Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 652 – 659

Procedia
Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

Identity of User Thrashing and Privacy Protection of Fingerprints

Reshma K V*, Anitha T Nair, Tina Babu, Mehbooba P Shareef, Nimisha Abraham

Computer Science and Information Sytems (Dept), Federal Institute Of Science And Technology
Hormis Nagar, Angamaly, Ernakulam 683577, Kerala, India

Abstract

A novel system used for fingerprint privacy protection by creating a new fingerprint identity and thrashes the user identity within the fingerprint image. A combined minutiae template containing only a partial minutiae feature of each of the two fingerprints captured in the enrolment phase, will be generated and stored. In the authentication process, a two-stage fingerprint matching process is proposed for matching the two query fingerprints against the enrolled template. Construct a new virtual identity, combined fingerprint by reconstructing the combined minutiae template having similar topology with it. The Dual-Tree Complex Wavelet Transform (DTCWT) domain is used to thrashing the user identity. Experiment results show the robustness of the algorithm against image rotation and different types of image noises.

Keywords: combined minutiae template; two stage matching; DTCWT; thrashing; combined fingerprint image

1. Introduction

Fingerprint is a very vital index in the field of security. It is used for personal identification due to its feasibility, distinctiveness, permanence, accuracy, reliability, and acceptability used for personal identification. The protection of privacy of the fingerprint becomes an important issue. Traditional protection methods like encryption and decryption of fingerprint is not a better method because decryption is required before the fingerprint matching.

* *Corresponding Author*: Tel: +919961373905
Email: reshma2890@gmail.com

doi:10.1016/j.procs.2015.02.118

Most of the existing techniques for the fingerprint privacy protection make use of a key and which creates the inconvenience. When both the key and the protected fingerprint are stolen and there may open for attacks. Teoh et al[2] propose a bio-hashing approach, which generates a unique code for a person by combining tokenized random data with the fingerprint. The accuracy of this two factor authentication approach is depends on the key, which is assumed to be never stolen or shared. It is vulnerable to intrusion and linkage attacks when both the key and the transformed template are stolen.

There are only a few schemes that are able to protect the privacy of the fingerprint without using a key. Ross and Othman [3] propose this approach by using visual cryptography for protecting the privacy of biometrics. The fingerprint image is decomposed using a visual cryptography scheme to produce two noise-like images (termed as sheets) which are stored in two separate databases. During the authentication, the two sheets are overlaid to create a temporary fingerprint image for matching. The advantage of this system is that the identity of the biometrics is never exposed to the attacker in a single database.

Berrin Yanikoglu et al [4] propose a biometric authentication framework to address the privacy by using two separate biometric features, combined to obtain a non-unique identifier of the individual. A combined biometric ID composed of two fingerprints is stored in the central database, and imprints from both fingers are required in the verification process, reduce the misuse and privacy loss. The concept of combining two different fingerprints into a new identity is first proposed, where the new identity is created by combining the minutiae positions extracted from the two fingerprints. The original minutiae positions of each fingerprint can be protected in the new identity. However, it is easy for the attacker to identify such a new identity because it contains many more minutiae positions than that of an original fingerprint.

Arun Ross et al [5] propose mixing fingerprints for template security and privacy, to combine two different fingerprints in the image level. In this work, an input fingerprint image is mixed with another fingerprint, in order to produce a new mixed image that hides the identity of the original fingerprint. To mix two fingerprints, each fingerprint is decomposed into continuous and spiral components. After pre-aligning generate a mixed fingerprint by combining the two components of each fingerprint.

When the user identity is linked with the fingerprint features to add more authentication factors to the authentication process. If monitoring and owner identification applications place the same watermark in all copies of the same content, it may create a problem. To solve that problem the user identity is thrashed with the fingerprint image using watermark approach. A digital watermark algorithm is one of the most researched methods to protect fingerprint images and there are several characteristics that a good watermark technique it should be perceptually invisible and resistant to common image processing operations.

Rhoads [6] described a method that adds or subtracts small random quantities from each pixel. By comparing a binary mask of bits with the LSB of each pixel thus determine the method is added or subtracted. If the LSB is equal to the corresponding mask bit, then the random quantity is added, otherwise it is subtracted. This method does not make use of perceptual relevance and provide some robustness to low-pass filtering. This scheme does not consider the problem of collusion attacks.

Recently [7, 8] proposed a watermarking algorithm for fingerprint image protection without corrupting minutiae points. This method embeds a watermark into a fingerprint image using the DCT technique. The idea behind this method is the watermark is embedded into the DCT blocks which contain two minutiae points or less. The template and the host fingerprint are exactly the same image. The watermark effect is determined by comparing the total number of minutiae points before and after watermark embedding.

2. Proposed System

Fig: 1 shows the process flow of Identity of user thrashing and privacy protection of fingerprints. The proposed system is used for protecting fingerprint privacy, by combining two different fingerprints into a new identity and thrashes the user identity information into the fingerprints virtual identity. In the enrolment phase, the system captures two fingerprints from two different fingers, say fingerprints A and B. Extract the minutiae positions like ridge ending and ridge bifurcation from fingerprint A using cross numbering method [10] and the orientation from fingerprint B using gradient based method [11]. Then extract reference points like core point from the two fingerprints using complex filtering convolution operator [12]. Then a combined minutiae template[1] M_C is generated based on the minutiae positions $P_A = \{p_{ia} = (x_{ia}, y_{ia}), 1 \leq i \leq N\}$ of fingerprint A, orientation O_B of fingerprint B and reference points detected from both fingerprints A and B. Finally, a combined minutiae template is stored in the database. In the authentication phase, two query fingerprints are required from the same two fingers; say fingerprints A and B. As what done in enrolment phase, extract the minutiae positions from fingerprint A and orientation from fingerprint B. Reference points are detected from both query fingerprints. This extracted information's are matched against the corresponding combined minutiae template stored in the database by using a two stage fingerprint matching process[1]. The authentication is successful if the matching score is better than a predefined threshold value. Fig: 2 show the enrolment and authentication phase for protection of the fingerprint combination.

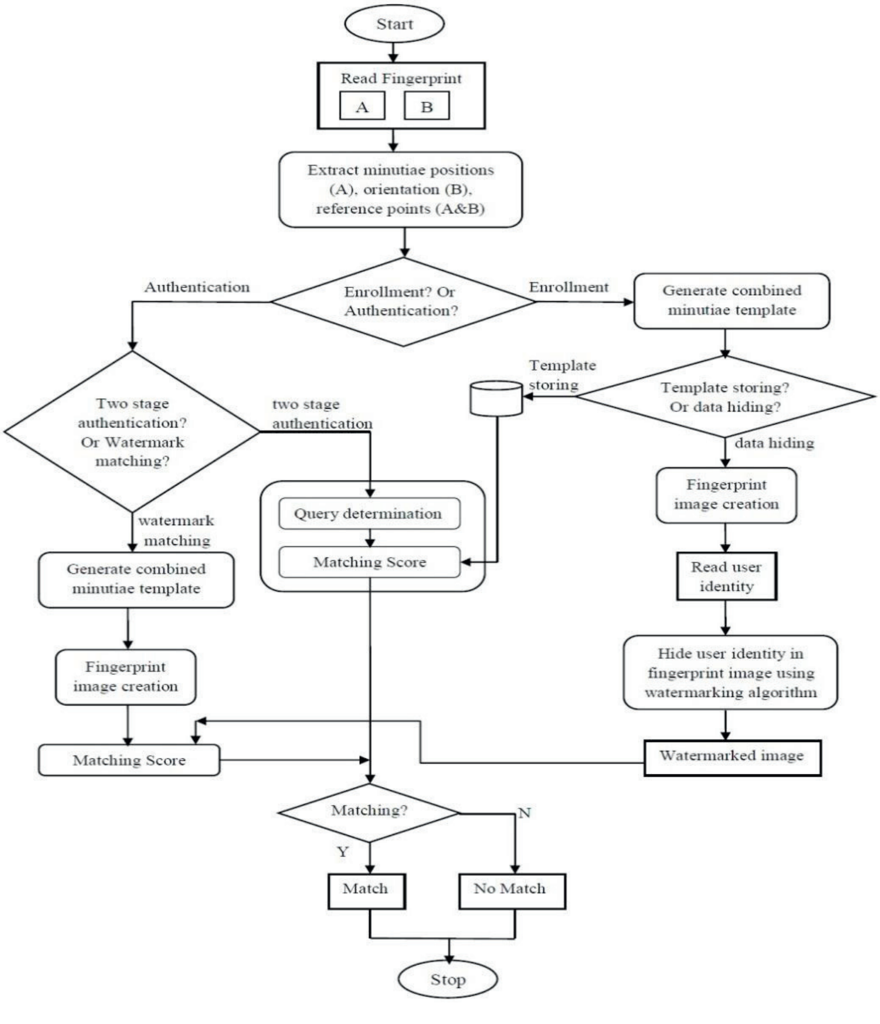

Start
Read Fingerprint
A
B
Extract minutiae positions (A), orientation (B), reference points (A&B)
Authentication
Enrollment? Or Authentication?
Enrollment
Generate combined minutiae template
Template storing
Template storing? Or data hiding?
data hiding
Two stage authentication? Or Watermark matching?
two stage authentication
Query determination
Matching Score
Fingerprint image creation
Read user identity
Hide user identity in fingerprint image using watermarking algorithm
watermark matching
Generate combined minutiae template
Fingerprint image creation
Matching Score
Watermarked image
Matching?
N
Y
Match
No Match
Stop

Fig. 1 Proposed System

2.1. Combined Fingerprint Generation

In a combined minutiae template, the minutiae positions and orientations are extracted from two different fingerprints separately and they shares similar topology with the original fingerprints. Therefore, the combined minutiae template has a similar topology to an original minutiae template. By using FM model based fingerprint reconstruction approach converts the combined minutiae template into a combined fingerprint image because of their similar topology. Given any two different fingerprints as input, first generate a combined minutiae template using the combined minutiae template generation algorithm[1]. Then, a combined fingerprint is reconstructed from the combined minutiae template using the fingerprint reconstruction approach [13].

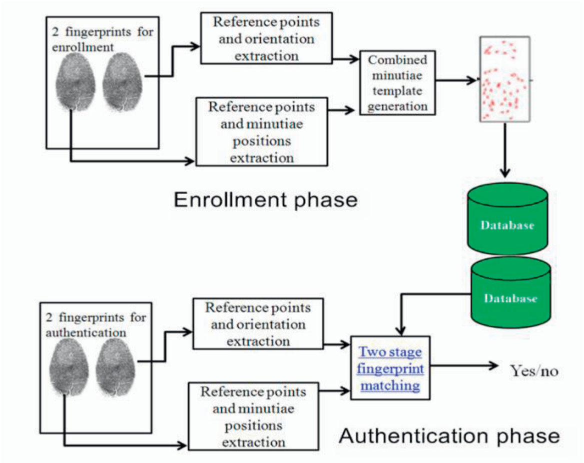

2 fingerprints for enrollment
Reference points and orientation extraction
Reference points and minutiae positions extraction
Combined minutiae template generation
Enrollment phase
Database
Database
2 fingerprints for authentication
Reference points and orientation extraction
Reference points and minutiae positions extraction
Two stage fingerprint matching
Yes/no
Authentication phase

Fig. 2 Enrolment and Authentication phase

2.2. Watermarking Algorithm

In this algorithm [9], user identity is combined with biometric identification during the authentication process. The user identity consists of name and an id. It is encoded using the SHA2 hash function which generates a unique hash value. SHA2 is a secure one-way hash function, so it is not possible to obtain a user identification number based on the hash value and it is infeasible to change a message without modifying its hash value. The hash value is then converted into binary and then converted into image as a watermark of size 256x256, equal to the size of the fingerprint image.

The Dual-Tree Complex Wavelet Transform (DTCWT) domain is used to embed the watermark data into fingerprint images. DTCWT removes the directionality and shift variance problems present in the wavelet transforms by using complex basis functions. For decomposition purposes, DTCWT uses directional filters. These directional filters are able to extract the same information, such as minutia locations, even after the watermark has been embedded into the image.

Multiplicative fusion is used to distribute the watermark evenly over the whole fingerprint image, including the real and imaginary parts, without affecting the information present in the fingerprint image. Then use the multiplicative fusion rule to combine the fingerprint image coefficients and the watermarked image coefficients after decomposition. The multiplicative fusion rule does not greatly affect fingerprint image coefficients due to the fact that the number of high value coefficients in the watermarked image is much less. In order to make the coefficients values very low, perform normalizing for the coefficients after the decomposing process. In this step, divide the DTCWT coefficients of that level to the average value of coefficients. Moreover, when decompose a fingerprint image using DTCWT, the high value coefficients correspond to the minutia points. Other continuous lines correspond to the low value DTCWT coefficients. By multiplying the watermarked image coefficients with the fingerprint image coefficients, these high values remain high and the distribution of minutiae points is not changed. In this way, the watermark is embedding into the fingerprint images. This algorithm relies on the information fusion-based approach. After that apply the inverse wavelet transform to retrieve the image domain and finally obtain the watermarked image.

Fig: 3 show the block diagram of the watermarking algorithm. The algorithm comprises the following steps:

- User information that identify the user, encode using hash function (SHA2)
- Convert hash value to binary image to construct water-marked image

- DTCWT is performed on both fingerprint and water-marked images up to 4 levels
- Combine fingerprint and watermarked image using multiplicative fusion rule
- To obtain watermarked image apply inverse DTCWT

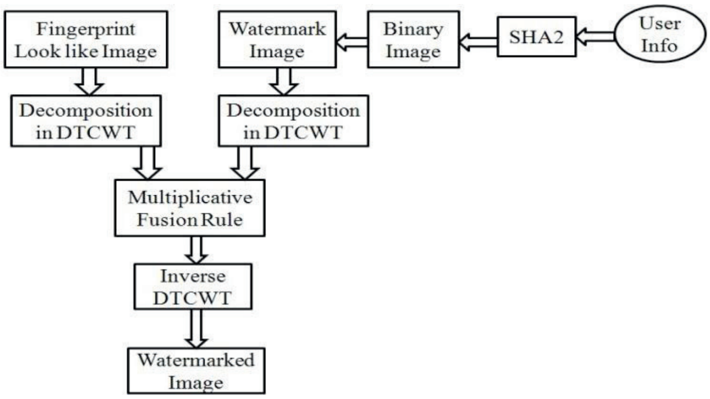


Fig. 3 Diagram of Watermark Algorithm

2.3. Watermark Extraction

To extract the watermark image, the following processes are applied

- Decompose template image and watermarked image using DTCWT
- Inverse the multiplicative fusion rule in embedding stage
- Obtain watermark coefficients of each level
- Perform inverse DTCWT to obtain watermark

Fig: 4 show the diagrammatic representation of watermark extraction steps.

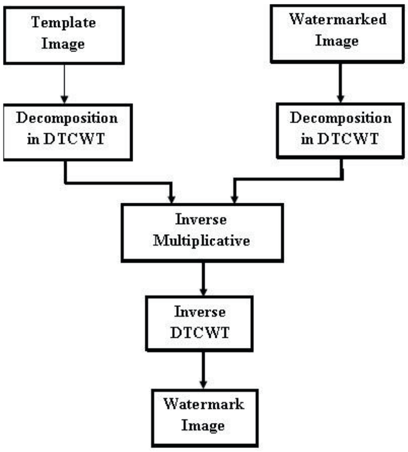


Fig. 4 Diagram of Watermark Extraction

3. Results

Identity of user thrashing and privacy protection of fingerprints has tested by using fingerprint dataset of different persons. The experiments are done using images having size 300 x 300. The main flow of the project is through enrolment and authentication phase. After the enrolment phase the identity of the user is thrashed into the generated fingerprint image of the particular person by using two fingerprint images of that person itself. Acquire two fingerprint images of a person from the dataset. Fig: 5a shows the selected fingerprint images. After acquisition extract termination and bifurcation points from the first finger as minutiae points' extraction. Extracted termination and bifurcation points are shown in fig: 5b. Figure also shows gray color image, black and white image and image after thinning. After thinning operation minutiae points are extracted. Here, threshold value T_P for converting gray image to black and white image by setting as 170. In the fig: 5b, first image is the gray colored image, second one is the binary image, third one shows the image after thinning, and the last image detect the termination point as circle and bifurcation point as star. At the meantime, estimate the orientation of finger2 as per the methodology. Estimated orientation is shown in fig: 5c. Reference point extraction of two fingers is carried out and which is shown in fig: 5d. The reference points of the two fingerprint images are shown as star.

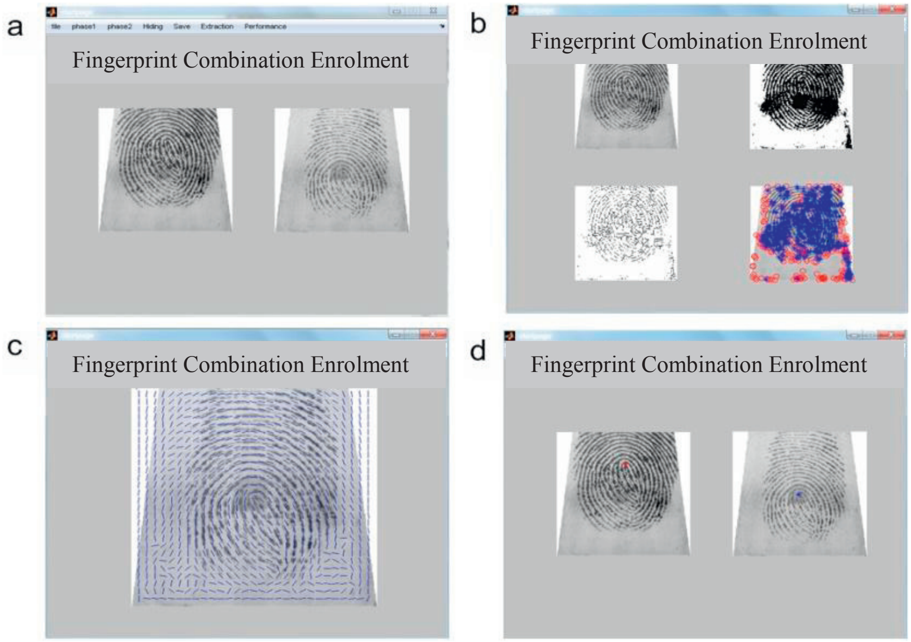

a
file phase1 phase2 Hiding Save Extraction Performance
Fingerprint Combination Enrolment
b
Fingerprint Combination Enrolment
c
Fingerprint Combination Enrolment
d
Fingerprint Combination Enrolment

Fig. 5a) Fingerprint acquisition b) Minutiae feature extraction c) Orientation estimation d) Reference point detection

Extracted information from the enrolment phase used to generate combined minutiae template. First estimate minutiae position alignment and minutiae direction assignment. By using these two information's generate combined minutiae template as shown in fig: 6a. Then, a combined fingerprint is reconstructed from the combined minutiae template using fingerprint reconstruction approach, FM model. The reconstructed fingerprint image is shown in the fig: 6b.

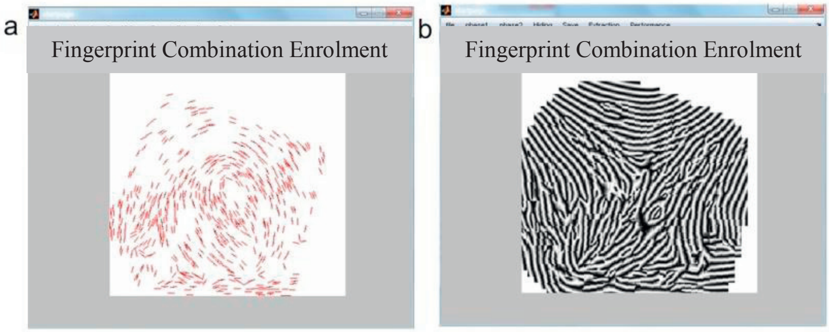
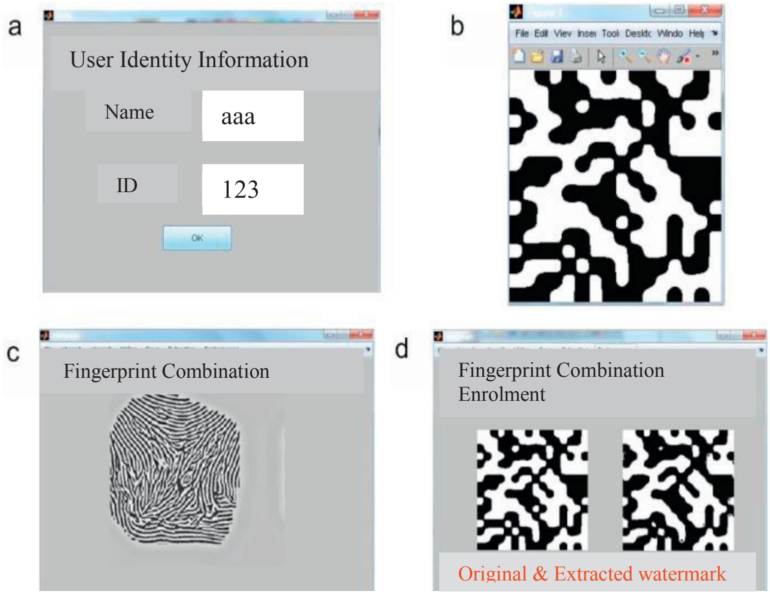

a
Fingerprint Combination Enrolment
b
Fingerprint Combination Enrolment

Fig. 6a) Combined minutiae template b) Reconstructed fingerprint image



User Identity Information

Name aaa

ID 123

Fingerprint Combination

Fingerprint Combination Enrolment

Original & Extracted watermark

Fig. 7a) Read user identity b) Watermark image c) Fused image d) Original and extracted watermark image

Next is user identity thrashing, for that read user name and id as shown in fig: 7a and construct a watermark image after SHA2 hash function as shown in the fig: 7b. After decomposition of reconstructed fingerprint image and watermark image, apply multiplicative fusion rule and generated watermark image by applying inverse decomposition. Fig: 7c shows the watermark embedded into the fingerprint image. After saving the combined minutiae template, extract watermark image from the fused image. Fig: 7d shows the original and extracted watermark image of the user identity. In that window, left side image is the original user identity watermark image and right side image is the extracted watermark image.

Authentication is the next main phase in the process flow. After reading the query fingerprints, extract minutiae points, estimate orientation and detect reference points as done in the enrolment phase. By using the two stage matching process authenticate the user by calculating the local features and construct combined minutiae template as first stage of the matching process and find out the valid user from the database by calculating the matching score between template in the database and query template. The system retrieves the name and id of the particular user from the database when the query fingerprints matches with the template in the database. If the better matching score value is not obtained then shows the user is not valid.

Perform an experiment to test the robustness of the proposed watermarking algorithm against image rotation and different types of image noises. To evaluate the robustness of the proposed watermarking technique against rotation, add some rotations to the fingerprint images. The original image is set as the template for comparison purposes and it is rotated on three different rotation angles 5, 10, 15. The watermark data is embedded only into the rotated images. Then, determine the matching score between the original and the watermarked images. Table I shows the matching scores between template image and rotated images after watermark embedding process. Angle 0 refers to the matching score between the template image and the watermarked image without rotation.

Table 1 Matching Score of different rotated images

Rotation Angles	**Matching Score**
0	0.86
5	0.8
10	0.8
15	0.79

Then test the algorithm against different types of noise attacks. Here use Gaussian noise with high noise variance, Salt and Pepper noise, Speckle and Poisson noise. Every type of noise exhibits different properties in the image. To evaluate the algorithm, here use PSNR (peak signal to noise ratio) as the measure. This ratio is used as the quality measure between the original image and the noisy image. High PSNR means the noisy image quality is high and the noisy image is similar to the original image. The algorithm results can preserve high PSNR values of watermarked images which mean noise attacks do not affect the fingerprint image much. PSNR is defined as;

$$PSNR = 10log_{10}\left(\frac{R^2}{MSE}\right)$$

where R is the maximum grey level of the image (for an 8-bit image R=255) and MSE is defined as mean squared error. According to the experiment, the proposed algorithm shows good performance under noisy conditions with PSNR value 50.9299.

4. Conclusion

The system is used for fingerprint privacy protection by combining two fingerprints into a new identity and user identity thrashing. Generate a combined minutiae template containing minutiae features of each of the two fingerprints captured in enrolment phase and stored in a database. In the authentication process, a two-stage fingerprint matching process is proposed for matching the two query fingerprints against the enrolled template. Reconstruct a fingerprint look like image from combined minutiae template. A new watermarking algorithm using DTCWT is used to thrash the user identity information into the fingerprint image to add more authentication factors to the authentication process. The robustness of the algorithm has been evaluated under different rotation angles and different kinds of noise attacks and a high level of robustness is achieved.

References

1. Sheng Li and Alex C. Kot, Fingerprint Combination for Privacy Protection, *IEEE Transactions on Information Forensics and Security*, vol. 8,No. 2,p. 350-360, Feb.2013
2. S. Li and A. C. Kot, Privacy protection of fingerprint database, *IEEE Signal Process. Lett.,* vol. 18, no. 2, p. 115-118, Feb. 2011.
3. A. Ross and A. Othman, Visual cryptography for biometric privacy, *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, p. 70-81, Mar. 2011.
4. B. Yanikoglu and A. Kholmatov, Combining multiple biometrics to protect privacy, Proc. *ICPR- BCTP* Workshop, Cambridge, U.K.,Aug. 2004.
5. A. 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. 29Dec. 2, 2011.
6. Rhoads G.B., Identification/authentication coding method and apparatus, *World Intellectual Property Organization*, vol. IPO WO 95/14289, 1995.
7. Juan R Hernandez, Martin Amado, and Fernando Perez-Gonzalez, Dct domain watermarking techniques for still images: Detector performance analysis and a new structure, *Image Processing, IEEE Transactions* on, 9(1):p. 55-68, 2000.
8. Mauro Barni, Franco Bartolini, and Alessandro Piva, Improved wavelet based watermarking through pixel-wise masking. *Image Processing, IEEE Transactions* on, 10(5):p. 783-791, 2001.
9. Mohammed Alkhathami, Fengling Han and Ron Van Schyndel Fingerprint Image Watermarking Approach Using DTCWT without Corrupting Minutiae, *6rd International Congress on Image and Signal Processing 2013 (CCISP 2013).*
10. Ravi J et al, Fingerprint recognition using minutiae score calculation, *International Journal of Engineering Science and Technology*, vol 22 2009 ,p. 55-62
11. Yi Wang *, Jiankun Hu, Fengling Han, Enhanced gradient-based algorithm for the estimation of fingerprint orientation fields, *ELSEVIER Applied Mathematics and Computation* 185 (2007) 823–833
12. K. Nilsson and J. Bigun, Localization of corresponding points in fingerprints by complex filtering, *Pattern Recognition. Lett.*, vol. 24, no. 13, p. 2135-2144, 2003.
13. Jianjiang Feng and Anil K. Jain, FM Model Based Fingerprint Reconstruction from Minutiae Template, *ICB 2009*