DOI: 10.21917/ijivp.2013.0094

A STRONG SECURITY PROTOCOL AGAINST FINGERPRINT DATABASE ATTACKS

U. Latha[1] and K. Ramesh Kumar[2]
[1]*Department of Information Technology, Dhaanish Ahmed College of Engineering, India*
E-mail: latha_umapathy1@yahoo.co.in
[2]*Department of Information Technology, Hindustan University, India*
E-mail: krkumar@hindustanuniv.ac.in

Abstract
The Biometric data is subject to on-going changes and create a crucial problem in fingerprint database. To deal with this, a security protocol is proposed to protect the finger prints information from the prohibited users. Here, a security protocol is proposed to protect the finger prints information. The proposed system comprised of three phases namely, fingerprint reconstruction, feature extraction and development of trigon based security protocol. In fingerprint reconstruction, the different crack variance level finger prints images are reconstructed by the M-band Dual Tree Complex Wavelet Transform (DTCWT). After that features are extracted by binarization.A set of finger print images are utilized to evaluate the performance of security protocol and the result from this process guarantees the healthiness of the proposed trigon based security protocol. The implementation results show the effectiveness of proposed trigon based security protocol in protecting the finger print information and the achieved improvement in image reconstruction and the security process.

Keywords:
Fingerprint Reconstruction, Complex Wavelet Transform (CWT), 2D Dual Tree Complex Wavelet Transform (DTCWT), Trigon Based Security Protocol, Binarization

1. INTRODUCTION

The measurement of biological data is known to be Biometrics. To make sure the certification of an individual by investigating the physical characteristics, such as fingerprints, handprints, eyes and voice, or the behavioral characteristics, such as signatures [5], the phrase biometrics is frequently used at these days. In the present day, fingerprint technology is the most broadly used technique in individual recognition and it has nearly become the synonym of biometrics [6] [7].

A model of ridges and valleys is a fingerprint image, with ridges as dark lines while valleys as light areas among the ridges. Commonly ridges and valleys run corresponding to each other, and their patterns can be determined on a worldwide and local level [8]. In the fingerprint pattern, minutiae are local discontinuities. Forged ridge arrangement may vary the individuality of input fingerprints. Ridges and valleys has a well-defined frequency and orientation in a local area form a sinusoidal-shaped plane wave [9]. Massive numbers of fingerprints are captured and stored every day in a extensive range of applications such as forensics, access control, and driver license registration.

On the other hand, recognizing unfinished fingerprints from fingerprint database ruins a difficult challenge today. Emergence of incomplete fingerprint from a lot of scenarios can be found. Consequently, they may not provide accommodation for sufficient minutiae or ridge details for undertaking a normal matching process [10]. As a result the repairing of incomplete regions in fingerprint images correctly and efficiently and thereby guaranteeing the subsequent matching and other processing has to be settled immediately. We describe our proposed fingerprint security protocol process is briefly explained in Section 2. The experimental results and the conclusion of the paper are given in section 3 and 4.

2. PROPOSED SECURITY PROTOCOL

The proposed security system comprised of three phases, namely, fingerprint image reconstruction, feature extraction and development of security protocol. In our proposed system, the given input fingerprint image is reconstructed by the DTCWT and that reconstructed image features are extracted by the morphological operations. The extracted features from the fingerprint images are stored in the feature database and that database information is need to be protected from the unauthorized users. Hence, we provide a security for the fingerprint information by developing a trigon based security protocol using the valid user's username and password. The structure of our proposed security system is given in Fig.1.

2.1 FINGERPRINT IMAGE RECONSTRUCTION

The given input fingerprint image is to be reconstructed by decomposing the input cracked fingerprint images via 2D DTCWT. The reconstructed image is obtained by analyzing the sub band and the coefficients form the wavelet transform in different direction.

The steps for fingerprint reconstruction is,

(i) Initial Value Assignment by NN algorithm

(ii) 2D DTCWT Processing

(iii) Coefficients Thresholding

(iv) Reconstruction

The value assignment process is initiated by finding the closest entries and replaced by the Nearest Neighbor (NN) algorithm. The fingerprint image is given to the wavelet process after the initial value assignment process. The M-band 2D dual Tree Complex Wavelet Transform (DTCWT) is used in our proposed technique which contains the unique geometrical features for frequency domain conversion. Local, multi-scale directional analysis is provided by this decomposition. Cascading of M-band filter banks are kept in the wavelet

transform. We get the M-band trees obtained by performing two M-band multi resolution analyses in parallel in the real case, or four in the complex case respectively. The coefficients values are acquired from the wavelet transform and then the thresholding process is performed by initially creating the diagonal matrix is obtained.

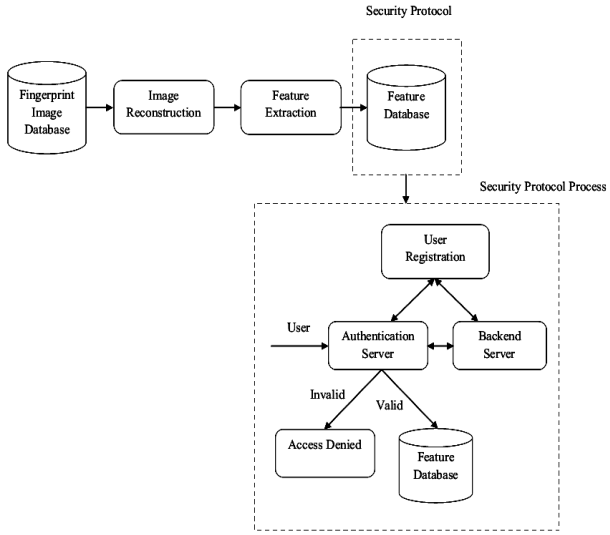

Fig.1. Structure of Our Proposed Security System

2.2 FEATURE EXTRACTION

After the image reconstruction process, the features are extracted from the fingerprint reconstructed images. The features extraction process is performed in two steps, namely, binarization and morphological operations. Before the binarization process the reconstructed fingerprint images are given to the segmentation and image enhancement process. In segmentation the image is divides into number of blocks and in each block the gradient value is calculated. Based on the gradients standard deviation and the threshold values the blocks values are filled with ones or zeros. Thus the segmented image is given to the image enhancement process to get the accurate minutiae point extraction. The segmented and enhanced image is provide to the binarization process.

2.2.1 Binarization:

Binarization is the process of converting a grey level image into a binary image. It improves the contrast between the ridges and valleys in a fingerprint image, and thereby facilitates the extraction of minutiae. The grey level value of each pixel in the reconstructed image $r_{(i_n)_{xy}}$ is examined in the binarization process. The binarization process is performed by,

$$B\left(r_{i_n}\right)_{xy} = \begin{cases} 1; \text{ if } p_{xy}^{i_n} \geq t \\ 0; \text{ otherwise} \end{cases} \quad (1)$$

In Eq.(1), the grey value is greater than the threshold value means the pixel value is set to a binary value one; or else, it is set to zero. The output of binarization process is a binary image containing two levels of information, the foreground ridges and the background valleys.

2.2.2 Morphological Operation:

Following the binarization process, morphological operators are applied to the binarized fingerprint image. The objective of the morphological operations is to eliminate obstacles and noise from the image. Furthermore, the unnecessary spurs, bridges and line breaks are removed by these operators. The process of removal of redundant pixels till the ridges become one pixel wide is facilitated by ridge thinning. The resultant fingerprint image produced by the morphological thinning algorithm composes of ridges each one pixel wide. This improves the visibility of the ridges and enables effective and effortless of minutiae points.

2.3 DEVELOPMENT OF TRIGON BASED SECURITY PROTOCOL

The trigon based security protocol [12] is developed to protect the fingerprint feature information from the invalid users. The feature values i.e. the ridges values from the feature extraction process are stored in the feature database f_D. The database f_D comprised of three fields $f_D = \{u_n, p_n, R_n\}$ where u_n is the given input fingerprint image corresponding user name, p_n denotes the password, R_n is the image ridge values and n represents the total number of users images. Based on the corresponding fingerprint image users, username and password the security protocol is to be developed. The trigon based security protocol is composed of three steps,

(i) Registration process

(ii) Users Verification

(iii) Validation

2.3.1 Registration Process:

During the registration process, the valid users register their username and password in Authentication and Backend server. Initially, the database users register their username and password in the authentication Server. At that time, the Authentication server randomly generates two prime numbers n_1, n_2, which are considered as the two sides of a trigon. The angle between these two prime values n_1, n_2, is denoted as a_i. Now, the Authentication server can easily determine the opposite side of the angle a_i, termed Units as n_3. With these trigon parameters, the user determines s, $V_{n_1 n_2}$ and $P_{n_1 n_2}$ as follows,

$$V_{n_1 n_2} = n_1 - n_2 \quad (2)$$

$$P_{n_1 n_2} = n_1 - n_2 \quad (3)$$

$$s = 2P_{n_1 n_2} - n_3^2 \quad (4)$$

where n_1, n_2 and n_3 and are the three sides of the trigon, s is a strengthening parameter used as the index to represent user credentials, $V_{n_1 n_2}$ and $P_{n_1 n_2}$ are the Variance and the product of the sides n_1 and n_2 respectively. After the calculation of these

values, the Authentication Server stores the s and forwards the $V_{n_1n_2}$ and $P_{n_1n_2}$ to the Backend Server along with the username.

2.3.2 Users Verification:

After the valid users registration process, if any user enter to access the fingerprint information from the database f_D means, the Authentication server checks whether the corresponding queried user is a valid user or not. The process of user's verification by the Authentication server is described below,

Step 1: Authentication Server gets the user name u_n and password p_n from the nth user.

Step 2: Authentication Server computes the key value for the password by,

$$PK_n = \begin{cases} \dfrac{A_{p_n}}{10^{m-2}}; & \text{if } A_{p_n}(l) \geq 180 \\ \dfrac{A_{p_n}}{10^{m-3}}; & \text{else} \end{cases} \quad (5)$$

In Eq.(5),

A_{p_n} – is the ASCII-interpreted value of the given password p_n

m – is the total number of digits in A_{p_n}

$A_{p_n}(l)$ – represents the first l digits of A_{p_n}

Step 3: Afterward, the Authentication Server computes the Authentication Key for the user u_n by,

$$AK_n = \frac{PK_n}{2} \quad (6)$$

After that the Authentication server send the s_n is sent to the backend server along with u_n.

2.3.3 Validation:

In validation, the backend servers validate the information from the Authentication Server. The backend Server receives the s_n and the username u_n from the Authentication Server. After receiving the s_n and u_n, Backend server searches the s_n corresponding $V_{n_1n_2}$ and $P_{n_1n_2}$ values, which have been already stored in the server database during the registration. Based on the corresponding user values in Backend Server, computes the authentication Token AT_n and sends it to the Authentication server to authenticate the u_i. The AT_n can be calculated as,

$$AT_n = \frac{s_n + V_{n_1n_2}^2}{2P_{n_1n_2}} \quad (7)$$

In Eq.(6), $V_{n_1n_2}$ and $P_{n_1n_2}$ are pre-calculated values computed during individual user registration. After the retrieval of AT_n from the Backend server, the Authentication server authenticates the user based on the token from the Backend server and the key value is calculated at the Authentication server. The condition which is given in Eq.(7), is satisfied means thus the given user is valid to access the feature database otherwise the access is denied.

$$\sin(AK_n) = \left(\frac{1 - AT_n}{2}\right)^{1/2} \quad (8)$$

The users which are satisfy the Eq.(7), they are allowed to access the feature database f_D. By exploiting the aforementioned process our proposed trigon based security protocol protects the fingerprint information from the unwanted users.

3. EXPERIMENTAL RESULTS AND DISCUSSION

Initially the given sample fingerprint images from the fingerprint database FVC 2002 are reconstructed by the DTCWT technique. The sample fingerprint and the reconstructed results images are shown in Fig.2 and Fig.3.

Fig.2. Sample Fingerprint Images

Fig.3. Reconstructed Image Results

The extracted feature values and the feature extraction process result images are illustrated in Fig.4 and Table.1.

(a) (b) (c) (d) (e)

Fig.4. Result Images from Feature Extraction (a) Segmentation (b) Image enhancement (c) Morphological Operation (d) Minutiae Extraction and (e) Final result

Table.1. Extracted Feature Values

Image	Feature Values
1	(82,19), (45,40), (193,40), (182,42), (159,45), (117,46), (78,54), (129,57), (85,60), (115,60), (131,75), (147,81), (121,85), (227,86), (138,88), (162,88), (40,89), (49,101), (136,121), (195,123), (80,136), (161,157), (44,161), (227,161), (124,34), (133,34), (142,34), (167,37), (56,38), (55,50), (144,50), (35,57), (206,58), (101,60), (147,100), (161,100), (147,101), (127,103), (166,106), (168,116), (242,118), (90,122), (244,122), (147,123), (80,124), (144,131), (38,134), (243,141)

The extracted feature values from the fingerprint images are stored in the feature database and that the database information is protected by our security protocol. The protocol is tested with five valid and five invalid users. Each of the five valid users has their own username and password. Initially, the user registration process is performed to evaluate the valid and invalid users in the feature database access. The fingerprint images and the corresponding username, password and trigon parameters of the five users are given in Table.2.

Table.2. Usernames, Passwords and the trigon parameters at the time of registration

Number of users	User Name	Password	s	$V_{n_1n_2}$	$P_{n_1n_2}$
1	U1	Hello	-25	-5	14
2	U2	WELCOME	1.60E+01	4	77
3	U3	HAI	0	0	49
4	U4	Rose	2.50E+01	5	14
5	U5	sample	-25	5	14

The five valid user's username, password and trigon parameters have been given in Table.1. These five users are the valid users to access the feature database. The α values for the five valid users mentioned in the Table.1 have been stored in the authentication server and $V_{aa'}$ and $P_{aa'}$ have been stored in the Backend server for the corresponding usernames. When the servers authenticate any user, the servers determine some authentication elements based on the values which have been stored in the database and the login credential provided by the user. Our proposed security protocol performance result of five valid and invalid users' authentication elements and that database access is given in Table.3.

As can be seen from Table.3, ten users can try to access the feature database f_D. Among the ten users five users are authenticated and other users are unauthenticated users. The authenticated five user's authenticated elements are computed and verified by the authentication and backend servers. Based on the verification result from the both servers, the users are allowed to access the feature database. Other five users try to access the database by giving wrong passwords but the passwords are most similar to the authenticated user's password. The authenticated elements are also computed for these unauthenticated users and verified by the authentication and backend servers. The servers easily find out these invalid users by comparing those users with the authenticated users. Thus our trigon based security protocol more secure in protecting the fingerprint information from the unwanted users.

4. CONCLUSION

In this paper, we have proposed a trigon based security protocol to protect the fingerprint information from the prohibited users. The proposed fingerprint security protocol performance was evaluated by using the more number of fingerprint images. The experimental results proved that our proposed Trigon based fingerprint security protocol has given high performance security when protect the fingerprint information from the illicit users. The proposed trigon based protocol performance in protecting fingerprint information was tested with authenticated and unauthenticated users. When the unauthenticated users try to access the feature database, our proposed security protocol eliminates their access based on their authenticated elements. Hence, it is proved that our proposed trigon based security protocol more securely protect the information from the illegitimate users.

Table.3. Performance of proposed security protocol

No. of users	User Name	Password	PK_n	AT_n	AK_n	$\sin(AK_n)$	$\left(\frac{1-AT_n}{2}\right)^{1/2}$	Authentication	Access
1	U1	Hello	14318.03	-1.07143	7159.013	0.626472	1.071429	Valid	Allowed
2	U6	Helo	14318.03	-0.2	7159.013	0.626472	0.2	Invalid	Denied
3	U3	HAI	6918.164	0	3459.082	0.187522	0	Valid	Allowed
4	U8	HI	5418.18	-0.28571	2709.09	0.860949	0.285714	Invalid	Denied
5	U2	WELCOME	6.62E+03	-7.79E-02	3310.962	0.272941	0.077922	Valid	Allowed
6	U7	welcome	3629.775	-0.28571	1814.888	0.815108	0.285714	Invalid	Denied
7	U4	Rose	4.52E+03	-7.14E-01	2260.264	0.993732	0.714286	Valid	Allowed
8	U5	sample	1528.993	-0.71429	764.4964	0.886336	0.714286	Valid	Allowed
9	U9	rose	10528.53	-0.16667	5264.264	0.865124	0.166667	Invalid	Denied
10	U10	samples	2.43E+03	-6.67E-02	1214.496	0.96355	0.066667	Invalid	Denied

REFERENCES

[1] Muna F. Hanoon, "Contrast Fingerprint Enhancement Based on Histogram Equalization Followed by Bit Reduction of Vector Quantization", *International Journal of Computer Science and Network Security*, Vol. 11, No. 5, pp. 116-123, 2011.

[2] Arun A. Ross, Jidnya Shah and Anil K. Jain, "Towards Reconstructing Fingerprints from Minutiae Points", *Proceedings of SPIE Conference on Biometric Technology for Human Identification II*, Vol. 5799, pp. 68-80, 2005.

[3] Brendan Babb, "Evolved Transforms Surpass the FBI Wavelet for Improved Fingerprint Compression and Reconstruction", *Proceedings of the GECCO Conference Companion on Genetic and Evolutionary Computation*, pp. 2603-2606, 2007.

[4] Jianjiang Feng and Anil K. Jain, "Fingerprint Reconstruction: From Minutiae to Phase", *IEEE transactions on Pattern Analysis and Machine Intelligence*, Vol. 33, No. 2, pp. 209-223, 2011.

[5] K. Srinivasan, C. Chandrasekar, "An Efficient Fuzzy Based Filtering Technique for Fingerprint Image Enhancement", *American Journal of Scientific Research*, No. 43, pp. 125-140, 2012.

[6] Dhruv Batra, Girish Singhal and Santanu Chaudhury, "Gabor Filter based Fingerprint Classification using Support Vector Machines", *Proceedings of the IEEE India Annual Conference*, pp. 256-261, 2004.

[7] Muhammad Umer Munir and Muhammad Younas Javed, "Fingerprint Matching using Gabor Filters", *National Conference on Emerging Technologies*, pp. 147-151, 2004.

[8] Avinash Pokhriyal and Sushma Lehri, "A new method of fingerprint authentication using 2d wavelets", Journal of Theoretical and Applied Information Technology, Vol. 13, No. 2, pp. 131 – 138, 2010.

[9] Poramate Prasarn, Keokanlaya Sihalath and Somsak Choomchuay, "A dynamic enhancement method for fingerprint matching", *The 3rd Biomedical Engineering International Conference*, pp. 237-241, 2010.

[10] Jie Zhang, Bo Zhang, Xinjing Liu and Xiaojun Jing, "A Matching-Improved Reparation Method for Incomplete Fingerprint", *Proceedings of IEEE International Conference on Cloud Computing and Intelligence Systems*, pp. 75-79, 2011.

[11] Yang Jian-Bin, "Image inpainting using complex 2-D dual-tree wavelet transform", *Applied Mathematics – A Journal of Chinese Universities*, Vol. 26, No. 1, pp. 70-76, 2011.

[12] Anitha K. K, Sudha S. G., Megala A and Aishwarya S, "Trigon Based Authentication Service Creation with Globus Middleware", *Proceedings of the International Conference on Process Automation, Control and Computing*, pp. 1-6, 2011.