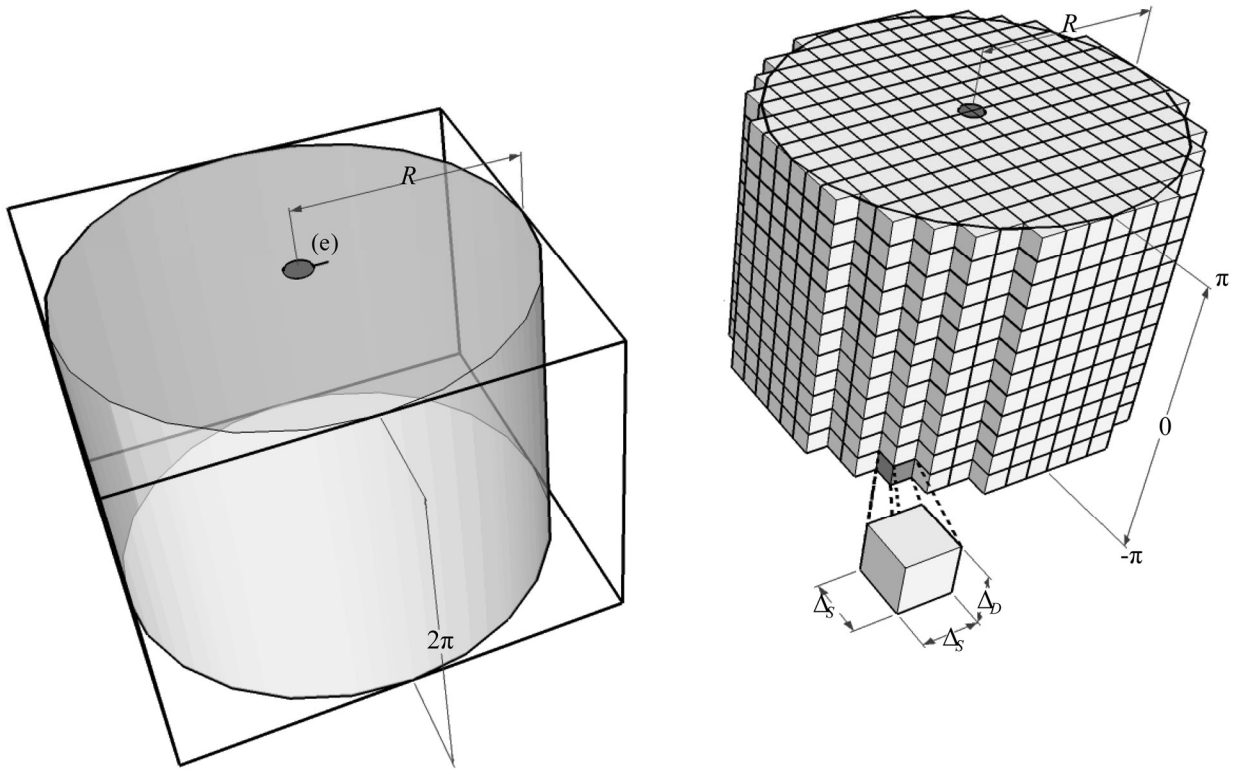
5.1. The Local Structure.

The Minutia Cylinder-Code representation (MCC) associates a local descriptor to each minutia m: this descriptor encodes spatial and directional relationships between the minutia and its neighborhood of radius R, and can be conveniently represented as a cylinder, whose base and height are related to the spatial and directional information, respectively.

5.2. The Cylinder of a Minutiae.

The cylinder is divided into sections: each section corresponds to a directional difference in the range $[-\pi, \pi]$; sections are divided into cells. The cylinder is enclosed inside a cuboid whose base is aligned according to the minutia direction θ_m ; the cuboid is discretized into $N_C = N_S \times N_S \times N_D$ cells. Each cell is a small cuboid with ΔS base and ΔD height, where $\Delta S = 2 \cdot R / N_S$ and $\Delta D = 2 \cdot \pi / N_D$ (Figure 4).

`



(a) The cylinder with the enclosing cuboid (b) The discretization of the cuboid into cells

Figure 4: A graphical representation of the local structure associated to a given minutia **[10]**

5.3. The Cell Values.

During the creation of a cylinder, a numerical value is calculated for each cell, by accumulating contributions from minutiae in a neighborhood of the projection of the cell center onto the cylinder base. The contribution of each minutia m_t to a cell (of the cylinder corresponding to a given minutia m), depends both on: the Spatial Information (how much m_t is close to the center of the cell), and the Directional Information (how much the directional difference between m_t and m is similar to the directional difference associated to the section where the cell lies). In other words, the value of a cell represents the likelihood of finding minutiae that are close to the cell and whose directional difference with respect to m is similar to a given value.

`

5.4. The Cylinder-Set.

Given a template *T, MCC* creates a cylinder set *(CS)*, which contains the cylinders associated to all minutiae in *T* with a sufficient number of neighbors. Each cylinder is a local descriptor:

• *Invariant for translation and rotation, since i) it only encodes distances and directional differences between minutiae, and ii) its base is rotated according to the corresponding minutia direction;*

• *Robust against skin distortion (which is small at a local level) and against small feature extraction errors, due to the smoothed nature of the functions defining the contribution of each minutia;*

• *With a fixed-length given by the total number of cells in the cylinder.*

Also, each cylinder in the Cylinder-Set can be treated as a feature vector $v_m \epsilon [0, 1]^n$ obtained by linearizing the cells of the cylinder C_m corresponding to a given minutia *m*. Hence, from a template *T*, a set of feature vectors *V* can be derived:

$V = \{v_m \mid v_m$ obtained from $C_m, C_m \epsilon CS\}$

Where v_m is the feature vector obtained from the cylinder of minutia *m* and *CS* is the cylinder set of template *T*. Hence, the similarity between two cylinders can be simply defined using a vector correlation measure. The similarity is always in the range [0, 1]; zero means no similarity and one denotes maximum similarity.

`

5.5. P-MCC

The MCC structures **[10]** are provided protection using a non-invertible function based on dimensionality reduction and binarization. The resulting protection scheme is called P-MCC. The procedural steps are described in the block diagram in Figure 5. The non-invertible transform consists of a KL projection [11] followed by a binarization step: in the following, it is referred to as Binary-KL (B-KL).

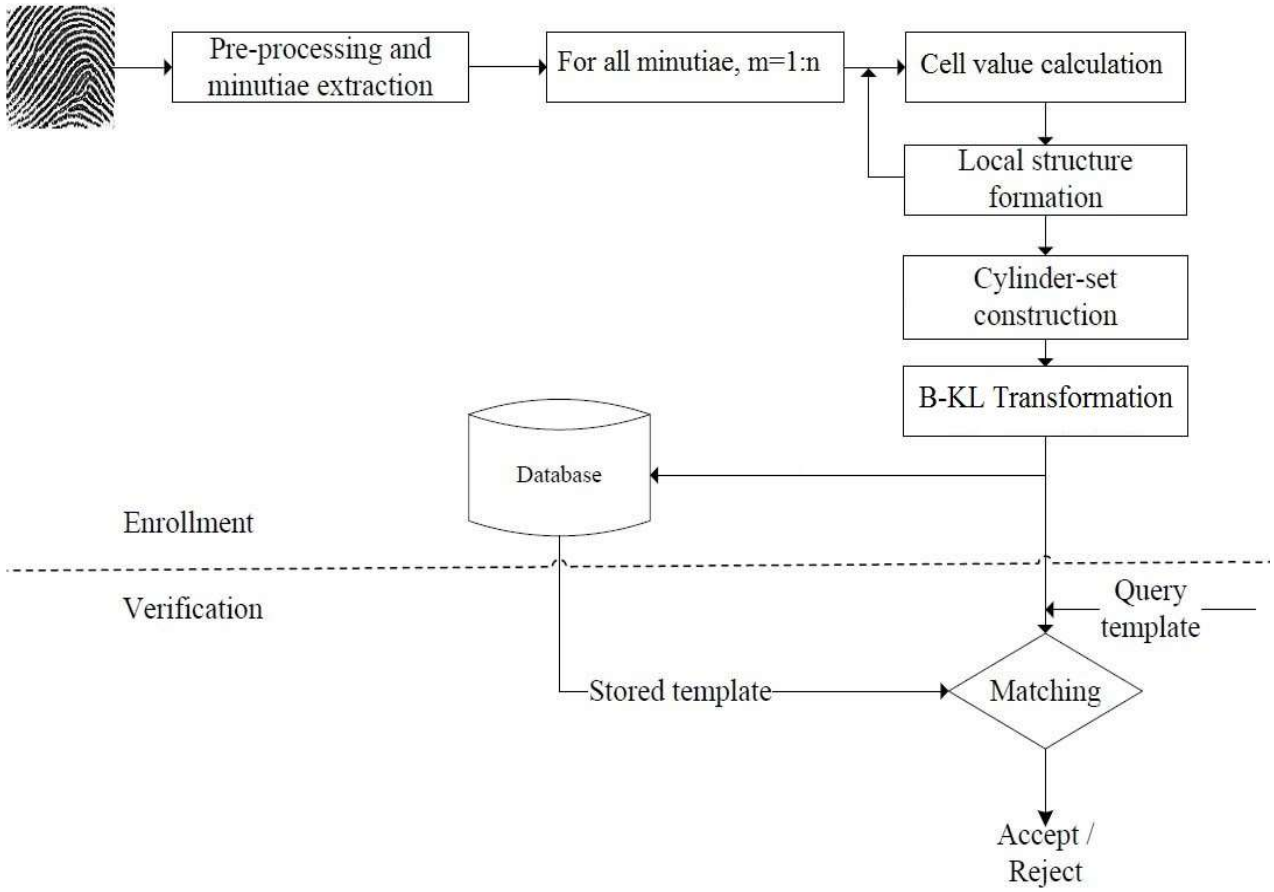


Figure 5: Fingerprint Verification using P-MCC

`

5.6. The Transformation Function

The non-invertible transform $T_k : [0,1]^n \rightarrow \{0,1\}^n$ encodes the feature vector v_n into a k-dimension binary space. It is defined as:

$$T_k(v_n) = \overrightarrow{B - KL}(v_n, \bar{x}, \Phi_k)$$

And $\overrightarrow{B - KL}(v_n, \bar{x}, \Phi_k) = \mathrm{B}(v_n, \bar{x}, \Phi_k)$

Where $B(y) = [H(y_1), H(y_2), \dots, H(y_k)]$

Binarizes each element of vector $y = [y_1, y_2, \dots, y_k]$

By a unit step function $H: R \rightarrow \{0,1\}$

$$H(v) = \begin{cases} 1, & v \geq 0 \\ 0, & v < 0 \end{cases}$$

5.7. The B-KL Parameters

$\bar{x}\ and\ \Phi_k$ are known as the B-KL Parameters.

Let P be the matrix containing the MCC feature vectors of a fingerprint, then $\bar{x}$ is the mean vector of P and, Φ_k is the matrix whose columns are the eigenvectors corresponding to the k largest eigenvalues of the covariance matrix C of P.

`

5.8. Cylinder Noninvertible Transform

Given the feature vector $v_m$obtained from a cylinderC_m, and the B-KL parameters $\bar{x}$ and Φ_k , the noninvertible transform encodes v_m into a k dimensional binary space. $\bar{x}$ and Φ_k can be computed offline starting from a generic dataset of fingerprint images. Then, given the set of feature vectors derived from a minutiae template *V*, the protected template is a set of bit vectors defined as:

$$\widetilde{V} = \{\widetilde{v_m} \mid \widetilde{v_m} = T_k(v_m); v_m \in V\}$$

5.9. Similarity between Two Protected Cylinders

The similarity between two protected bit vectors v_a and v_b is computed as:

$$\gamma(\widetilde{v_a}, \widetilde{v_b}) = 1 - \left\| \widetilde{v_a} \; XOR \, \widetilde{v_b} \right\|_1 / \mathrm{k}$$

Where XOR denotes the bitwise exclusive-or between two-bit vectors, $\| \, . \, \|_1$ represents the 1-norm, and k the length of the bit vectors. The similarity $\gamma(\widetilde{v_a}, \widetilde{v_b})$ is always in the range [0,1] , where zero means no similarity and one maximum similarity.

`

5.10. The Similarity between Two Protected Templates

In order to compare two protected templates, a single value denoting their overall similarity has to be obtained from the local similarities between protected bit-vectors. Given two protected templates $\widetilde{V_A}$ and $\widetilde{V_B}$, the global score is calculated as the average of the bit-vector pairs with the largest similarity, but discarding pairs that contain at least a bit-vector already selected. The value of $n_P$is not an overall constant, but partially depends on the number of bit-vectors in the two templates:

$$n_P = min_{n_P} + \left\lfloor max_{n_P} - min_{n_P} / \left(1 + e^{-\tau_P (min\{|\widetilde{V_A}|, |\widetilde{V_B}|\} - \mu_P)}\right)\right\rfloor$$

Where τ_P, $\mu_P, max_{n_P}, min_{n_P}$ are parameters, and $\lfloor . \rfloor$ denotes the rounding operator.

6. Performance Evaluation

The experiment was conducted on a publicly available fingerprint database FVC 2002 DB1 since most of the published approaches on fingerprint template protection utilized FVC datasets. Each set of the first three databases comprises of 100 subjects with 8 images per subject. The P-MCC was programmed and executed in Matlab R2014a with K = 64. Three performance metrics are used to evaluate the performance of the method:

- FMR: The probability of mistakenly accepting an imposter as a genuine user.
- FNMR: The probability of mistakenly rejecting a genuine user as an imposter.
- EER: The error rate where FMR and FNMR hold equality.

The computation of these performance metrics involve the evaluation of genuine scores and imposter scores. Genuine score refers to the matching a fingerprint impression of a subject with

`

the other impressions of the same subject, while imposter score is derived by comparing a fingerprint impression of each subject against the fingerprint impressions of all other subjects. Also, standard FVC protocol is used to compute the performance of the method. In the FVC protocol, each fingerprint image of a subject is matched with the remaining fingerprint images of the same subject to compute the FNMR. To evaluate the FMR, the first fingerprint image of each subject is matched with the first fingerprint image of the different subject. This results in providing ${}^{8}C_{2}$*100 = 2800 genuine scores and ${}^{100}C_{2}$ = 4950 imposter scores for the FVC2002 DB1 database. Different values of threshold are applied to compute the FMR and FNMR. The results are provided in Table 1. Table 1 shows that FMR declines with the increase in the threshold value while FNMR exhibits the opposite tendency; it increases as the threshold is increased.

Threshold Value	FMR	FNMR
0.05	1	0
0.1	1	0
0.15	0.998384	0
0.2	0.968889	0
0.25	0.864848	0
0.3	0.682424	0.000357
0.35	0.443232	0.001071
0.4	0.186263	0.007857
0.45	0.049899	0.023571
0.5	0.005051	0.061071
0.55	0.000202	0.132857
0.6	0	0.236429
0.65	0	0.41
0.7	0	0.802857
0.75	0	0.994643
0.8	0	1

Table 1 : FMR & FNMR Values for Progressive Threshold Values

`

- The FMR_{1000} was calculated to be 6.824 percent.
- The $ZERO_{FMR}$ was calculated to be 8.648 percent.
- The EER was calculated to be 3.56 percent.

The approaches in [1, 2, 3] used FVC 2002 database to evaluate the performance of their method using standard FVC protocol. Therefore, we compare our method with these approaches [1, 2, 3] in the literature. Table 2 summarizes the results of the comparison in terms of EER, FMR and FNMR on FVC 2002 database for FVC protocol. Therefore, from the reported results it is evident that our approach performs better over the existing approaches.

Method	**EER (%)**	**FMR_{1000} (%)**	**$ZERO_{FMR}$ (%)**
P-MCC_{64}	3.56	6.824	8.648
P-MCC_{64} (Original)	3.33	6.54	8.11
Kumar Et al. [5]	10.4	-	-
Zhe and Jin [6]	7.38	-	-
Krivokućа Et al. [8]	-	9.5	-
Ahmad and Han [9]	6.8	-	-

Table 2 : Result Comparison
('-' represents authors have not reported the results for FVC2002 DB1 dataset.)

`

The ROC curves for FVC2002 DB1 dataset are shown in Figure 6. It is clearly visible that FMR declines with the increase in threshold while FNMR increases with increasing threshold.

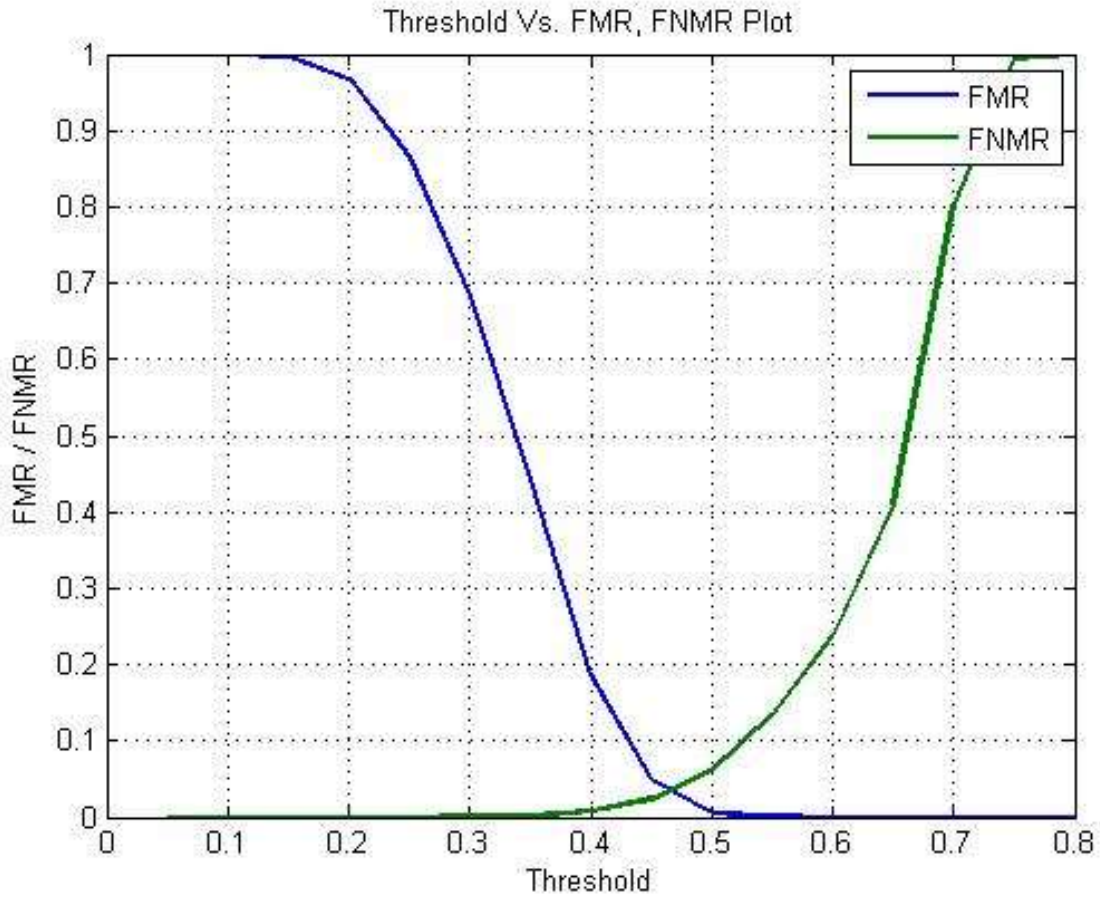


Figure 6: Threshold v/s FMR, FNMR Plot

`

A zoomed view of the intersection point of the ROC curves in Figure 6 is shown in Figure 7. It is observed that the intersection i.e. EER occurs at threshold value of 0.466.

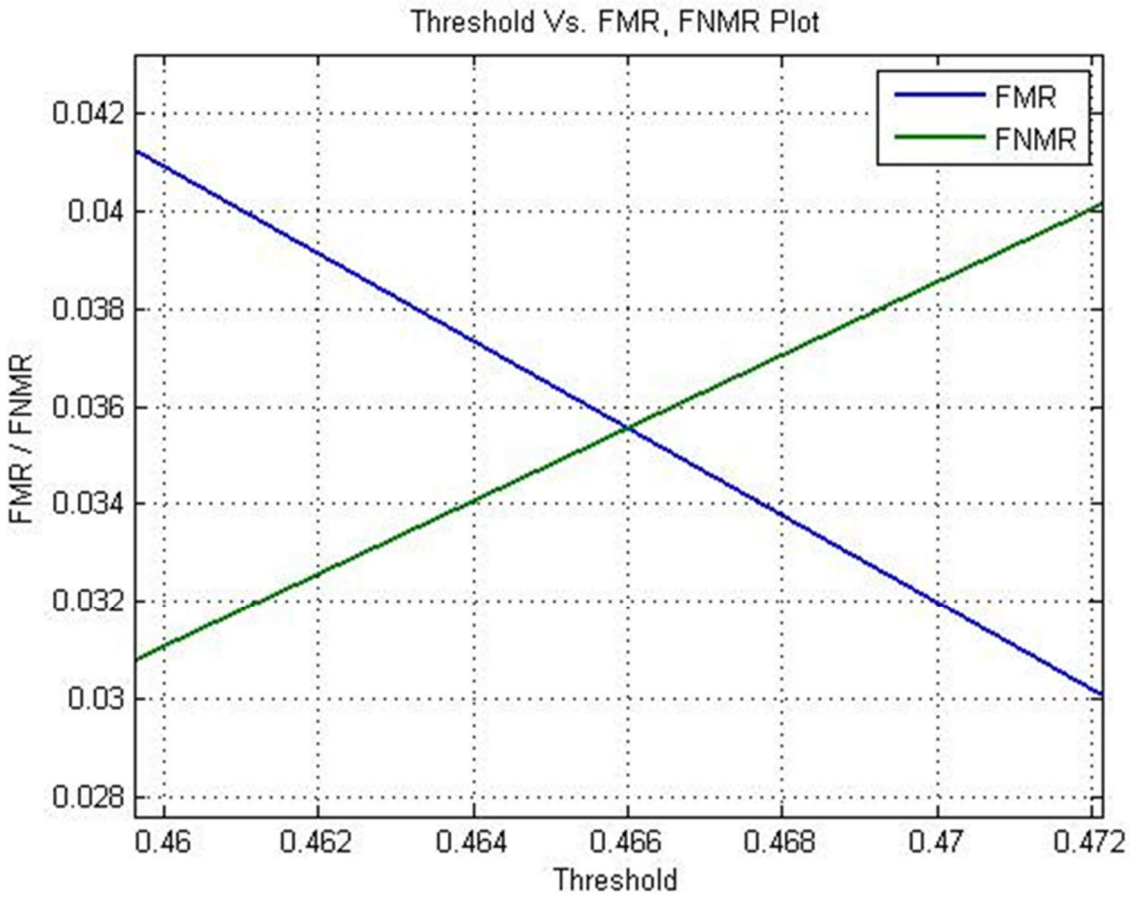


Figure 7: Graphical Calculation of EER

`

7. Conclusion

Since biometric traits are permanently associated with a user, they cannot be changed. If a biometric identifier is compromised, it is lost forever. Hence, instead of storing the original biometric data, it is transformed using a one-way function or some cryptography technique, thus preserving privacy. In this report, a protection technique for Minutia Cylinder-Code (MCC), which is a well-known local minutiae representation has been implemented in Matlab R2014a. An EER of 3.56 percent was achieved which is comparable to the original value of 3.33 percent. The FMR_{1000} was calculated to be 6.824 percent and the $ZERO_{FMR}$ was calculated to be 8.648 percent. Experimental results have demonstrated that P-MCC is more accurate than well-known minutiae matching techniques ([5], [6], [8], [9]). While it is evident from Table 2 that P-MCC advances the state-of-the-art fingerprint template protection techniques, this approach is still far from being perfect and that relevant research efforts are still necessary in this field. In particular, further work needs to be devoted to: i) carrying out a more in-depth theoretical study of P-MCC by evaluating the feasibility of various kinds of brute force attacks; ii) adding a user-specific secret key to P-MCC to achieve diversity and revocability; iii) evaluating other transformations to be applied to MCC descriptors.

`

8. References

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar*, Handbook of Fingerprint Recognition*, 2nd ed. New York: Springer-Verlag, 2009.

[2] J. Feng, A. K. Jain, "Fingerprint Reconstruction: From Minutiae to Phase, IEEE Trans. On Pattern Analysis and Machine Intelligence", 33-2-209-223, FEB. 2011.

[3] N. K. Ratha, K. Karu, S. Chen, A. K. Jain, "A Real-Time Matching System for Large Fingerprint Databases", IEEE Tran. On Pattern Analysis and Machine Intelligence, 18 8 AUG. 1996.

[4] L. Hong, Y. Wan, A. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation", IEEE Transactions On Pattern Analysis And Machine Intelligence, 20-8-777-789, AUG. 1998.

[5] G. Kumar, S. Tulyakov, and V. Govindaraju, "Combination of Symmetric Hash Functions for Secure Fingerprint Matching," in Proc. 20th Int. Conf. Pattern Recognition (ICPR), Istanbul, 2010, pp. 890–893.

[6] Zhe Jin, and Andrew Teoh Beng Jin, "Fingerprint template protection with minutia vicinity decomposition", International Joint Conference on Biometrics IEEE, 2011.

`

[7] Z. Jin, M.-H. Lim, A. B. J. Teoh, B.-M. Goi, "A Non-invertible Randomized Graph-based Hamming Embedding for Generating Cancelable Fingerprint Template", *Pattern Recognition Letters*, vol. 42, pp. 137-147, 2014

[8] Krivokuća, V., et al.: "A non-invertible cancelable fingerprint construct based on compact minutiae patterns.", Int. J. Biometrics. 6, 125–142.

[9] T. Ahmad, F. Han, "Cartesian and Polar Transformation-based Cancelable Fingerprint Template", 978-1-61284-972-0/11/, 2011 IEEE.

[10] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate based cancelable fingerprint templates." *Pattern Recognition*, 44(10-11):2555– 2564, 2011.

[11] R. Cappelli, M. Ferrara, D. Maltoni, "Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition", *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 32, no. 12, pp. 2128-2141.