Gabor-based Fingerprint Authentication for Anti-phishing System

Dr. Soukaena H. Hashem
Computer Science Department, University of Technology/Baghdad.
Dr. Rehab F. Hasan
Computer Science Department, University of Technology/Baghdad.
Rajaa K. Hasoun
Computer Science Department, University of Technology/Baghdad.
Email:rajaamena@yahoo.com

Received on:27/8/2015 & Accepted on:21/4/2016

ABSTRACT

E-banking is banking system in which the customers conduct transactions electronically via the Internet. Most of these sites are prone to a phishing attack. The usual fears with phishing attack are that the user may be an attacker and impersonating the identity of the authorized user, but the most dangerous in E-bank that the website which is to be hacker (phisher website), and this will lead to steal sensitive information of customers. The trend of this research is to introduce proposed security system represent "E-bank website anti-phishing attack". The proposal tries to prevent that the security concerns remain on the attacker impersonating an authenticateduser. In traditional authentication techniques, such as use of username and password is not sufficient for securing E-banking system. The reason of using fingerprint in authentication is based on fingerprint individuality. The proposal introduces a suggested treatment of pattern recognition of fingerprint with lowest False Acceptance Rate "FAR" and False Rejection Rate "FRR" among all traditional fingerprint authentication mechanism. The proposal enhances the traditional recognition system by applying Gabor filter during the preprocessing stage which makes our proposal able to recognize the rotated impression, so the accuracy of fingerprint matching is improved.
Keywords: fingerprint, Gabor filter, authentication and phishing attack.

INTRODUCTION

Today, financial organizations rely on IT infrastructures such as E-exchange, E-marketing and E-banking. E-banking is known as delivering of banking product and service directly to customer through the internet [1]. So with the increased use of the internet, different types of attacks have been grown and one of themis phishing [2].Phishing is a try by person or a group to gain access to the sensitive information like password, credit details to use the person private identifying information usually for financial gain by pretending to be from trustworthy or public organization [2]. Anti-phishing it the process of saving users'sensitive information and keeping this information from leakage to any website that is not "trusted". So there is a need for reliable and secured authentication mechanism [3].

The fingerprint is the constructing of a pattern of lines which known as Ridge and each individual ridge is separated by spaces named as valleys.Ridges itself comes with end or split into two ridges, the point where one ridge is splitting into two ridges is called bifurcation and the place where the Ridge terminated is called termination [4].Terminations and Bifurcation are the two basic types of interesting thing of the fingerprint part which is called minutiae**;** Minutia is the interesting point for fingerprint recognition. Fingerprint study is not new method it's

https://doi.org/10.30684/etj.34.5B.4
2412-0758/University of Technology-Iraq, Baghdad, Iraq

fromtheseventieth century where fingerprint recognition was manually and there was something like art for this method, and it being developed until it comes automated [5].
The fingerprint verification system can classify in term of extracted feature into two kinds [4, 5] global and local features.Global features; describe the fingerprint image as a whole. Ridge flowing is compared at all position between any two fingerprint images. The flow of ridges composes global pattern of the fingerprint. There are two other features sometimes used in matching: core and delta. Global features include different fingerprint patterns such as, Loop and Whorl. The core is the center of fingerprint Patterns. The delta can be described as a unique point from which three patterns diverge. Figure (1) shows three types of patterns.

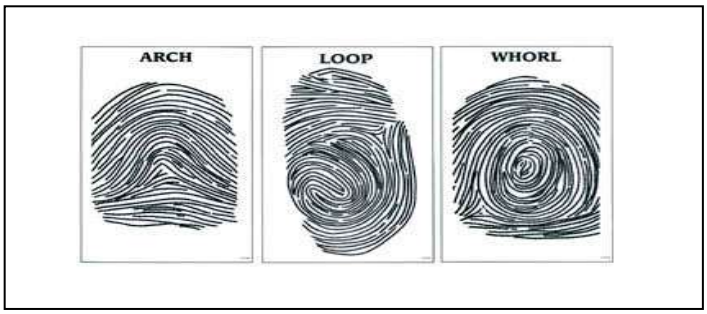

Figure (1) Types of Fingerprint patterns

Local features, is called local processing of fingerprint such as minutiae matching. There are following minutiae types as explain in figure (2). "Ridge ending": It is features which indicate terminate or end of ridge. "Bifurcation": it is a feature which indicates a point at which ridge split into parts."Enclosure": Formation where ridge bifurcation and rejoin to be one in short distance."Island": it is a line which is stand alone. (That means it does not touch any other linein the pattern area of interest.). "Delta": It is a triangular pattern and it's considered as ridges meeting of different fingerprint. "Core": it refers to the center area of a fingerprint. A fingerprint may have many cores or no one [6, 7].

Figure (2) Fingerprint minutiae: ending and bifurcation.

The fingerprint recognition system can be evaluated by measuringits false reject rate "FRR" and false accept rate "FAR". The threshold value of matching score is deciding whether rejects or accepts matching. If it takes less value of the threshold this means the probability of accepted imagewill be high and rejected image will be low, so chances of error occurring will be increased and vice versa [8,9]. In traditional there are the two probabilities these are: two fingerprints from two different persons may produce a high Matching Score (an error); or two

fingerprints from the same person may produce a low Matching Score (an error). So as usual in all systems there are two types of error [4, 6]:

a. FAR is equal to ratio of number of instances of pairs of different fingerprints found to (erroneously) match to total number of match attempts.

b. FRR is equal to the ratio of the number of instances of pairs of same fingerprint are found not to match to total number of match attempts.

Related Works

The following related work will present fingerprint recognition system as much as related to the proposal:

In 2004, Munir M. et al.; they proposed two different techniques for core detection, a circular region around these core point located and tessellated into 128 sectors. This region is filtered using a bank of 60 Gabor filtered to produce a set of sixteen filtered images. The average absolute deviation within a sector quantifies the underlying ridge structure and used as feature vector [10]. In 2008, Aguilar G. et al.; they proposed in this work a method for fingerprint recognition by using combination of fast Fourier transform and Gabor filters for image enhancement [11] . In 2011, Mudegaonkar P. et al.; they propose fingerprint identification based on bank of Gabor filter, initially find core point, circular region around the core point was tessellated into 80 sectors these region was filtered using bank of eight Gabor filter and then extract the feature vector, when applying the proposed procedure on FVC 2000 database got 98.22% accuracy [12].In 2011, Muhammad; proposed method to protect privacy of digital biometric data (e.g. fingerprint image) that stored in central database, scrambling the fingerprint image by applying permutation algorithm and then using visual cryptography in order to decompose the image into two sheets and stores in two different database, so it is impossible to construct the scrambled image without accessing both shares and apply XOR operator to superimpose the two noise image in order to get the scrambled image [13].In 2012, Sharma; explore new approach to generate key by using fingerprint. In this work also describe some of the used technique for generation and extraction of minutia point from fingerprint. In this proposal the input image is converted to binary image and then apply thinning process in order to reduce thickness of lines, after that marking minutia point is relatively easy, false minutia are removed, so the set of generated minutia need to be reduced to derive 64 bit set. Original minutia set is repeated until 64 bit key is obtained [14]. In 2012, Gopi K. et al.; they proposed in this work a method for fingerprint recognition by using combination of fast Fourier transform and Gabor filter to enhance the image [15]. In 2012, Hongchang K. et al.; they proposed new method by using Gabor filter for fingerprint image enhancement, the method consist of two steps, step 1:enhance image by using Sobel filter and then using Gabor filter as second step of enhancement [16].In 2013, Patel et al.; they have proposed anti-phishing technique to prevent users from phished pages by using fingerprint of the user and its ID and password during initial registration or sign up .this technique make user sure about the legitimacy of web page he visits where he is already registered, so no phisher can access to the user account because the two level of authentication and verification (i.e. fingerprint verification and code verification with pattern matrix [17]. In 2015, Azzoubi e. et al.; they proposed algorithm for fingerprint recognition that includes using bank of Gabor filter after determining the core point and tessellate the region of interest to be input to the five Gabor filter to produce feature vector [18].

The Proposal of Anti-Phishing

The proposed system consists of two main phases: Registration phase and Identification phase (login phase), as shown in figures (3) and (4).

In registration phase; the user will interact with the bank website and enter the key (user name and password) and fingerprint image which is stored in a file, pattern recognition process will be done to generate user template and store it in the server database. The database will be

encrypted, so this process will protect biometric data that stored in centralized database because it's vulnerable to eavesdropping and attacks, the website will display a unique image captcha for that user in order to verify the bank website is trusted website and not phishing site. In identification phase (login), user will log in by entering his key (user name and password) in order to use his/her account. Next the user is asked to enter his fingerprint image that's stored on file, pattern recognition process will be done in order to compare the produced template with stored template in server database, if no match occurs then the server will know that the user is a hacker and cannot access the account. But if there is a match, the user is allowed to enter the system, but the user still confused this website is phishing until displaying the captcha that is related to that user. By this step the user will be sure the bank site is trusted and not a phishing site.

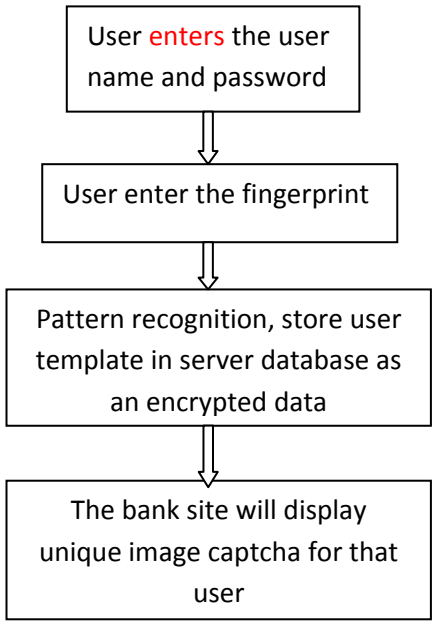

Figure (3) Block diagram of registration phase

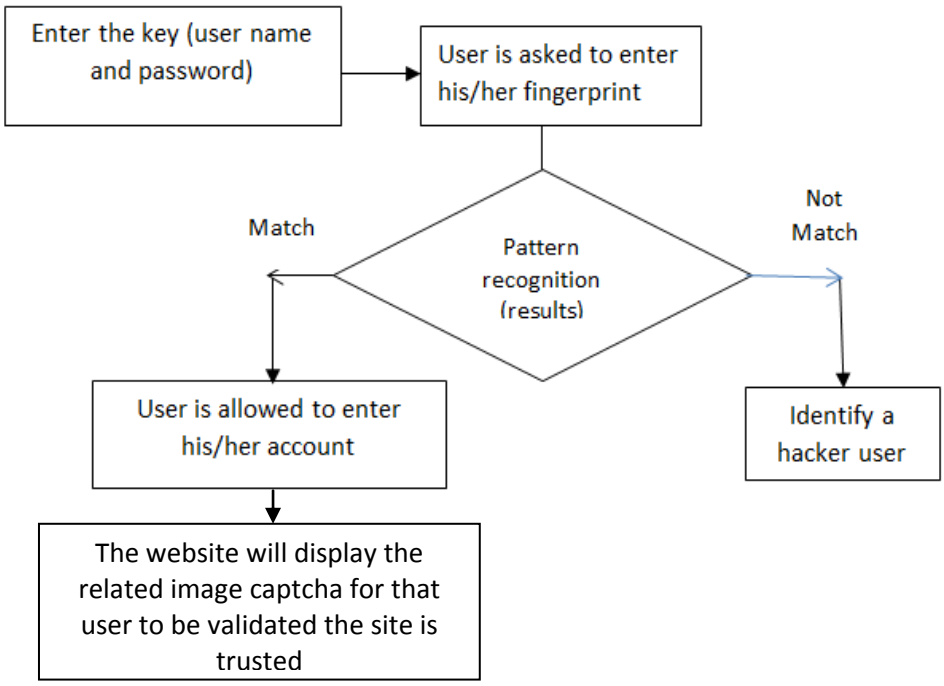

Figure (4) The general block diagram of login phase/ authentication

Proposed Fingerprint Recognition

This stage consists of the following steps: preprocessing, minutia extraction,Post-processing and fingerprint matching.

Preprocessing

This stage consists of the following steps

Image Enhancement

In this step used combination in spatial domain and frequency domain in order to use the complete advantages of each domain. So in this steps use histogram equalization in spatial domain and Gabor filter in frequency domain. Unlike most of the related work which is used "fast Fourier transform" because the "Gabor filter" is (Gaussian * Fourier) and in addition to when using fast Fourier transform some noise may appear and this required to use the histogram again before next step which is binarization, and this is time consuming.

When applying histogram equalization, first for each gray level in fingerprint image find number of pixels with gray level (k) and then calculate the cumulative frequency, after this step find maximum gray level and number of pixels, for more explanation see algorithm (1) step1 and figure (5) which show the original fingerprint image and enhanced image by using histogram equalization. Second steps of image enhancement by using Gabor filter, first step initialize the parameter in practical to the following values:

a. Wavelength (lambda λ)" cosine factor of Gabor function" which is determine in pixels, accepted value are real number in the range (2to 256), so λ=8.

b. "Orientation (theta θ)": determine the orientation which is specified in degree, accepted values are real numbers in the range (0 to 180), so θ=0.

c. "Phase offset (phiΦ)": determine the phase offset of "cos factor of the Gabor function", it'sgiven in degree, accepted values are real numbers in the range (-180 to 180), phi=[0 pi/2].

d. "Aspect ratio (gammaσ)": determine the ellipticity of the "Gaussian factor". Accepted values lie between 0.2 and 1, so gamma=0.5.

e. Bandwidth (BW): determine spatial frequency band width of Gabor filter when it is used as a filter kernel, values lie between 0.4 and 2.5, so bw=1.

In practical Gabor enhancement, ridge direction is quantized into 8 directions 0^0, 22.5^0, 45^0, 67.5^0, 90^0, 112.5^0, 135^0, 157.5^0. So initial value of theta=0^0 and need eight iteration to implement these eight directions and increment of theta became 22.5.In each iteration calculate real component of Gabor function, where x-theta and y-theta. For more details see algorithm (1) Step2 and figure (6) which show the fingerprint image after enhanced by using Gabor filter.

Algorithm (1) Fingerprint Image Enhancement
Input: Original fingerprint image Output: Enhanced fingerprint image
Process Step 1: Histogram equalization For each gray level $0 \leq i \leq 2 \leq 55$ do Find number of pixel with each gray level H(k) Find the cumulative frequency C(i)=$\sum_{k=0}^{i} H(k)$ Find maximum gray level M Find number of pixels N Histogram equalization replace i with I=$C(i) * \frac{M}{N}$ Step 2: Gabor filter Initialize parameter (λ, θ, Φ, σ, bw)

$Sigma - x = \lambda$
$sigma - y = \frac{\lambda}{6}$
For I=1 to 8 do
$x - theta = x * cos(theta) + y * sin(theta);$
$y - theta = -x * sin(theta) + y * cos(theta);$
$gb = (-0.5 * (x - theta\text{^}2/sigma - x\text{^}2 + y - theta\text{^}2/sigma - y\text{^}2)) * cos(2 * \pi/lambda * x - theta + psi);$
theta=22.5*I
end for
End process

Figure (5) Image enhancement by histogram equalization

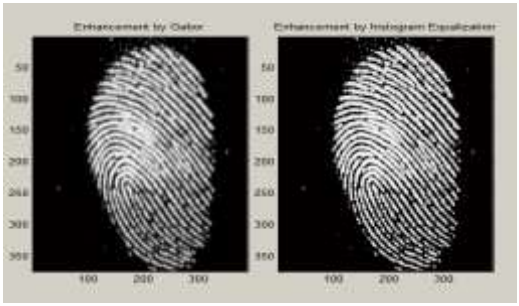

Figure (6) image enhancement by Gabor filter

Image Binarization

In this step the gray scale image will be binarized, it will be in black and white (i.e. array of '0' and '1' elements) this done by choosing carefully threshold value. And the value for image over the threshold value become 1 (black) and value less than threshold will be 0(white). By experience threshold value is equal to 0.8. See algorithm (2) and figure (7) which show the image after applying binarization process.

Algorithm(2) Fingerprint Image Binarization
Input: Enhanced fingerprint image Output: binarized image

Process
Threshold=0.8
For each pixel in image do
If value of pixel > threshold then
Value of Pixel =1
Else
Value of pixel =0
End for

End process

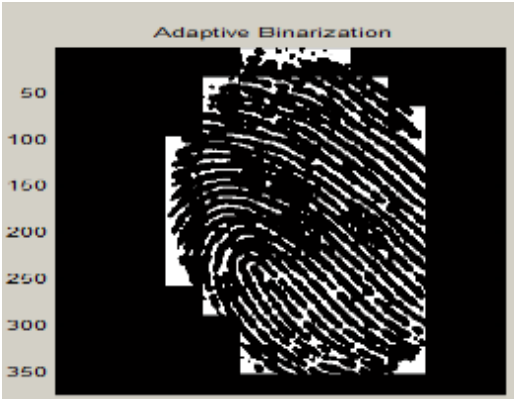

Figure (7) image binarization

Image Segmentation

There are two steps for image segmentation which is block direction and region of interesting.

A. Block Direction, the horizontal and vertical value (g_x, gy)must be computed for all pixels in the enhanced image by applying Sobel mask in both direction(vertical and horizontal). The gradient magnitude and gradient direction is computed. When applying this process for each block, the unnecessary blocks will be discarded.

B Region of Interest, after specifying the valuable direction in the previous step, here can use morph operation on image which is dilation followed by erosion to reduce the image by removing the small cavitations, this is done by using Close operation. And then apply erosion followed by dilation in order to show new image and cut off the peaks in background figure, this is done by using Open operation. So by subtracting the close area from the open area will get a bound area and inner area. See algorithm (3) and figure (8) for more details.

Algorithm (3) Fingerprint image segmentation
Input: binarized image Output: segmented fingerprint with its direction

process
For every pixel in binarized image do
Find the values of the edge in X and Y direction by using "Sobel masks". "$gx(x,y) = hx * f(x,y);\ gy(x,y) = hy * f(x,y)$"
Calculate the Gradient magnitude= $g = \sqrt{{g_x}^2 + {g_y}^2}$
Calculate the Gradient direction= $\theta = tan^{-1}\left(\frac{g_x}{g_y}\right)$
Calculate least square approximation for block direction
"$tg2\ \beta = 2\sum\sum(g_x * g_y)/\sum\sum(gx^2 - gy^2)$"
End for
Threshold=0.05
For each block with size W do
Find unnecessary block by applying the unnecessary blok formula. $E = \frac{\{2\sum\sum(gx*gy)+\sum\sum(gx2-gy2)\}}{W*W*\sum\sum(gx2+gy2)}$
If this block< threshold then discard it
Apply morph operation (dilation followed by erosion) to reduce the image (close area)

A apply erosion followed by dilation to cut off the peaks in background (open area) End for Subtract the close area from the open area to get bound and inner area Return bound area and inner area End process

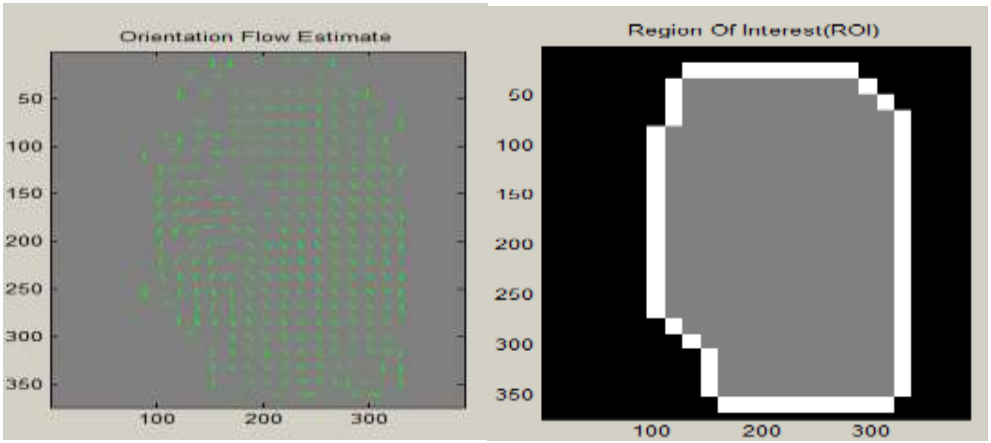

Figure (8) block direction and region of interest

Minutia Extraction

This step involve two main tasks: thinning and minutia specifying

I. Thinning

In fingerprint recognition system two types of minutia are used which is ridge ending and bifurcation. In this process all the ridge will be thinned to be one pixel wide. This is done by checking the eight neighborhoods of every pixel in binarized image and check if the pixel needs to be thinning or not. See algorithm (4) which explain the thinning process and figure (9) which shows all the ridge of one pixel wide.

Algorithm (4) Fingerprint Thinning
Input: binary image Output: thinning image

Process
Repeat
For every black pixel
If there is one white pixel below it then
begin
From bottom to above do
Check the 8-neighbor
If black pixel has also black one (in the same neighbor) then reverse it to white.
If all (8neighbors) are white then don't change this pixel and leave it black.
End
Else If there is one white pixel above it then
Begin From above to bottom do
Check the 8-neighbor
If black pixel has also black one (in the same neighbor) then reverse it to white.
If all (8neighbors) are white then don't change this pixel and leave it black.
End

Else If there is one white pixel on the left then
begin
From left to right do
Check the 8-neighbor
If black pixel has also black one (in the same neighbor) then reverse it to white.
If all (8neighbors) are white then don't change this pixel and leave it black.
End
Else If there is one white pixel on the right then
begin
From right to left do
Check the 8-neighbor
If black pixel has also black one (in the same neighbor) then reverse it to white.
If all (8neighbors) are white then don't change this pixel and leave it black.
End
End for
End process

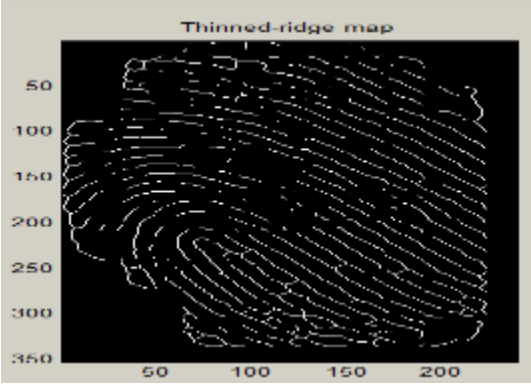

Figure (9) Ridge thinning

II. Minutia Specifying

In this process will be used (3*3) block in order to check each pixel in the thinned image. If the central pixel has value of "1" with three neighbors "1" pixel value then the pixel is representing as a bifurcation, while if the central pixel has value of "1" with a unique "1" value pixel as a neighbor then the pixel determined as a termination, but if the pixel has two black neighborhoods of eight pixel so the pixel doesn't contain any feature.Algorithm (5) will show how to determine types of minutia.

Algorithm (5) Determine type of minutia
Input: thinning image Output: minutia type

Process
Repeat
For each black pixel
If there is one black pixel from8-neighbor then mark this as "ridge ending".
If there is two black pixel from8- neighbors then mark this as "normal".
If there is three black pixel from8-neighbors then mark this as "ridge bifurcation".
End for
Until marking all pixels
End process

The result thinned image may contain some of unnecessary spikes and breaks and this should be removed because it may lead to recognition of false minutia. Algorithm (6) describes

a way to deal with this situation. Figures (10 and 11) will explain fingerprint image after removing breaks and spike and then marking all minutia in fingerprint image.

Algorithm (6) for removing spikes and breaks
Input: thinned image Output: thinned image after removing spikes and breaks

Process
For each pixel in thinned image do
If an angle with a branch and ridge>70^0 and <110^0 then
If length of the branch<20 pixels then remove this branch
If a break in ridge<15 pixels and no other ridge will pass through it then connect this break
End for
End process

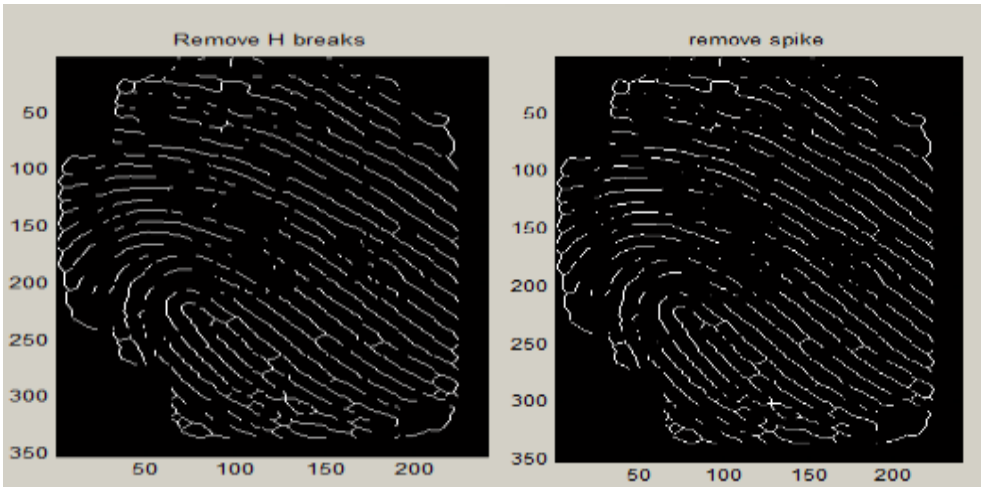

Figure (10) Removing the breaks and spike

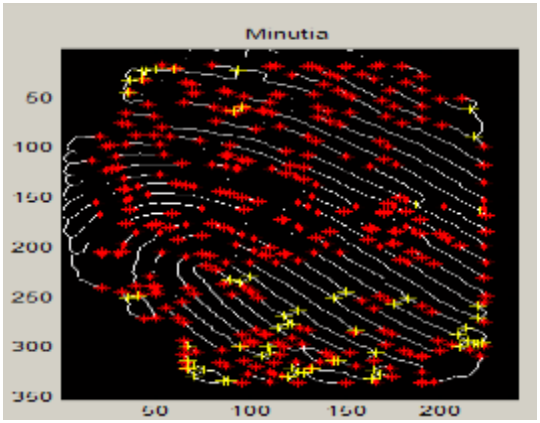

Figure (11) Extract all minutia in fingerprint

Minutia Post-Processing

The enhancement of image in the preprocessing stage may some ink spots as part of image and result as minutia, so these minutia's could be removed by calculating the average distance between any two neighborhoods minutia. This distance considered as a threshold value.For a given raw the sum of the value of its pixel will be calculated and then finding the average distance by dividing the sum by number of pixels for this raw.For a given two bifurcation and terminations, if the distance is less than the previous average distance (threshold) so both of

them will be removed.If distance of two bifurcations less than the average distance (threshold) then they will be removed.In short ridge if it contains two terminations but their distance is less than average distance (threshold), so remove both of them. Algorithm (7) will explain main steps to extract the real minutia, see figure (12) which explain the fingerprint image after removing false minutia.

Algorithm (7) Real minutia extraction
Input: thinned image Output: extract real minutia

Process
Calculate the average distance between any two neighborhoods minutia
Threshold=average distance
For each minutia in minutia list
Find distance between two minutia
If two minutia is bifurcation and termination and their distance < threshold then remove both of them
If two minutia is two bifurcation and termination and their distance < threshold then remove both of them
If two minutia is two bifurcation and their distance <threshold then remove both of them
Else
If two minutia is termination and their distance <threshold then remove both of them
End for
End process

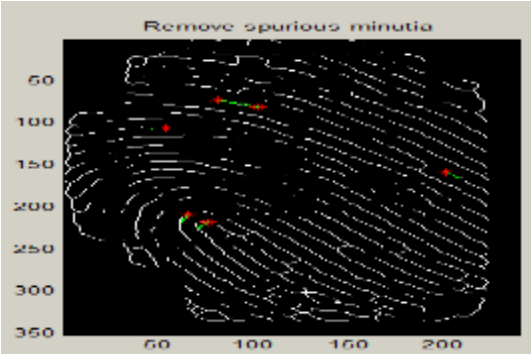

Figure (12) Extract Real Minutia

Fingerprint Matching

Fingerprint minutia matcher, see algorithm (8), based on ridge alignment which consist of choosing any two pairs of minutia as a reference pair and calculate matching score which must be greater than threshold and then do translate and rotate other related minutia depending on these pairs, and return the maximum similarity of two fingerprints.Template file save as N*3 array with the format shown in figure (13).

Minutia_1position_x minutia_1position_y minutia_1 orientation
…..
Minutia_nposition_x minutia_nposition_y minutia_n orientation
Ridge_1point1 pos. _x ridge_1 point1 pos._y ridge_ID(1)
…….
Ridge_1 point m pos._x ridge_1 point m pos._y ridge_ID(1)
Ridge_2 point 1 pos._x ride_2 point1 pos._y ridge_ID(2)
……
Ridge_n point 1 pox._x ridge_n point 1 pos._y ridge_ID(n)
……
Ridge_n point m pos._x ridge_n point m pos._y ridge_ID(n)
n refers to the total minutia number
m is the value of average inter-ridge width

Figure (13) The format of template file

Algorithm (8) Fingerprint matching

Input: template1, template2
Output: percent matching

Process
Threshold=0.8;
Percent-match=0;
num-match=0;
If template1 or template2 is empty then
Percent-match= -1; {there is no match}
Repeat
1- Choose any two pair from template1 and template2
2- Find the distance in each point in template1 ridge with its associated point in template2 ridge
3- Find the sum of the above distance
4- Calculate the matching score by applying matching score formula
$S = \sum_{i=0}^{m} x_i X_i \; (\sum_{i=0}^{m} x_i X_i)\text{^ } 0.5$ where x_i and X_i are template1 and template2
5- If value of matching score< threshold then go to step1
6- Do translate and rotate method for each match minutia in each template to check if there is a scale or not
7- If no scale occur the two template are identical
8- Else go to step 1
9- Num-match=num-match+1
Until no other pair
Percent-match=num-match*100/no. of minutia
End process

Experimental Works and Results

The results of fingerprint recognition in this proposal was acceptable results when compared with traditional fingerprint recognition system because of using Gabor filter in the preprocessing step after using image enhancement by histogram equalization. The dataset that used in this proposal collected from (30) different finger; (8) samples for each finger, the images were taken with varying position and orientation. So the total number of fingerprint images in the database is 240 (30*8). Some images of fingerprint with their samples are chosen from the dataset that is used in this work and are shown in figure (14).

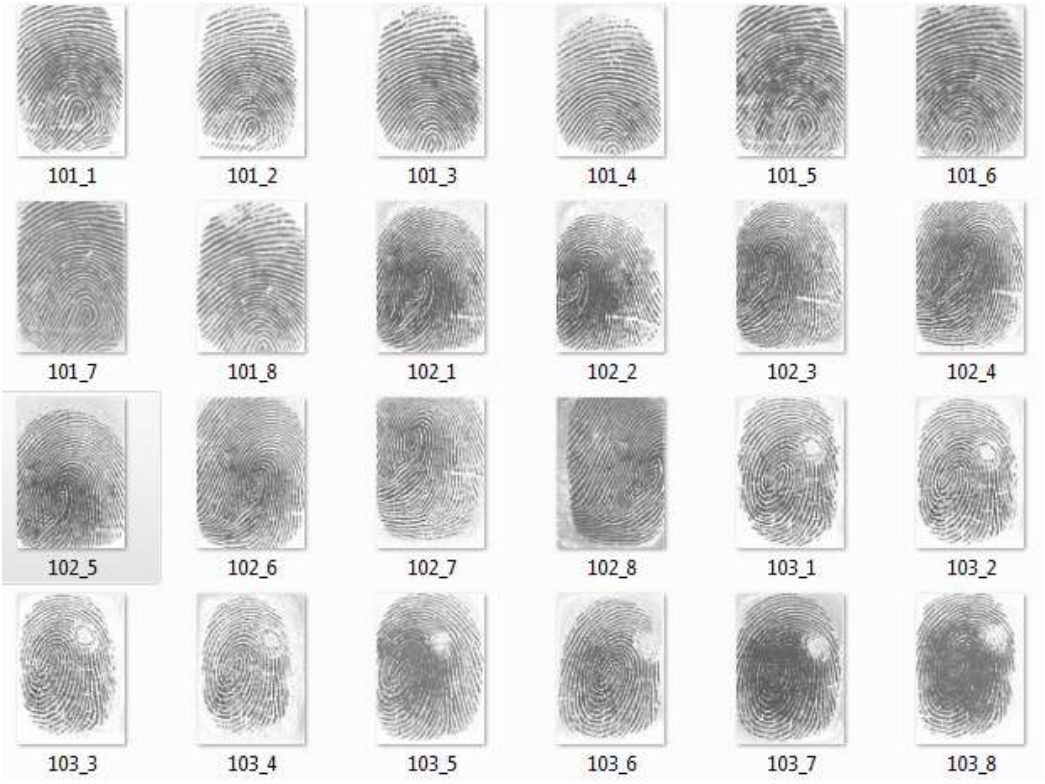

Figure (14) some fingerprint images with their samples chosen from data set

Because of each fingerprint have 8 different samples, ridge direction in Gabor enhancement is quantized into 8 directions: 0^0, 22.5^0, 45^0, 67.5^0, 90^0, 112.5^0, 135^0, and 157.5^0 to be able to recognize the rotated fingerprint impression that enquired in different impressions.

First of all enrollment process will be done for these entire in order to store template file for each fingerprint image. When applying FRR and FAR must be carefully choose the threshold of matching score which is deciding if reject or accept a match. When choosing less threshold value that means, probability of accepting image will be high and rejected image will be low. And according to this situation the chance of occurring error will be increased and vice versa. So our simulation results will explain in Table (1) as show below with threshold ratio 0.98 and 0.99.

Table (1): FAR and FRR with traditional and proposal

Recognition System	Traditional (FTT) only	Traditional (FFT+Gabor) enhancement [11]	Proposal (histogram + Gabor) enhancement
FAR threshold 0.98	0.94%	3.1%with acceptance threshold=10	0.61%
FRR threshold 0.98	0.40%	0.8% with acceptance threshold=10	0.25%
FAR threshold 0.99	0.91%	0.0% with acceptance threshold=20	0.31%
FRR threshold 0.99	0.45%	7.8% with acceptance threshold=20	0.30%

The result which is shown in table (1) are taken from the result of traditional fingerprint recognition which is used fast Fourier transform (FFT) in image enhancement that is required to apply histogram equalization before and after enhancement by (FFT) in order to remove some

noise that's accord after applying (FFT) and lead to false minutia and this is time consuming, so we implement two fingerprint recognition system one of them use (FFT) in image enhancement and the other used Gabor filter and the results of FAR and FRR was explained in table (1) and which means the FAR in traditional was 0.94% because the high number of different fingerprints and erroneously give match. The FRR in traditional was 0.40% because of high number of pairs for the same fingerprint and give no match, and On the other hand can see the acceptable result of the proposal that uses Gabor filter which is deal with orientation .
The main difference between the proposal and related work that use Gabor filter, the proposal is minutia based matching that use Gabor filter in enhancement step while some of other related work used bank of Gabor filter to filter the circular region around the core point, and others use combination of FFT and Gabor filter or Sobel filter with Gabor filter in the enhancement of images.

CONCLUSIONS

We have proposed an efficient algorithm for fingerprint recognition with two steps of image enhancement (by using histogram equalization and Gabor filter) which make our proposal able to recognize the rotated impression and makes the ridge smoothness and reduce the "hairy" structure in the ridge during thinning process because Gabor=Gaussian * Fourier, and this will give less effort in post processing stage when spurious minutia must be removed. The proposed algorithm shows that the accuracy of fingerprint matching is improved as shown in table (1) with two thresholds.

REFERENCES

[1] Oguniye G.B. andAfolabi O.M., "A Hybrid Authentication Mechanism For Preventing Phishing Attack On E-Banking System: The Nigeria Case Study", International Journal Of Emerging Technology And Advanced Engineering, Volume 4, Issue 12, December, 2014.
[2] Nanaware K., Kanade K., Bhat M., PatilR.andDeokar A.S., "Malicious Website Detection Using Visual Cryptography And OTP", International Journal Of Current Engineering And Technology, Volume 4, No. 5, 2014.
[3] Kirda E. andKruegel Ch., "Protecting Users Against Phishing Attacks", The Computer Journal, Volume 00, No.0, 2005.
[4] Yoon S., "Fingerprint Recognition: Models and Applications", PHD. , ThesisinComputer Science toMichiganState University, 2014.
[5] Prabhakar S., "Fingerprint Classification And Matching Using A Filter Bank", PHD. , ThesisInComputer Science &Engineering To Michigan State University, 2001.
[6] Hashem S. H., Maolod A. T. and Mohammad A. A., " Proposal To Enhance Fingerprint Recognition System ", International Journal Of Computer Engineering & Technology (IJCET), Vol. 4, Issue 3, May-June 2013.
[7] Zhang D.D., "Automated Biometrics Technology And System", Book, Springer Science + Business Media, LLC, May 2000 Newyork.
[8] Wieclaw L., "A Minutiae Based Matching Algorithms in Fingerprint Recognition System", Journal Of Medical Informatics & Technologies, Vol. 13, 2009.
[9] Chandana, Yadav S. and Mathuria M., " Fingerprint Recognition based on Minutiae Information",
International Journal of Computer Applications, Volume 120, No.10, June 2015
[10]Munir M. And Javed, M. "Fingerprint Matching Using Gabor Filters" National Conference On Emerging Technologies, 2004.
[11] Aguilar G., Sánchez G., Toscano K., Nakano M. M. and Pérez M. H., "Automatic Fingerprint Recognition System Using Fast Fourier Transform And Gabor Filters", Científica Vol. 12 No.1 Pp. 9-16 © 2008 ESIME-IPN. ISSN 1665-0654.

[12] Mudegaonkar P. M. AndAdgaonkar R. P.,"A Novel Approach To Fingerprint Identification Using Gabor Filter-Bank", ACEEE Int. J. On Network Security, Vol.,02, No. 03, July 2011.
[13]Muhammed R.P.,"A Secured Approach to Visual Cryptographic Biometric Template", ACEEEInt. J. On Network Security, Vol.02, No. 03, July 2011.
[14] Shara R.K., "Generation ofBiometrickeyFor Use In DES", International Journal Of Computer Science, Vol.9, Issue 6, No. 1, November2012.
[15] Gopi K. And Pramod J.T., "Fingerprint Recognition Using Gabor Filter And Frequency Domain Filtering", IOSR Journal Of Electronics And Communication Engineering (IOSRJECE) ISSN : 2278-2834 Volume 2, Issue 6 (Sep-Oct 2012), PP 17-21.
[16] Hongchang K., Wang H. and Kong D., "An Improved Gabor Filtering For Fingerprint Image Enhancement Technology", 2nd International Conference On Electronic & Mechanical Engineering And Information Technology (EMEIT-2012).
[17] Patel Y., Ms. Diana S.Ch., "Fingerprint Authentication Technique To Prevent Phishing Using Pattern Matrix", International Journal Of Engineering Research And Development, Vol. 6, Issue 8, Pp. 88-92, April 2013.
[18] Azzoubi E. A., and Ibrahim R.B., "An Enhancement Algorithm Using Gabor Filterfor Fingerprint Recognition", Journal of Theoretical and Applied Information Technology, Vol.74 No.3, 30th April 2015.
[19] Ali E. ,Ali H. A., Jaber H. "Fingerprint Recognition Using Gabor Filter With Neural Network", Eng. &Tech. Journal, Vol. 32 Part(A), No.2, 2014.
[20]Al-AlaghaS. A. " A Block Compression Method For Fingerprint Image Storing" , Eng. &Tech. Journal, Vol. 27, No. 11, 2009.