Privacy Protection using Random Combination of Fingerprints

Jayakumar. S
Assistant Professor, Department of CSE,
SRM University, Ramapuram, Chennai

Nithya. V
M.Tech Student, Department of CSE,
SRM University, Ramapuram, Chennai

ABSTRACT

The aim of this paper is to protect the information in database by combining two different fingerprint images into a new identity. This is done in two phases a) Enrollment and b) Authentication. In Enrollment phase the ***minutiae*** position from one finger and the ***orientation*** position from another finger are extracted. These two images are being combined into a new template. It is done by using a special technique called ***Watermarking***. Once the enrollment is over the furnished information will be stored in the server as template. In Authentication phase the fingerprint matching uses two stage query processing. The images obtained from two queries are being combined and checked with the stored template. Only if both the images are matching the access is granted to the user or else an error message is sent by the server. Since the combined template is visually realistic it is difficult for the hacker to break the security by separating the two fingerprint images. Compared with the existing system, our proposed system creates a new virtual identity when two fingerprints are chosen at random. The usage of invisible watermarking technique will increase the security by hiding the original information.

Keywords: Combination, Minutiae, Watermarking, Privacy protection, Orientation **.**

1. INTRODUCTION

Biometric based authentication system provides more security and robustness when compared with the conventional methods. Among different methods using fingerprints is more reliable because of its usability and high performance. Considering fingerprint is reliable protecting the privacy becomes a very common issue. In this paper we provide a solution to protect the privacy and improve the security. This is already implemented in existing systems but it have more drawbacks and hence we proposed a new solution to increase the privacy

The existing system using keys is more vulnerable to the attackers. Using the keys the fingerprints are scanned and encrypted for a single finger and it is stored in the database for authentication. And in authentication stage the stored fingerprint is decrypted and matched with the enrolled fingerprint. If this is not matching then the access to database is restricted.

According to brute force attack if the key is hacked then it is easy to decrypt the data and hack the database. So this method does not provide completed security and privacy.

According to S. Li and A. C. Kot [1], the system protects the privacy by combining the fingerprint of same fingers with use of a known key value. Though this provides security it becomes very easy for the hackers to know the key value and trace the fingerprint. Thus this has a high error rate and is proven to be not accurate by B.J.A.Teoh[2]. The solution is to provide a random number has key value but that is also easy to trace because same fingerprint will be used. [2] proposes a solution by using a pseudorandom key value which proves to be more secure and can never be stolen.[3] work by S. Chikkerur and N. K. Ratha , the privacy is protected by using cancelable fingerprints . This is encrypted with a common key value. Once the fingerprint is transformed and stored in database the original template is being destroyed. Comparatively this provides more security but implementation becomes difficult for large database. The problem is the destroyed template can be easily recovered and linked with the common key value. It leads to intrusion and leakage attacks.

[4] system by K. Nandakumar protects the privacy by using fuzzy logic. This uses the minutiae position of fingerprint so that original image cannot be traced. This can be hacked by Key inversion technique .When the image is enhanced dark area becomes darker, grey remains grey and bright area becomes brighter. This is converted into binary form and original image is extracted. This is proved by T.E.Boult.

According to the work proposed [5] it does not use any key values and is known as Visual Cryptography. In this technique the fingerprint image is being decomposed into two different sheets and stored in two different databases. For authentication the two sheets are overlapped to produce the original image. So, it becomes difficult for the attackers to hack the image with one sheet. The problem with this technique is maintaining two different databases is difficult practically impossible but produces low error rate.

[6]-[8] uses two different fingerprints to protect privacy. In [6] minutiae position is extracted from two fingerprints and stored in database. But the combined template is very much similar to the original fingerprint images and it is easy for the attackers to trace the images. Works in [7], [8] propose to combine the fingerprint images in image level. The images are decomposed into continuous component based on the FM-AM model. Then it is combined with spiral component to provide a new identity. But experimental result show that EER is about 15%. And is proven to be wrong if the fingerprints are being chosen at random.

The advantages of our proposed system over the existing techniques of fingerprint combinations are:

1) The proposed system is able to achieve low error rate .

2) Compared with feature level technique ,we are able to create a new identity which is difficult to be distinguished from the original minutiae templates.

3) Compared with the existing technique here we are able to create a new virtual and performs better when the two different fingerprints are randomly chosen.

2. PROPOSED SYSTEM OF FINGERPRINT COMBINATION

In our proposed system, the fingerprint images are being chosen at random and combined. The Fig.1 describes the complete process of combining images.

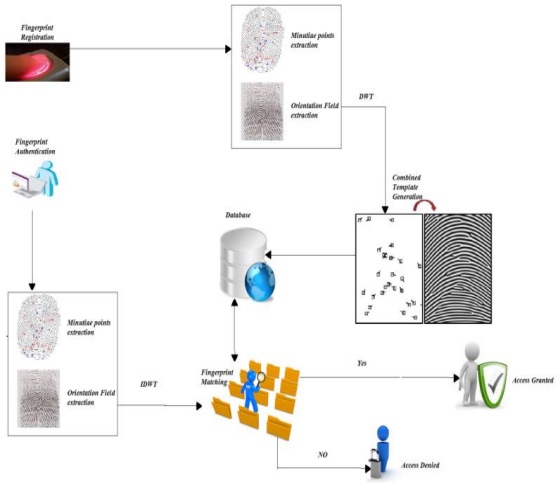

Fig.1 Proposed fingerprint privacy protection system

In the enrollment phase, the system scans two fingerprint image from two different fingers, say fingerprints A and B respectively. The minutiae positions are extracted from fingerprint A and the orientation from fingerprint B by using our proposed technique. A combined template is generated based on the minutiae positions and the orientation positions detected from both fingerprints.

Finally, the combined template is stored in the database and during authentication stage, two query fingerprints are required from the same two fingers. Similar to the enrollment, we extract the minutiae positions from fingerprint A and the orientation from fingerprint B. These extracted information will be matched against the corresponding template stored in the database by using a two-stage fingerprint matching. The authentication is considered successful if the matching is over a predefined threshold.

3. COMBINED TEMPLATE GENERATION

This section describes how the two different fingerprint images chosen at random are being combined to produce a new template which is a real look-alike image of the original images. Here we continue the processing by using different modules :

a) Authentication
b) Blind Cryptography
c) Data Verification
d) Report Generation

A. Minutiae Position Extraction

In the Minutiae template authentication module every user will be authorized by the admin or the main controller of the process. The user should register with their personal info and have a secure key if additional authentication is needed. After the permission is granted by the admin controller they can access the processing units as well as transfer data.

While registering the users account to the admin, it's important to note the user IP and host where they are from. After the successful registration users can access data using the login process. The login process verifies the user details form data store whether they are registered or a new one or they are intruders (unauthorized persons). Basically in login process the user needs to enter the user name with their corresponding password. In some other secure application, user needs to submit the secure key during authentication process (login). Along with the personal information the two fingerprints images are being collected and stored as a new template.

The fingerprint image is being thinned. The skeleton of the image is formed. The minutiae points are extracted based on the following steps. The fingerprint is converted into binary image and it is thinned. All the ridges are compressed to one pixel width. The points with pixel value of one (ridge ending) as their neighbor or more than two ones (ridge bifurcations) in their neighbourhood. Thus the minutiae points are extracted. This may contain false minutiae points at the borders of the ridge. This will result in false recognition of the image. Using segmented mask the false points are deleted.

Fig.2 Fingerprint Image

Fig.3 Thinned Image

Fig.4 Thinned Image Along with Minutiae Points

Fig.5 Minutiae Position after deleting false points

The minutiae position is extracted from fingerprint A image and then is combined with the orientation position of fingerprint B. This is done by Watermarking technique and it is the next section of our paper.

B. Watermark Technique Execution

By using this technique we combine the two different fingerprint images into a new identity. This hides the details of how the template is being overlapped and combined. A digital watermark is a kind of marker embedded in a noise-tolerant signal. It is typically used to identify the ownership of copyright of these signals. "Watermarking" is a process of hiding information in a carrier signal; the hidden information does not need to contain a relation to the carrier signal.

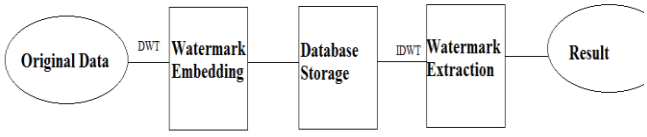

Fig.6 Implementation Stages Of Watermark Technique

The watermark technique is implemented in two stages namely Embedding and Extraction. In Watermark embedding Stage the two images are overlapped and a new template is created. Unlike metadata that is added to the carrier signal, watermark will not change the size of the carrier signal. The digital copy of any input data is the same as the original information, watermarking is just a passive protection tool. It only marks data, but will not degrade it nor controls access to the data. In the proposed system we have used this watermarking method to combine two different fingerprint into one new template. So it becomes a difficult process for the attackers to identify the exact position of two fingerprints by which the security level increases.

1) Watermark Embedding Process

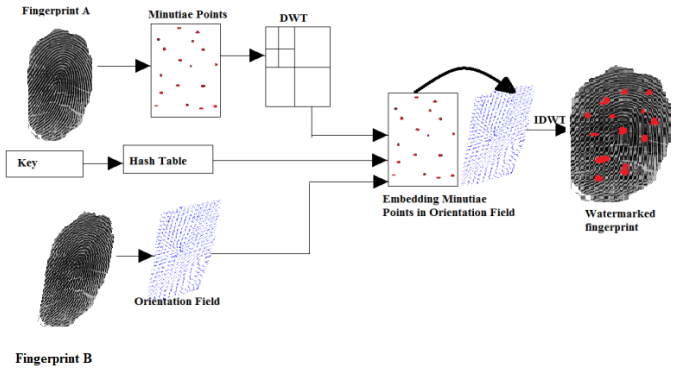

Fig.7 Watermark Embedding Process

Step1: Discrete Wavelet Transform algorithm is applied on the fingerprint image A denoted as F_A. The coefficients of the band contains the details of fingerprint image and hence it is not modified.

Step 2: The sub bands are divided into blocks of size M*N and the coefficients are numbered. From each block the first wavelet coefficient with positive phase and less than threshold value η is selected. The second LSB is replaced by one bit from fingerprint image B denoted as F_B and is represented as:

$$F_w(i,j) = \begin{cases} LSB_2(F_A(i,j)) = F_B(x,y) \\ \quad \text{if Phase}(F_A(i,j)) \geq 0 \text{ and } F_A(i,j) < \eta \\ F_A(i,j)) \\ \quad \text{if Phase}(F_A(i,j)) < 0 \end{cases} \quad (1)$$

Step 3: If the number of bit in fingerprint image B is less than the blocks of F_A, then all the bits are embedded or else the following procedure is implemented:

(a)For each F_A block, a message block MB is formed by selecting the higher order bits and a key K is appended. The value of key is large such that it cannot be found by brute force attack.

(b)The hash value of message block is calculated as

$$H_A = H(MB)K \quad (2)$$

(c) The value of $[H_A \bmod (M*N)]$ gives the position to embed the watermark bit. If the MSB of H_A is 0 then the F_B bit is inserted unchanged or else the compliment is inserted.

Step 4: Now, IDWT is applied in order to generate the secure watermarked fingerprint image. Any small change in F_A will result in a different hash value. The key vale K is unknown to the hacker so it is difficult to find the hash values.

2) Watermark Extraction Process

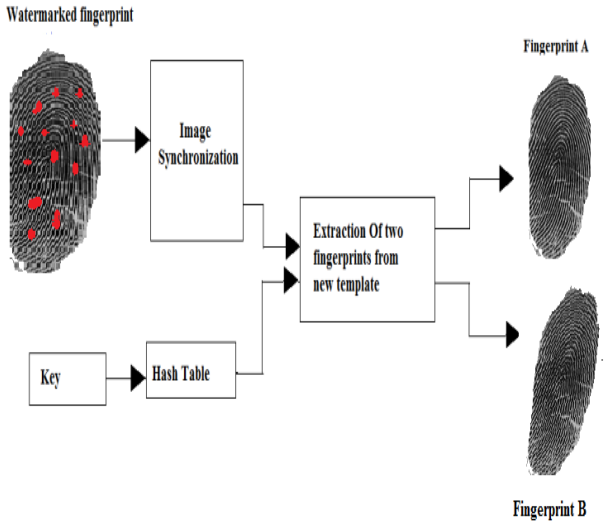

Fig.8 Watermark Extraction Process

Step 1: The image is synchronized with the block.DWT is applied on the image and sub-bands are divided into blocks of size (2M-1)*(2N-1).

Step 2: For each block synchronization is done as follows:

(a) A message block MB is embedded and a key K is appended to it.

(b) The hash vale is calculated based on equation (2).

(c) The synchronized blocks are identified by comparing the last few bits of H_A with the LSB of neighboring blocks.

Step 3: From the synchronized blocks the coefficient with positive phase and less than threshold value η is extracted from watermarked image.

Step 4: The remaining bits by calculating the pixel position. The pixel position is calculated by $[H_A \bmod (M*N)]$. The MSB of H_A is checked to find if the bit is inserted as such or compliment is taken and is extracted.

Step 5: These extracted bits are again rearranged to form the fingerprint image F_B and IDWT is applied to generate the original fingerprint images F_A and F_B from the watermarked image.

We have used this watermark technique to match the images stored in the databases. At the time of enrollment the client stores two fingerprints by combining into one new template. During authentication the same two fingers are placed and combined , later the combined image is encrypted. Then the server matches by uploading the saved combined fingerprint image and registered image. At that time data wavelet algorithm is used to match the two combined fingerprint stored in server database and the other from client database, then matching result appears.

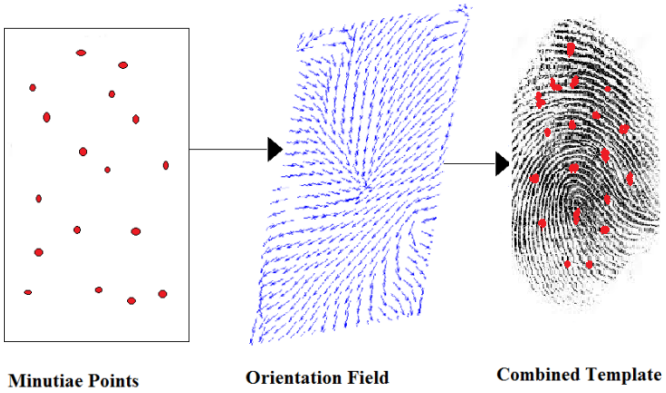

Fig.9 Combination of fingerprint images

After the login process the user will enter into the main form which will contain the basic operations. To transfers the data user needs to include and make a verification data for it. Both the data and minutiae template verification data will encrypt to prevent unauthorized access. In this module using the MD5 algorithm convert the biometric data to cipher text, earlier conversion methods convert the data's in bytes code format or in text format, that's not enough for healthy communication, MD5 algorithm make the secured data mechanism, converted data's are in cipher text format, so hacker cant able to read the exact data, this process only make the exact Minutiae template authentication process.

In general, server chooses the random number for key authentication. As like the sender side it will also give the same key in another end to retrieve data. Using the random key value the further authentication process will be held. After the data verification blind secure protocol performs the additional security to the data which was contains the following steps,

a) Retrieve the key from server,

b) Initialize the doubling technique to change the server key,

c) A blind level of process also initialized for key generation,

d) New key will be generated based on the methods,

e) Transfers the data with new key,

The Biometric authentication process purely depends on the technique which the protocol uses. It may be addition or subtraction. Once the blind process completed the key was transferred to the receiver end, as well as verification data also sent.

C. Two-Stage Query Processing

This section describes a fingerprint matching algorithm using BLPOC function. The algorithm consists of the three steps Rotation and displacement alignment, Common region extraction and Matching score calculation with precise rotation.

(1) Rotation And Displacement Alignment

Normalized rotation and the displacement between the registered fingerprint image f(x1, x2) and the input fingerprint image g(x1, x2) in order to perform the high-accuracy fingerprint matching.

First normalize the rotation by using a straightforward approach as. Generate a set of rotated images f'(x1, x2) of the registered fingerprint f(x1, x2) over the angular range $-50^{\circ} \leq \theta \leq 50^{\circ}$ with an angle spacing 1°. The rotation angle Θ of the input image relative to the registered image can be determined by evaluating the similarity between the rotated replicas of the registered image f'(x1, x2) ($-50^{\circ} \leq \theta \leq 50^{\circ}$) and the input image g(x1, x2) using BLPOC function.

Next, align the translational displacement between the rotation-normalized image f'(x1, x2) and the input image g(x1, x2). The displacement can be obtained from the peak location of the BLPOC function between f'(x1, x2) and g(x1, x2). Thus, we have normalized versions of the registered image and the input image, which are denoted as g(x1, x2) and f(x1, x2).

(2) Common Region Extraction

Next step is to extract the overlapped region (intersection) of the two images f(x1, x2) and g(x1, x2). This process improves the accuracy of fingerprint matching, since the non-overlapped areas of the two images become uncorrelated noise components. In order to detect the effective fingerprint areas in the registered image f(x1, x2) and the input image g(x1, x2), we examine the x1-axis projection and the x2-axis projection of pixel values. Only the common effective image areas, f(x1, x2) and g(x1, x2),with the same size are extracted for the use in succeeding image matching step.

(3) Matching Score Calculation

The phase-based image matching is highly sensitive to image rotation. Hence, we calculate the matching score with precise correction of image rotation. We generate a set of rotated replicas f ' (x1, x2) of f (x1, x2) over the angular range $-2^{\circ} \leq \theta \leq 2^{\circ}$ with an angle spacing 0.5°, and calculate BLPOC function r K1 K2 f θ g (x1, x2). If the rotation and displacement between two fingerprint image is normalized, then the correlation peak is observed at the center of the BLPOC function.

The BLPOC function may give multiple correlation peaks due to elastic fingerprint deformation. Thus, the matching score between the two images is defined as the sum of the highest P peaks of the BLPOC function r K1 K2 f θ g (x1, x2), where search area is B × B-pixel block centered at (0,0). In this paper, we employ the parameters B = 11 and P = 2. The final score S P ($0 \leq S P \leq 1$) of phase-based matching is defined as the maximum value of the scores computed from BLPOC function r K1 K2 f θ g (x1, x2) over the angular range $-2^{\circ} \leq \theta \leq 2^{\circ}$.

4. EXPERIMENTAL RESULTS

Fingerprint comparison is based on the matching of minutiae points. The minutiae considered in automatic identification systems are normally reference points, ridge bifurcations etc. Here we present a different technique for the extraction of fingerprint minutiae from Skeletonized binary images.

The goal is to extract the real minutiae of a fingerprint image from the 200 contained in typical Skeletonized and binarized images and to generate a new combined template which is a real look-alike image of the original fingerprint .

Table 1 . Accuracy Compared to Other Algorithms

Attacks	DFT Algorithm			LSB Algorithm			DWT Algorithm		
	Fingerprint 1	Fingerprint 2	Combined Template	Fingerprint 1	Fingerprint 2	Combined Template	Fingerprint 1	Fingerprint 2	Combined Template
No Attacks	98.94	94.78	99.57	98.94	92.16	99.41	98.94	94.16	99.48
JPEG 50%	98.94	0.00	0.00	98.94	90.87	99.10	98.94	91.42	99.25
Gaussian Noise	96.56	0.00	0.00	98.10	91.22	99.18	98.10	91.67	99.21
Blurring	97.11	43.52	61.22	97.02	81.65	97.99	97.22	91.45	99.02
Cropping	98.94	91.92	99.01	97.99	53.69	82.18	97.98	89.75	98.83
Rotation 10°	98.94	98.99	98.10	94.66	45.23	74.08	98.70	89.41	98.25
Affine Transform	91.76	74.31	82.19	91.20	25.62	67.25	92.13	75.47	90.69

The use of the fingerprint minutiae extraction algorithms has also been considered in a fingerprint Identification system of the existing system but it shows false reject or acceptance rate. The minutiae extraction method performs correctly in dirty areas and the background. The results are confirmed by visual inspections of validated minutiae of reference fingerprint images in the database. This experimental result shows that the EER of matching two fingerprint is about 15% when it is are randomly chosen for creating a new template. If the two different fingerprints are carefully chosen according to a compatibility measure the EER can be reduced to about 4%. In the proposed technique watermark can be embedded in different two types :

(a)Spatial watermarking :

It is applied on the input image such that the watermark appears in only one of the colour bands. The watermark appears when the colour is separated. This process involves addition of pseudo-noise into the image. It modifies the least significant bits of original image. In this technique the watermark can only be hidden but the LSB data are visually irrelevant.

(b)Transformation based watermarking:

Watermark is applied in the transform domain it includes different transforms such as discrete Fourier, discrete cosine, and wavelet. Here, the host data is transformed and then to the transformed coefficients modifications are applied . It is done in DFT, DCT and DWT domain coefficients

D. DCT DOMAIN WATERMARKING

This algorithm is secure only for simple image processing operations like low pass filtering, contrast and brightness adjustment, etc. And also it is difficult to implement and is computationally costly. This technique is weak against geometric attacks like scaling, rotation ,cropping etc.

E. DWT DOMAIN WATERMARKING

DWT Algorithm is most commonly used in signal processing and image compressing schemes.

(a)Characteristics of DWT

1) It decomposes the image into three spatial directions vertical, horizontal and diagonal.
2) The Wavelet Transform is mathematically efficient.
3) The magnitude of coefficient value is high in lower level bands .

(b)Advantages of DWT over DCT
1) The transformed image has multi-resolution and an image can be continuously processed from low resolution to high resolution.
2) Visual artifacts are been introduced in wavelet transformed images and hence at high compression rates the blocks are well noticeable in DCT , whereas in wavelet coded images it is much clear.
4) In DFT and DCT transformation any change in the transform coefficients will affect the entire image but in a wavelet transform it provides both frequency and spatial information for an image.

Table1 summarizes the verification of performance of the fingerprint images using different algorithms based on watermark technique like DFT based algorithm, LSB based algorithm and our proposed algorithm (DWT). The performance is evaluated using two fingerprint images and the combined template generated by the corresponding algorithm. The fingerprint verification is based on the minutiae positions matching and it is done by using the band limited phase only correlation function. The results are tested under different conditions like no attacks, noise attack, compression attack etc.

The watermarked fingerprint image is also subjected to different geometric attacks like cropping, resizing, rotation. Under normal conditions when there is no attacks all the three algorithms appear to be efficient. But when considered under geometric attacks LSB based algorithm performs 18% more efficient than DFT.

Thus produces a blurring effect to the input fingerprint images. For the frequency based attacks DCT based algorithm shows a poor performance. Our proposed technique is more robust and secure. It is also affected to some attacks but comparatively the quality of image is not much altered.

The experimental results show that the combined minutiae template generated by our proposed strategy is efficient and real look-alike of original image. Fig.10 (left to right) shows a comparison of the original fingerprint images of A and B. Minutiae position extracted image and the combined template of our technique. The last image is combined template generated by conventional technique.

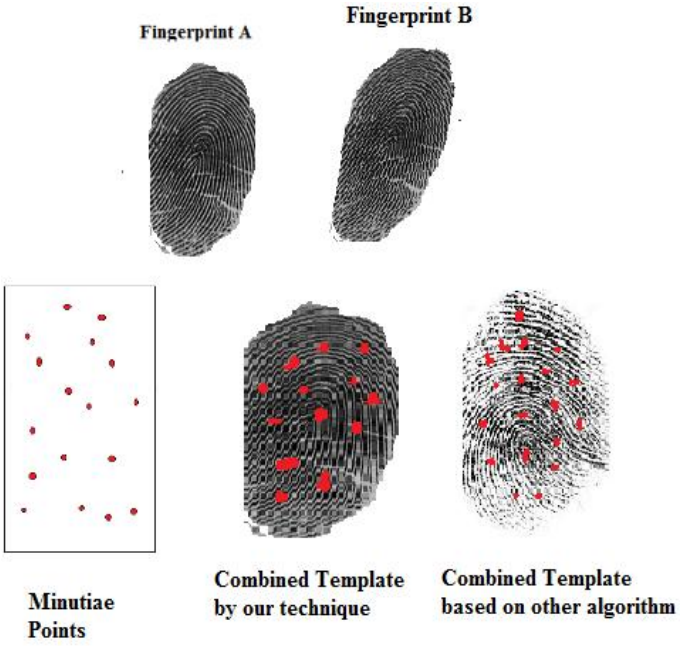

Fig. 10 Different Types Of Identities

The performance comparison graph of the existing and proposed strategies. It shows that the combination of fingerprint template generated by our proposed system achieves very low error rate.

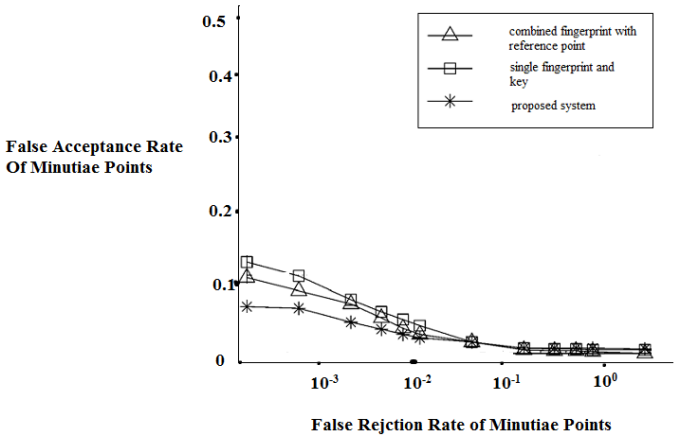

Fig. 11 Performance Measurement Graph

5. CONCLUSION AND FUTURE WORK

We introduce a novel system for privacy protection by combination of two fingerprints randomly chosen into a new template. During the enrollment stage, the system captures two fingerprint image from two different fingers. A combined template containing a partial minutiae feature of one finger and orientation field of another finger is created and stored in database for authentication. To make the combined minutiae template look real as an original template, three different techniques are introduced during the combined minutiae template generation process. In the authentication process, two input fingerprints are scanned. The fingerprint matching process is used to match the fingerprint images against the enrolled

template. The combined minutiae template is similar to the original minutiae template. Therefore, we successfully combine the two different fingerprint image into a new template using watermark technique which is a real look-alike image of input fingerprints.

Further work is required to enhance the performance due to mixed fingerprints by exploring alternate algorithms for pre-aligning, selecting and mixing the different pairs. Data's are stored into the Database. So large amount of Storage space is require. It's too difficult for Handicapped persons. Especially difficult for persons who doesn't having fingers. This application fails when user gets scratches in registered fingers. Since in Fingerprint matching using combined minutiae template to combine two finger print and create an single template, creating multiple combination of the finger print of an single finger and get the same procedure for other finger and create an multiple template.

6. REFERENCES

[1] S. Li and A. C. Kot, "A novel system for fingerprint privacy protection," in *Proc. 7th Int. Conf. Inform. Assurance and Security (IAS)*, Dec. 5–8, 2011, pp. 262–266.

[2] B. J. A. Teoh, C. L. D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, 2004.

[3] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–72, Apr. 2007.

[4] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: A security analysis," in *Proc. SPIE, Electron. Imaging, Media Forensics and Security*, San Jose, Jan. 2010.

[5] B. Ross and A. Othman, "Visual cryptography for biometric privacy," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 70–81,Mar. 2011.

[6] Ross and A. Othman, "Mixing fingerprints for template security and privacy," in *Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO)*, Barcelona, Spain, Aug. 29–Sep. 2, 2011.

[7] Othman and A. Ross, "Mixing fingerprints for generating virtual identities," in *Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS)*, Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.

[8] Camlikaya, A. Kholmatov, and B. Yanikoglu, "Multi-biometric templates using fingerprint and voice," *Proc. SPIE*, vol. 69440I, pp.69440I-1–69440I-9, 2008.