COMBINATION OF FINGERPRINT TEMPLATE GENERATION USING MULTI-BIOMETRIC SYSTEM

Sindhu.K[1], Soundariya.D[2], Kapila Vani R.K[3],

[1] *Student, Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, TamilNadu, India*

[2] *Student, Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, TamilNadu, India*

[3] *Assistant Professor, Department of Computer Science and Engineering, Prince Dr. K. Vasudevan College of Engineering and Technology, Chennai, India*

ABSTRACT

In this paper we mainly perform matching between minutiae templates since it mainly avoids information leakage and enhances security. Overall, minutiae structures contain only relative information and they are less reliable when compared to global minutiae structures. We make use of fuzzy vault to enroll minutiae positions exactly. In the proposed system we comprise of multi-biometric system i.e., combination of face, fingers etc. This is achieved by combining minutiae and orientation structures from two different fingerprints to provide security. By using this system we can improve security and privacy can be preserved.

KEYWORD: - *fuzzy- vault fingerprint cryptosystem, matching minutiae template, Multi-biometric.*

1. INTRODUCTION

The fingerprint cryptosystem plays a vital role in most of the security applications. In general, the fingerprint verification system comprises of two procedures: 1) during enrollment, the user fingerprints is extracted and stored as template, 2) verification process a new combined fingerprint template is matched against the real one [2]. Since, minutiae template are compact many researchers found that it does not contain sufficient information, but based on fingerprint reconstruction algorithm [3], reconstruction of combined minutiae template, which is similar to the original template can be obtained. Generally, fingerprint reconstruction algorithm will reduce the generation of excess spurious minutiae when compared to the original one [2]. Fingerprint privacy is being protected by combining two different fingerprints into a single new identity. The system captures or enrolls two fingerprints from two different fingers. In general the fingerprint template can be categorized into minutiae positions and orientation (direction) [2]. In this, the combined fingerprint template is obtained by combining minutiae positions and directions. The minutiae positions depend on one fingerprint and directions depend on orientation of the other fingerprint and coding strategies. The combined template will be stored in the database for authentication process. By using fuzzy extractor the minutiae positions and orientations are extracted from two different fingerprints. When compared to kernel methods fuzzy extractor is the most reliable and feasible method. The combined fingerprint template is further used for user authentication and user verification. Fingerprint template is based on global structures which resembles the overall pattern around minutiae. In this paper we mainly focus on combined minutiae template. Each individual has unique fingerprint. The uniqueness is determined. The two local characteristics are:

1. Ridge ending and 2. ridge bifurcation [3]

A ridge ending is a point where a ridge ends.

A ridge bifurcation is a point where the ridge diverges into branches. Most of the fingerprint matching algorithms are based on 2D structures [5], which is of less efficiency. In this paper we use 3D data structures in order to recognize the fingerprint accurately [5]. By using 3D data structures it mainly specifies the cores, deltas, ridge flows, ridge frequency for evaluating fingerprint recognition systems. For this system we use MCC (Minutiae Cylinder Code) [5]. This mainly evaluates global score.

2. MOTIVATIONS AND CONTRIBUTIONS

The common and primary motivation can be described below as follows:

2.1 High Performance *[2]:* ISO templates are being used so that if follows a certain standard and it will be of high performance.

2.2 Conversion of point to string*:* Existing method requires core point or delta point. This is excluded in ISO minutiae template. An exact representation of the fingerprint template is preferred since the template has been highly standardized.

2.3 Usage of Multi Bio Metrics*:* This system combines more than one biometric identifier like combination of face, fingerprint, iris, ear etc. This can be applied for making decision about a person. Due to the combination of multiple traits, Bio-metric system is expected to be more reliable. It combines more than one psychological character.

2.4 High Security*:* This system ensures high degree of protection as the fingerprint template are combined and reconstructed in such a way that it resembles like original fingerprint template.

2.5 Fingerprint Reconstruction process*:* In this system the minutiae and orientation fields are extracted from two different fingers. The minutiae and orientation are reconstructed to form a single template and stored in database. For the third user it resembles as a single fingerprint. By this way, we can enhance the security in our system.

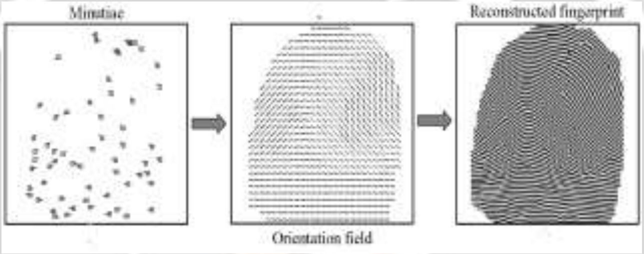

Fig -1: Finger print reconstruction

3. EXISTING METHOD

In current methodology regarding fingerprint template generation the fingerprint image is given as input [2] [3] [5]. But in our system we are going to use fingerprint sensor device to scan the finger. In the current existing system, for security it makes use of key for privacy that creates greater inconvenience. If the key is stolen or the system is being hacked, the user personal details can be stolen. The user identity may be stolen when both the key and the fingerprint are stolen. To implement fuzzy vault technique in the existing system it may cause vulnerable to key inversion attack because two separate databases are maintained that is not possible for the same application. Mainly decryption is needed. The fingerprint images are being scanned and then reconstruction process takes place [3] [6].

4. DRAWBACKS IN EXISTING SYSTEM*:*

4.1 Easily vulnerable to attacker*:* The fingerprint images are protected with the key, if the database is stolen the attacker can easily hack the data of a particular individual.

4.2 Hacking*:* since all the current methodologies make use of single biometric system it can be hacked easily. Hence the personal details can be corrupted.

4.3 Traditional approach*:* Traditional system makes use of key. If the key is stolen the database can be hacked easily.

5. PROPOSED METHOD

In our proposed system we make use of Multi-Biometric system which involves combination of face, fingers, iris etc.

This system is based on real- time application where we can provide high security. In our proposed system, the user wants to enroll his details along with two fingerprints from the two different fingers e.g., here we had considered thumb finger. A combined minutiae template generation algorithm is used to combine the extracted fingerprints. Minutiae positions are enrolled from one fingerprint, while the direction depends on the orientation of the other fingerprint and follow coding strategies. This combined minutiae template will be stored in the server database for the authentication process. It requires two query fingerprints for the matching process. Further, we propose a two-stage fingerprint matching process for matching the two query fingerprints against a combined single minutiae template.

By using a combined minutiae template, the minutiae feature will never be compromised. Hence, the final result shows a similar topology to the original minutiae template. By using fingerprint reconstruction approach, it can be converted into a real-look like combined fingerprint.

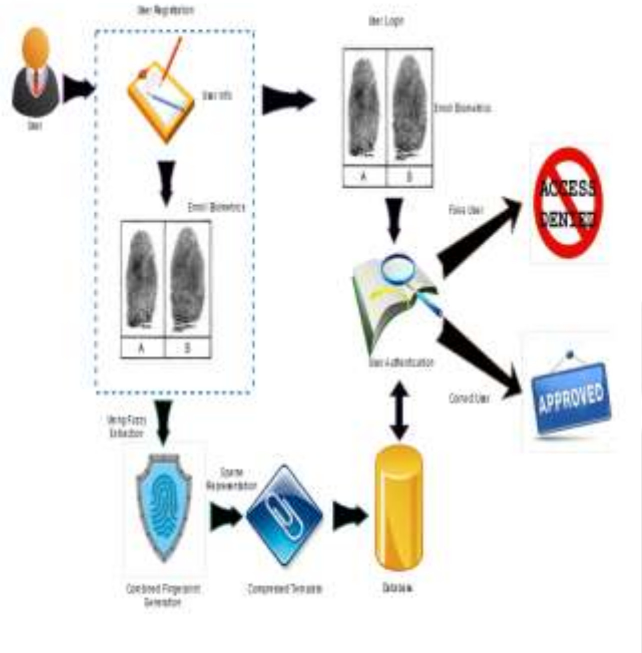

Fig -2: System Architecture

6. OVERALL FRAMEWORK

The steps that involved in this framework as follows,

6.1 Initially, the user has to undergo registration process by entering his personal details such as username, password, e-mail, security question etc.

6.2 And it also involves the process of enrolling the user's personal physiological character which majorly involves the fingerprint.

6.3 Template generation process takes place by combining the two different fingerprints of the user and combines it as a single minutiae template.

6.4 The combined single minutiae template will be stored in the database for further authentication process.

6.5 In the database it will be stored as a single template so that the third party user doesn't know that it involves two fingerprints in such way it can be secured.

6.6 The user can access the system any time by enrolling his fingerprints and get access to the system.

7. PHASES OF OUR PROPOSED SYSTEM

The proposed system consists of four phases,

7.1 User Registration phase: This phase is to mainly check whether the user is a valid one or not by gaining the user personal details, which mainly includes random chosen security question, answers, mail id, fingerprints, password, etc.

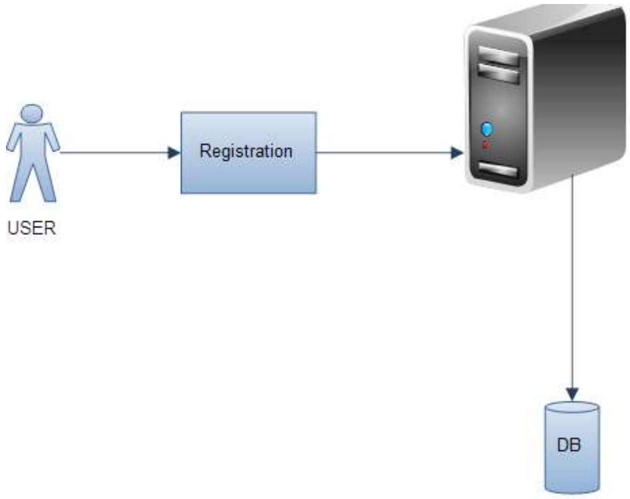

Fig -3: User enrollment phase

7.2 Compressed template generation Phase: Using sparse representation technique the two different fingerprint template is combined as a single template and compressed to the original size of the single minutiae template. The combined template is stored in the database for authentication process and to provide security as shown in figure4.

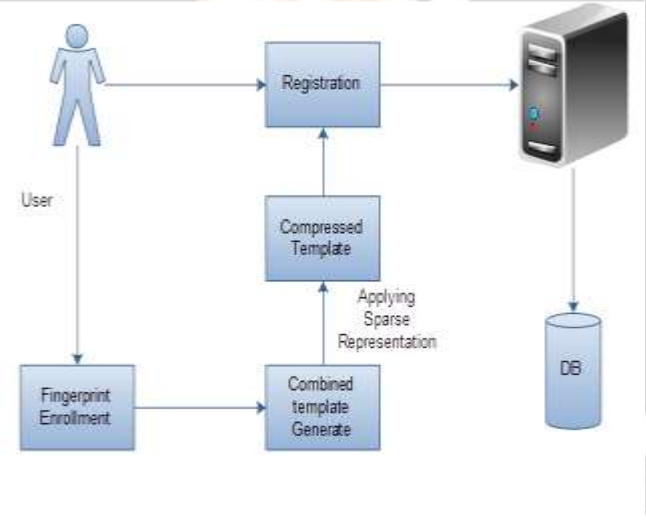

Fig -4: Compressed template generation phase

7.3 Server Authentication: In this phase it mainly authenticates the user login details and especially the fingerprint as described in figure2. The user details are matched against the details that are stored in the database. If the details provided by the user are matched against the stored one, the user is authenticated; otherwise the user is not an authorized user.

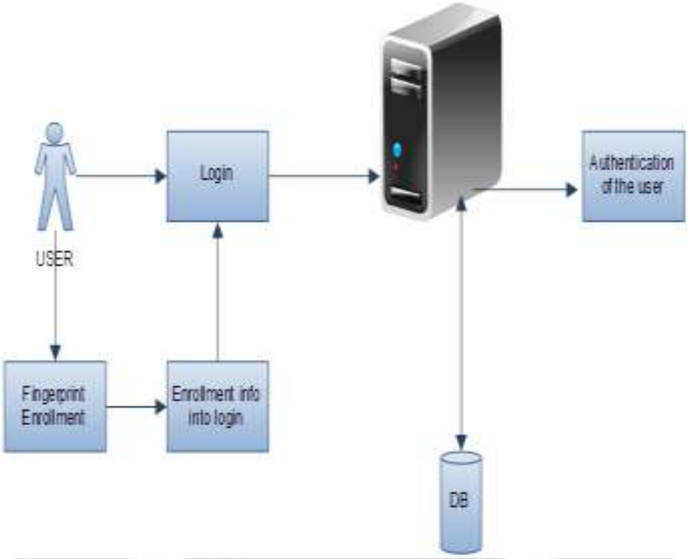

Fig -5: Server authentication phase

7.4 Access user information*:* This phase enables the user to access the information at any time and the user can upload any details. The information is updated in the server database also. This phase provides high security to the user details.

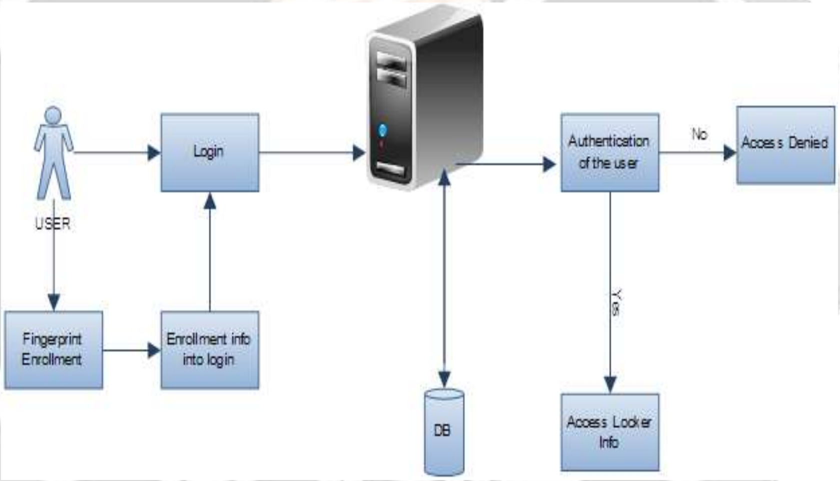

Fig -6: Access user information phase

In case if user finger has injured, in such cases the user cannot access it. For such situations the user cannot access the system, so the user needs to answer the security question. Once the user answers the question, OTP will be generated to the user registered mail id. With the help of OTP, the user can access the system.

8. ALGORITHMS USED*:*

The algorithms that are used in our system are:

8.1 Stage 1: Fuzzy Extractor: To extract the minutiae positions and directions from the user finger prints.

8.2 Stage 2: Combined Minutiae Template Generation: Combined template is generated and it is compressed to look alike the real one.

8.3 Stage 3: Two Stage Fingerprint Matching Algorithm: The combined minutiae template is being matched against the template stored in the database.

8.1 Algorithm

For any fingerprint template, the main steps of the reference point are detected as follows:

1) Compute the orientation O using the orientation estimation algorithm [16] for the fingerprint. The orientation Z in complex domain is obtained by

$$Z=\cos(20) + j\sin(20)$$

2) A certainty map of reference points, C_{ref}= Z $*$ T'_{ref} where '$*$' is the convolution operator and T'_{ref} is the conjugate of T'_{ref} =(x + iy).$1/2\pi\sigma^2$. exp (- $(x^2 + y^2)/2\sigma^2$).
3) Calculate improved certainty map as
   C'_{ref} ={ C_{ref}.sin (Arg(C_{ref})) if Arg (C_{ref})> 0
   0 otherwise
   Where, Arg (z) gives the principal value of the argument of z which is defined from –π to π
4) A reference point can be satisfied by two steps:
   i. The amplitude, C'_{ref} of the point.
   ii. The local maxima should be above the fixed threshold T.
5) Keep repeating step (4) until all the reference points are detected.
6) If no reference points are found in step (4) and (5) locate a reference point which has the maximum certainty value in the whole fingerprint image.

8.2 Algorithm

Minutiae template M_C is generated by minutiae position alignment and minutiae direction assignment.

A. **Minutiae Position Alignment**: Among all the reference points obtained from enrollment, we define a reference point with the maximum certainty value as the primary reference point. Therefore, we have two primary reference points R_a and R_b for fingerprints A and B respectively. Let R_a be located at r_a =(x_{ia}, y_{ia}) with the angle $\beta_a$and R_b be located at r_b=(x_{ib}, y_{ib}) with the angle β_b.

B. **Minutiae Direction Alignment**: Each aligned minutiae position p_{ic} is assigned with a direction $\emptyset_{ic}$as follows:

$$\emptyset_{ic}=O_B(x_{ic} y_{ic})+\rho i^{\pi}$$

Wherep_i, is the integer that is either 0 or 1 and the range of $O_B(x_{ic}, y_{ic})$ is from 0 to π.

Therefore the range of $\emptyset_{ic}$ will be 0 to 2π which is same as that of minutiae direction from an original fingerprint.

The following coding strategies are proposed for determining the value of p_i.

1. p_i is randomly selected from {0,1}
2. p_i is determined by

$$p_i=\begin{Bmatrix} 1\ if\ mod\ (\varnothing ia + \beta b - \beta a, \pi - OB(x_{ic}, y_{ic}) > 0) \\ 0 \qquad\qquad\qquad\qquad otherwise \end{Bmatrix}$$

where mod is the modulo operator and θia is the original direction of a minutiae position p_{ia} in fingerprint A. In other way p_i can be determined by

$$p_i=\begin{Bmatrix} 1\ if\ mod\ (ave\ b(x_{ic}, y_{ic}), \pi) - OB(x_{ic}, y_{ic}) > 0) \\ 0 \qquad\qquad\qquad\qquad otherwise \end{Bmatrix}$$

Where $ave\ b(x_{ic}, y_{ic})$ is the average direction of the n nearest neighboring minutiae points of the location ($x_{ic} y_{ic}$) in fingerprint B.

$$ave_b(x_{ic} y_{ic})=\frac{1}{n}\sum_{k=1}^{n}\theta_b^k(x_{ic}, y_{ic})$$

Where $\theta_k^b(x_{ic}, y_{ic})$ means the direction of the nearest neighboring minutiae points of the location (x_{ic}, y_{ic}) in fingerprint B, and n is set as 5 which is able to provide a good balance in matching accuracy of the combined minutiae template. At times, P_{ic} may be located outside the area of fingerprint, where $O_B(x_{ic} y_{ic})$ is not well defined. In such a case, we need to predict $O_B(x_{ic} y_{ic})$ before the direction assignment. In our paper, we simply predict the value of $O_B(x_{ic} y_{ic})$ as the value of nearest well defined orientation in O_B.

8.3 Algorithm

Input: Given the minutiae positions$P_{A'}$, of fingerprint A', the orientation $O_{B'}$of fingerprint B' and the reference points of the two query fingerprints.

Steps: In order to match the M_C stored in the database, we propose a two- stage fingerprint matching process [17] which includes the query minutiae determination and matching score calculation.

A. **Query Minutiae Determination**: This is very important steep during the fingerprint matching. We first introduce the local features extracted for a minutiae point inM_C. Given a minutiae point m_{ic} and another minutiae point m_{ic} in M_C, we define

1. L_{ij} as the distance between m_{ic} and m_{jc}
$$L_{ij} = \sqrt{\left(x_{ic}^2 - x_{jc}^2\right) - (y_{ic}^2 - y_{ic}^2)}$$

2. γ_{ij} as the difference between the directions of m_{ic} and m_{jc} (after modulo π):
$$\gamma_{ij} = \theta_{ic} mod\ \pi - \theta_{jc} mod\ \pi$$

3. σ_{ij} as a radial angle:
$$\sigma_{ij} = \kappa(\theta_{ic} mod\ \pi, atan2(\left(y_{jc} - y_{ic}\right), \left(x_{jc} - x_{ic}\right))$$

Where $atan2$(y, x) is a two- argument arctangent function in the range (-π, π) and
$$\boldsymbol{\kappa}(\mu 1, \mu 2) = \begin{Bmatrix} \mu 1 - \mu 2 & if -\pi < \mu 1 - \mu 2 \le \pi \\ \mu 1 - \mu 2 + 2\pi & if\ \mu 1 - \mu 2 \le -\pi \\ \mu 2 - \mu 1 + 2\pi & if\ \mu 1 - \mu 2 > \pi \end{Bmatrix}$$

Suppose we detect $k_1(k_1 \geq 1)$ reference points from fingerprint A' and $k_2(k_2 \geq 1)$ reference points from fingerprint B'.

1) Select a pair of reference points: one from fingerprint A' (say$R_{a'}$) and the other from fingerprint B' (say$R_{b'}$).Assume $R_{a'}$ is located at $r_{a'}$=($r_{xb'}, r_{yb'}$)with the angle $\beta_{b'}$, respectively.
2) Perturb $\beta_{a'}$ by T=$\beta_{a'} + k.\Delta$, where k is an integer and Δ is a permutation size. We choose Δ=3× π radians (i.e., 3 degrees) and -5≤k≤5. Thus, we have k=11 perturbed angles for the reference point$R_{a'}$.
3) Generate a combined minutiae template $M_{c'(T)}$ for testing from $P_{A'}$, $O_{B'}$, $R_{A'}$ (with a perturbed angle T)and $R_{B'}$ using the proposed combined minutiae template generation algorithm. The same coding strategy should be adopted for generating $M_{c'(T)}$ andM_c. In total, we generate K testing minutiae$M_{c'(T)}$.

B. Matching Score calculation: For a combined minutiae template, we directly calculate a matching score between M_Q and M_C using an existing minutiae algorithm. Hence the matching will be obtained.

9. CONCLUSION

In this paper, this system generally captures two fingerprints from two different fingers. A combined minutiae template containing only a partial minutiae feature of each of the two fingerprints will be generated and stored in the database. To make the combined minutiae template look real as the original minutiae template, it involves many coding strategies that are introduced in the combined minutiae template generation process. In the authentication process, two query fingerprints from the same two fingers are required. A two-stage fingerprint matching process is proposed for matching two query fingerprints against the enrolled template. Our combined minutiae template has a similar topology to an original template. Therefore, we are able to combine two different fingerprints into a new virtual identity by reconstructing it. This shows that our system achieves a very low error rate. It is also difficult for an attacker to break other traditional system by using the combined minutiae templates .Compared with the state-of-the-art technique; our technique can generate a better new virtual identity. Thus, the analysis shows that it is not easy for the attacker to recover the original template.

10. REFERENCES

[1] Kenneth Nilsson, Josef Bigun, "Localisation of corresponding points in finger prints by complex filtering", School of Information Science and Electrical Engineering(IDE).

[2] Jianjiang Feng, Anil K. Jain, "fingerprint reconstruction from minutiae to phase ", IEEE trans on pattern analysis and machine intelligence, vol 33, No. 2, February 2011.

[3] Raffaele Cappelli, Alessandra Lumini, Dario Maio, Davide Maltoni, " Fingerprint image reconstruction from standard templates", IEEE trans on pattern and machine intelligence, vol 29, no. 9, September 2007.

[4] Lin Hong, Yifei Wan, Anil Jain, "Fingerprint image enhancement:algorithm and performance evalutaion", IEEE trans on pattern and machine intelligence, Vol 20, no. 8, August 1998.

[5] Raffaele Cappelli, Alessandra Lumini, Dario Maio, Davide Maltoni, " Minutiae Cylinder Code: A new representation and matching technique for fingerprint recognition", IEEE trans on pattern and machine intelligence,Vol 32, No. 12, December 2010.

[6] a.Wahab,S. H. Chin and E. C. tan,"Novel approach to automated fingerprint recognition", IEEE proc. Vis. Image sognal process, vol. 145, no. 3, pp. 160-166,Jun. 1998.

[7]M. H. Lim,A. B. J. Teoh and K-A. Toh"An efficient Dynamic reliability –dependent bit allocation for biometric discretization". Pattern Recognit., vol. 45,no. 5, pp. 1960-1971, 2012.

[8]h. XU et al.,"Fingerprint verification using spectral minutiae representation", IEEE transaction Inf. Forensics secur.,vol. 4, no. 3. Pp. 397-409.sep. 2009.

[9]A. K. Hrechak and J.A. McHugh, “automated fingerprint recognition using structural matching”, pattern recognit. Vol. 244,no. 8,, pp. 893-904, 1990.
[10].M.Ferrara, D. Maltoni, and R. cappelli, “Noninvertible minutia code representation”, IEEE Trans inf. Forensics Secur., vol. 7,no. 6. Pp. 1727-1737, dec. 202.
[11]R.Cappelli,M.Ferrara and D. Maltoni, “A fast and accurate palm-print recognition system based on minutiae”, IEEE Trans. Sys., vol. 42, no. 3, pp. 956-962,Jun. 2012.
[12] M. S. Charikar, “Similarly estimation techniques from rounding algorithm”, in proc. ACM Symp. Theory comut., Monteral, QC, Canada, 2002, pp. 308-338.
[13]J.A. Rice, “Mathematical Statistics and Data Analysis”. Belmont, CA, USA: Duxbry press, 2001.
[14] W.B Johnson and J. Lindenstrauss, “extension of mapping into a Hilbert space”, contemp. Math. Vol. 26, pp. 189-206, jan. 1984.
[15](May 04, 2015.) Biolab, FVC2002, FVC2004. [online]. Available:http://bias.csr..unibo.it.
[16] K. Nandakumar “A fingerprint cryptosystem based on minutiae based spectrum” IEEE Workshop on YSA, 2010, pp. 1-6.
[17]J. Shawe-Taylor and N. Cristianini, “Kernel methods for pattern analysis”, Cambridge univ. press, 2004.
[18]T.-Y. Jea and V. Govindaraju, “A minutia based fingerpint recognition system”, pattern Recognit., vol. 38, no. 10, pp. 1672-6834, 2005.
[19] J. Bringer and V. Despie
gel , “Binary feature vector fingerprint representation from minutiae vicinities”, in proc. Int. Conf. Biometrics Theory.
[20] J.A.Rice, Mathematical Statistics and data analysis. Belmont, CA, USA: Duxbury Press 2001.