Securing Fingerprint Based Biometric System

Disha Lobo[1], Anoop C. V.[2], Mahesha Y[3]
Dept. of Electronics and Communication Engineering
St Joseph Engineering College, Vamanjoor

Abstract –

Nowadays biometric systems are in great demand. Biometric security systems are used to authenticate and provide access to a facility depending on the individual's physical characteristics. These characteristics which are stored in the database can be prone to theft. Hence there is a need to secure this identity which is stored in the database. Therefore in order to obtain a secure biometric system, two stages have been brought up. First stage is the enrollment stage, where two different fingerprints are taken and then two different features from each of these fingerprints are extracted. These two features are then fused to form a combined template and are stored in the database. In the authentication stage, the two query fingerprints are matched against the combined template which is produced in the enrollment. It is seen that the combined template is more secured and less prone to attacks.

Keywords - *Biometric database security; combined template; Minutiae; Matching; Orientation.*

I. INTRODUCTION

The major domain of this work is biometric database security. According to a number of research reports, it is seen that the need for biometric security is growing rapidly. This technology is having a great demand in today's world since most of the mobile users have become comfortable to use the tools such as fingerprint identification access. Biometric approaches include a fingerprint, face, voice, vein pattern, hand geometry etc. Biometric systems are commonly used to control access to laboratories, buildings, ATMs, personal computer accounts, secure electronic documents etc. The three steps in biometric system are, (i) Collection of biometric data. (ii) This collected data is described using digital representation called a template. (iii) This new template is compared with the previously generated templates stored in a database. The result of comparing this template will be a match or a mismatch. This result will be used to either permit access, sounding alarm etc. If the acquired template is not similar to the stored template, then it will result in a mismatch else it will result in a match. The degree of similarity required to result in a match declaration is called as threshold. Depending on the match score falling above or below the threshold, the acceptance or rejection of biometric data is decided. The major concern is that most of the times the databases which contain information of fingerprints could be stolen and misused. Since the biometric methods provide high levels of accuracy the threat of the intruder pretending like an authorized person and stealing his/her identity by obtaining this data is very high. Biometric readings cannot be replaced with another person from the valid person. Due to this other security issues like cutting off the finger of the valid person to gain access to a secure system might occur.

In order to avoid the harmful security threats occurring to the databases of a biometric system, the two different features of two different fingerprints can be combined to form a virtual identity [1]. Most of the techniques which are previously implemented make use of key for protecting the privacy of the fingerprint. One of them is the two factor authenticator based on the number of inner products between validated pseudo-random number and the users fingerprint feature, which produced a set of user specific code that is called as Bio-Hashing. It has achieved perfect accuracy [2].A biometric system itself is vulnerable to a number of threats. In biometric systems a critical issue is to provide security to the template of a user which is typically stored in a database or a smart card. A biometric cryptosystem such as fuzzy vault construct secures both the secret key and the biometrictemplate by binding them within a cryptographic framework, a fully automatic implementation of the fuzzy vault scheme based on fingerprint minutiae [3]. For privacy protection of the fingerprint template which is stored in the database, a fingerprint authentication system is introduced. The fingerprint data which is a binary thinned fingerprint image is considered. This is embedded with some private user information without causing any problem in the enrollment phase. In the authentication phase, for verifying the authenticity of the person who provides the query fingerprint, these hidden user data can be extracted from the stored template. Therefore, a data hiding scheme is proposed for the thinned fingerprint template [4]. Another form of security can be provided by taking an input fingerprint image and mixing it with another fingerprint image of different finger to produce a mixed image in order to hide the identity of the original fingerprint. In order to mix the two fingerprints, each fingerprint is decomposed into continuous and spiral components. Once the components of each fingerprint are pre-aligned, the continuous component of one fingerprint and the spiral component of the other fingerprint image are combined [5]. Another form of security can be provided by fingerprint enhancement algorithm in the

minutiae extraction module [6]. In addition, the combined template has a similar topology to the original templates, so it can be converted into a real-look alike combined fingerprint by using an existing fingerprint reconstruction approach [7]. Compared to these methods, the method used which is used in this work provides a higher level of security in terms of secrecy and piracy.

II. DESCRIPTION

Authentication means to confirm truth of an attribute of a single piece of data claimed true by an entity. Some of the authentication elements are personal identification numbers, security token, fingerprint, retinal pattern, smart cards or signatures etc. This project deals with protecting the fingerprint privacy which has become a major issue in sector of security.

A. Block Diagram

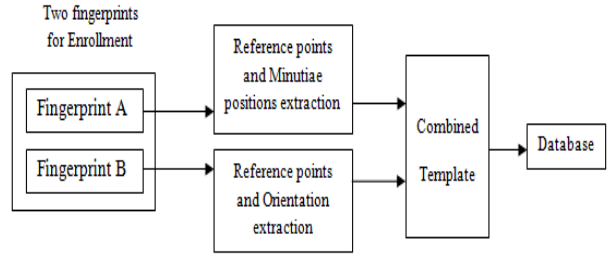

Figure 1: Enrollment

This project gives an idea where two different fingerprints are combined to form a new identity and further this new identity can be encrypted once again so that it becomes more secured. This new identity is a combined fingerprint. Here there are two stages [1].

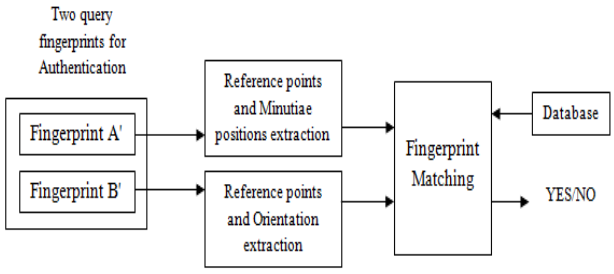

Figure2: Authentication

In the enrollment stage as shown in Figure 1, fingerprint software different fingers are taken and two separate features from each of the fingerprints is taken. Firstly, the minutiae positions from one fingerprint is extracted, the orientation from the other fingerprint is taken and at the end reference points from both fingerprints is taken. By making use of the extracted information and combined template generation algorithm, a combined template is formed and stored in database. Then using one of the existing fingerprint reconstruction approaches, a combined fingerprint is reconstructed from the combined template. In the authentication stage as shown in Figure 2, the system makes use of two query fingerprints from the same two fingers which were used in the enrollment. A two-stage fingerprint matching algorithm is proposed for matching the two query fingerprints against the combined minutiae template which was generated in the enrollment.

B. Methodology

First stage is the enrollment stage which is given in Figure 3. Initially two fingerprints are taken. One is chosen to be the main fingerprint i.e., thumb and another fingerprint can be of any other finger of the same person. Initially the two fingerprint images are converted to gray color images. This done because, if the fingerprints are colored then they will be three dimensional. By taking the threshold value of the gray scale image of these two fingerprints, black and white images of these two fingerprints are created.This is because the black and white image has only two intensities i.e., 0 and 1 whereas gray image will have intensity variation throughout. Another advantage is the black and white image will have only two intensities whereas in the gray image the intensity will keep varying. Further, morphological operation is done to remove the unwanted objects from the black and white images of the fingerprint. Once the morphological operation is done, two different features from each of the fingerprints is extracted. In this case the minutiae positions from the first fingerprint are extracted and orientation feature from the second fingerprint is extracted. After extracting the features, the two fingerprints are fused to form a combined template and is stored in the database. A combined fingerprint is generated from combined template using existing fingerprint reconstruction approaches. This creates a virtual identity i.e. a real look alike fingerprint.

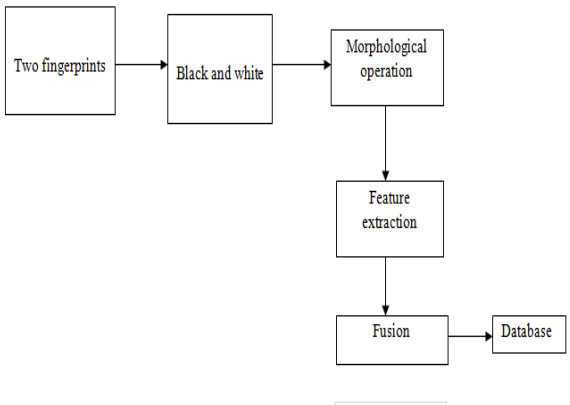

Figure 3: Enrollment Stage

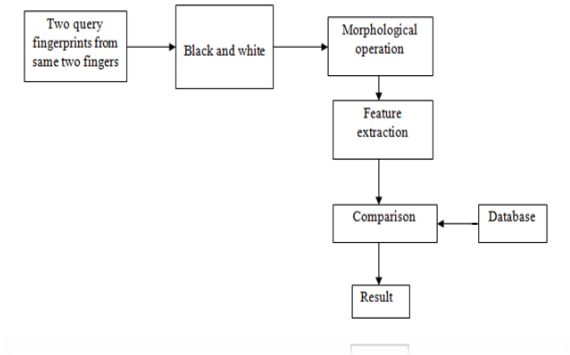

Figure 4: Authentication Stage

Second stage is the authentication stage which is shown in Figure 4. In this stage the combined fingerprint which is stored in the database is compared with the query fingerprints. Authentication is successful if the matching score is above a predefined threshold.

III. EXPERIMENTAL RESULTS

A. Minutiae and Orientation Extraction

Step 1: Figure 5 shows the original image of first fingerprint image. Therefore, provision is done to select a fingerprint image by concatenating the Filename and the Pathname.

Step 2: Conversion of original image to gray color image will result in a one dimensional image. Gray threshold of the image is found and the image is converted to black and white as shown in Figure 6.

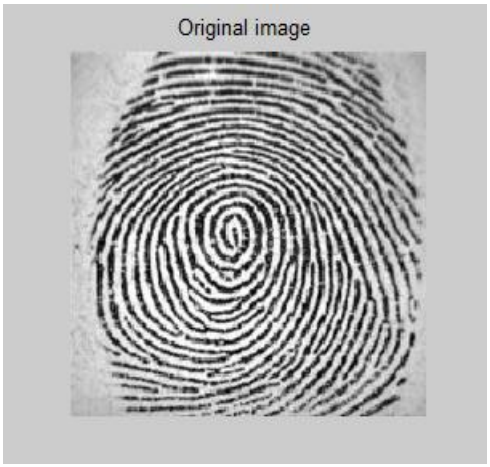

Figure 5: Original Image of First Fingerprint

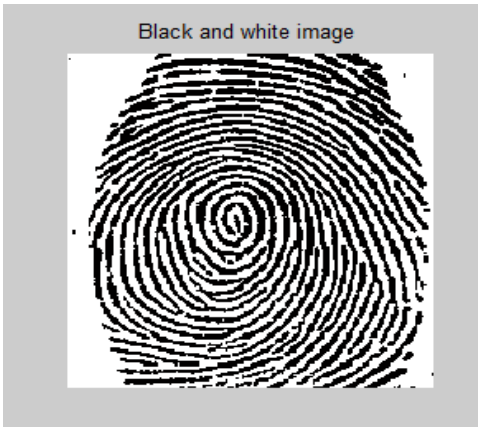

Figure 6: Black and White Image

If X_{ij} is the original image, with i rows and j columns andT_{gr} is the gray threshold, then

$$W_{i,j} = \begin{cases} 1 \; for all X_{i,j} \geq T_{gr} \\ 0 \; otherwise \end{cases} \quad (1)$$

Where W_{ij} is the black and white image with i rows and j columns.

Step 3: **Morphological operation:** After converting the image to black and white, it is then complemented because it easier to perform morphological operation when the ridges are white in color. The result of morphological operation is shown in Figure 7. Here morphological erosion is used.Let T be the 3*3 structuring element which is placed on every pixel of the 200*200 black and white image, I_m. Morphological operation can be mathematically represented as,

$$A = \sum_{i=-1}^{1} \sum_{j=-1}^{1} T(i+2, j+2) * I_m\,(a+i, b+j) \quad (2)$$

This implies that if A < 9 then I (a, b) = 0 and if A > 0 then I(a, b) = 1. Where a, b are the rows and column indices of the central pixel of 3*3 pixel neighborhood of image where the structuring element is applied.

Step 4: After performing the morphological operation minutiae positions of the original fingerprint are plotted. The minutiae positions include ridge termination positions and ridge bifurcation positions. These positions are shown in Figure8.

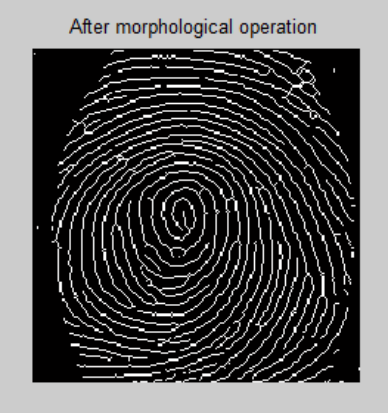

Figure 7: Result of Morphological Operation

Figure 8: Minutiae Positions of First Fingerprint

The result after removing spurious minutiae positions is shown in Figure 10.Let T be the 3*3 structuring element which is placed on every pixel of the 200*200 black and white imagesI_m.
The position of ridge termination location is found if,

$$T * I_m = 1 \quad (3)$$

The position of ridge bifurcation location is found if,

$$T * I_m = 3 \quad (4)$$

Where * is the pixel by pixel multiplication.

Step 5: If the ridge termination positions and ridge bifurcation positions come within 6 pixels range, which means their distance is less than D, then they are treated as spurious minutiae positions and are removed. This is shown in Figure 9.

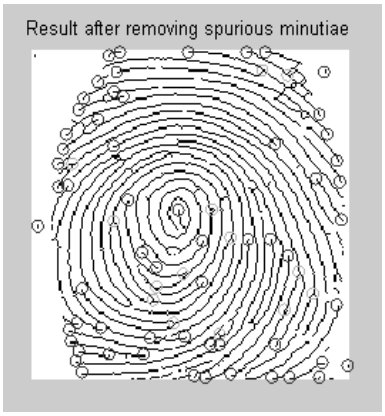

Figure 9: Result After Removing Spurious Minutiae

If (x_i, y_i) is the position of i^{th} minutiae and (x_j, y_j) is the position of j^{th} minutiae, then the Euclidean distance 'd' is given by,

$$d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (5)$$

Step 6: Finding Region of Interest (ROI): Here morphological closing is done by dilation followed by erosion. Morphological closing is performed by using a structural element which is a 7*7 sliding window. Next the holes from the resulting image are filled.

Once again from the resulting image the all the connected components fewer than 5 pixels are removed. This is the region of interest which is obtained.

Step 7: This step is performed on the image which is the result of morphological operation. The region of interest shown in Figure 10 is not the required region of interest since it covers some region which is more than the area covered by the fingerprint image. Therefore minutiae positions might be produced outside the area of fingerprint image due to some unwanted lines or marks.

Step 8: Once the required region of interest is found, the minutiae positions along with the region of interest are plotted and this is shown in Figure 11. Here it is seen that the minutiae positions are present outside the required ROI and must be suppressed.

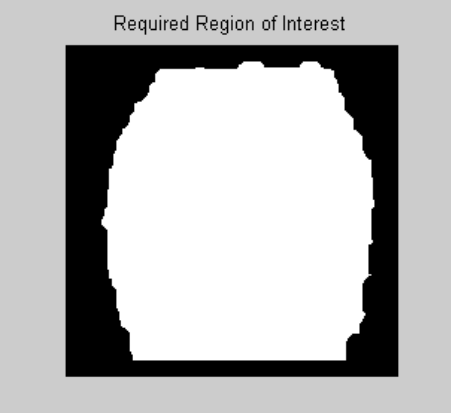

Figure 10: Required Region of Interest

Step 9: Then the original image is made black, but the locations where the ridge terminations positions are present are made white. After this pixel by pixel multiplication is done by multiplying ridge termination location with the transpose of ROI. This procedure is once again followed for all ridge bifurcation locations.

Finally all red and green plots are made visible. The suppressed extrema minutiae positions are shown in Figure 12.

Step 10: From this step the orientation and fingerprint matching criteria's are found for the second fingerprint image. Figure 13 shows the original image of second fingerprint.

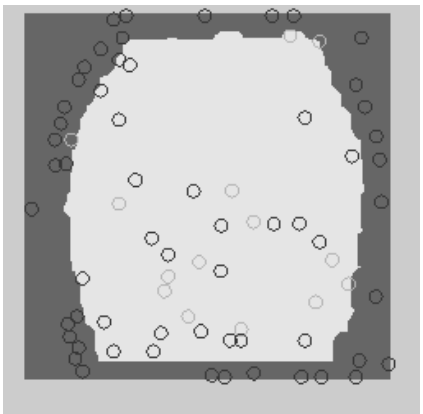

Figure 11: Minutiae Positions Along with ROI

Step 11: Conversion of original image to gray color image will result in a one dimensional image. Gray threshold of the image is found and the image is converted to black and white as shown in Figure14.

Figure 12: Suppressed Extrema Minutiae

Figure 13: Original Image of Second Fingerprint

Figure 14: Black and White Image of Second Fingerprint

Step 12: Morphological operation is shown in Figure 15.

Step 13: Orientation is found from the image which is complemented after morphological operation. Every pixel has orientation depending on the intensity of the gradient. After morphological operation four steps are followed to find the orientation of the second fingerprint image. Figure 16

shows the orientation of a small part of the second fingerprint image.

B. Combined Template

1) Combined template without Taking Reference Points into Consideration:

Here only the ridge termination locations are considered. All the minutiae termination locations and their corresponding angles at those locations are combined and plotted. A 200*200 white image is created. Then the minutiae termination locations are plotted in red and their corresponding orientations are plotted (Arrow marks). This is shown in Figure 17.

Figure 15: Result of Morphological Operation

For example if a ridge termination location is present in a (1, 3) pixel of the first fingerprint then it will get the orientation which is present in (1, 3) pixel of the second fingerprint. Here in order to combine the two features of the two different fingerprints reference points are not taken into consideration.

This is an advantage while combining because calculating reference points is time consuming. Therefore, without translating and rotating one fingerprints reference point to another, directly the orientation from second fingerprint is provided to the ridge terminations of the first fingerprint depending on the pixel where it is located.

2) Combined Template Taking Reference Points into Consideration:

The combined template by taking reference points into consideration is shown Figure18.This uses combined template generation algorithm. The main advantage of this method is that it won't matter if the input given by the user slightly changes by its position and direction each time he/she wants to access a place. This method will identify the valid user since the reference points are taken.

Therefore, now if the attacker steals the combined template she/he won't be able to get the information of the original two fingerprints since it has minutiae of one fingerprint and orientation of the other.

C. Fingerprint Matching

In the enrollment stage the fingerprints which are combined and stored in the database. Therefore when the user tries to access a place the combined input given by him/her will be matched with the combined templates stored in the database.

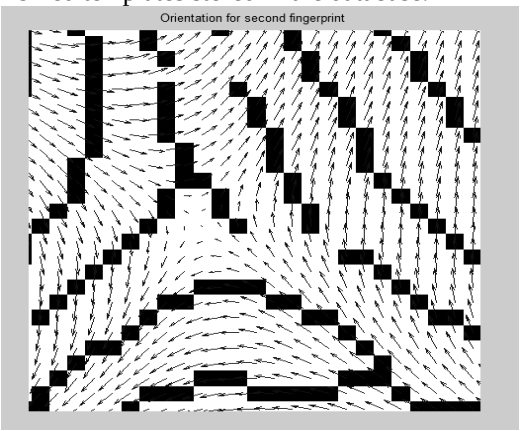

Figure16: Orientation of Part of Second Fingerprint

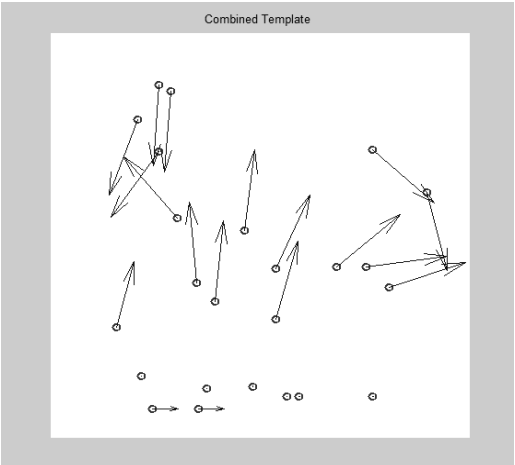

Figure 17: Combined Fingerprint Template Without Taking Reference Points

Case 1: If the fingerprints are combined and stored without taking reference points then the possibility of matching for a valid user is very low unless and until the user gives the input in the same position and direction. If the input is given in same position and direction then the score will be S = 1 which means perfectly matched. If the second fingerprint is changed with a different one as shown in Figure 19 then the score will be S=0.5417. But if both or any one of the fingerprints are slightly changed in position and direction then the score will be S=0.

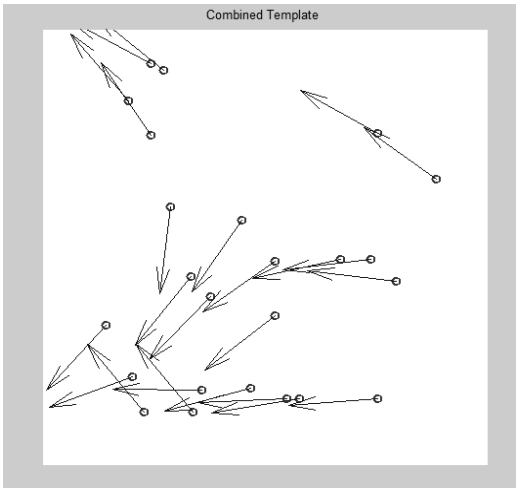

Figure 18: Combined Fingerprint Template By Taking Reference Points

Case 2: When the fingerprints are combined and stored by taking reference points possibility of matching for a valid user is very high even if the input slightly changes in position and direction within a given threshold. If the input is perfect in position and direction then score is 1. If any one of the fingerprint is tilted between -5 to +5 degrees then the estimated score is S= 0.9 and above. This implies that the system will recognize the valid user.

1) Match Score Based on the Effect of Tilt

This score is calculated when combining is done by taking reference points into consideration. The fingerprints which are used in enrollment are shown in Figure 5 and Figure 13. In the authentication stage fingerprint as shown in Figure 5 is kept as it is but the fingerprint as shown in Figure 13 is tilted by 0, 1, 2, 3, 4, 5 degrees respectively.

Figure 19: Query Fingerprint

These results of tilting are shown in Figure 20 below. The score is given as S=[1 0.9894 0.9685 0.9419 0.9299 0.9100].

2) Match Score Based on the Effect of Noise

Figure 5 is provided with noise of level of 1%,5%, 10%, 25%, and 50% respectively. During the enrollment noise is not given to both the fingerprint. During authentication different levels of noise is given to the first fingerprint. Figure 21 shows the how the score reduces drastically as the noise level increases.

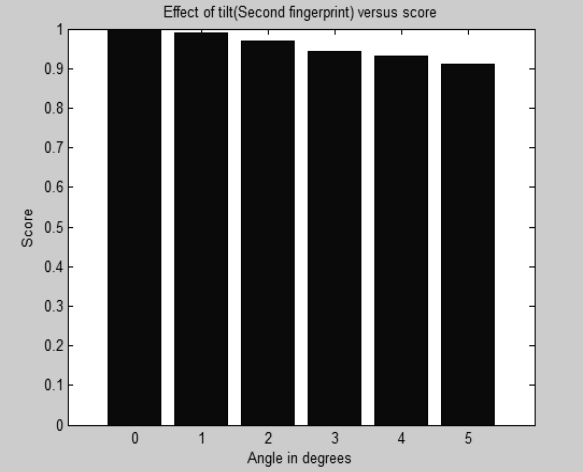

Figure 20: Effect of Tilt

IV. CONCLUSION AND FUTURE WORK

The main idea is to secure the database of a biometric system. Hence to do this, two stages namely enrollment and authentication are proposed. As per the enrollment stage, the combined template is produced and stored. And as per authentication two query fingerprints are taken and matched against combined template.

The minutiae positions of the first fingerprint image is found and plotted. Orientation feature for the second fingerprint is found and plotted. Combined template is obtained with and without taking reference points into consideration. This combined template which is stored is matched with the combined input which is produced in the authentication stage. Matching is done for different inputs and the result is analyzed. Also the impact of tilt and noise in authentication is analyzed.

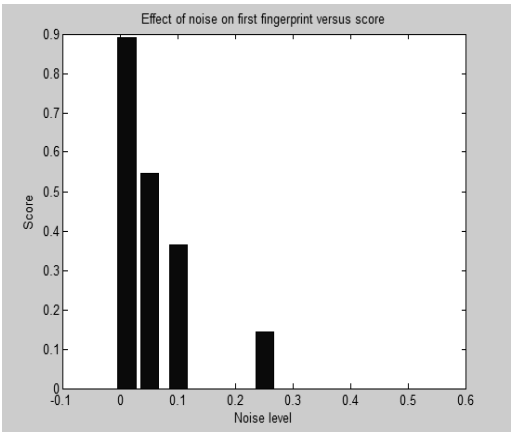

Figure 21: Variation Of Match Score In The Presence Of Noise

In future the combined template can be obtained by using other fingerprint features. The combined template which is obtained in this project can be converted into a look alike fingerprint using

fingerprint reconstruction algorithms. Further the level of security can be increased for high security systems by performing multiple stages of combining.

REFERENCES

[1] Sheng Li and Alex C. Kot, "Fingerprint Combination for Privacy Protection" IEEE Trans. Information Forensics and Security, vol. 8, no. 2, pp. 350-360, Feb. 2013.

[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] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," IEEE Trans. Inf. ForensicsSecurity, vol. 2, no. 4, pp. 744–57, Dec. 2007.

[4] S. Li and A. C. Kot, "Privacy protection of fingerprint database," IEEE Signal Process. Lett., vol. 18, no. 2, pp. 115–118, Feb. 2011.

[5] A. 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.

[6] L. Hong, Y. F. Wan, and A. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," IEEE Trans. Pattern Anal.Mach. Intell., vol. 20, no. 8, pp. 777–789, Aug. 1998.

[7] S. Li and A. C. Kot, "Attack using reconstructed fingerprint," in Proc. IEEE Int. Workshop on Inform Forensics and Security (WIFS), Foz doIguacu, Brazil, Nov. 29–Dec. 2, 2011.

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

[9] 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.

[10] S. Chikkerur and N. Ratha, "Impact of singular point detection on fingerprint matching performance," in Proc. Fourth IEEE Workshop on Automat. Identification Advanced Technologies, Oct. 2005, pp. 207–212.