A Proposed Hybrid Fingerprint, Image Fusion and Visual Cryptography Technique for Anti-Phishing

Rajaa K. Hasoun
rajaamena@yahoo.com
University of Technology - Computer Science Department
Assist. Prof. Dr. Soukaena H. Hashem
soukaena.hassan@yahoo.com
University of Technology - Computer Science Department
Assist. Prof. Dr. Rehab F. Hasan
surorh@yahoo.com
University of Technology - Computer Science Department

Abstract: *This paper proposes an anti-phishing web site system it is carried out by the two following stages: Registration phase; the user enters username and password then (his/her) fingerprint, server site selects virtual fingerprint image. The fusion will be applied to fuse real fingerprint with virtual one, fused image will be input to visual cryptography(VC) scheme to produce two shares, one share kept with user in addition to fuse image, and other shares are kept with the server. Authentication phase; in this phase the user enters the password and is asked to enter the fingerprint. Pattern recognition is done to determine if it is hacker or authenticated user, when the server accepts the fingerprint the user will be required to input (his/her) share, so the user share is stacked with server share and generated image is displayed. The user will decide if it's a phishing site or not depending on the*

displayed image (after matching it with the image that the server shared through registration phase).

From many experimental works conducted on the proposal, we notice the strength is centered in image fusion. Where the fused fingerprint images have higher quality (entropy) than the single fingerprint image, that increases randomness of the VC shares which are extracted from the fused fingerprint.

Keywords: fingerprint, phishing attack, visual cryptography and image fusion.

1. Introduction

Phishing is a type of online identity stolen that aims to steal personal details from users like "online banking passwords" and "credit card" details. Phisher will deceive the user and make him give away personal details [1, 2]. To prevent phishing attacks consider the use of powerful authentication techniques for the payment processing systems. This includes replacing traditional key with PIN, or with biometrics like fingerprint. Phisher can't break powerful authentication like biometrics [3, 4].

Fingerprint verification systems may be the best authentication systems for many reasons. Researchers have a great knowledge about how to deal with it because it has been used for hundreds of years, It is the most developed method till now, relatively inexpensive, fingerprints have unique patterns even with twin, and matching is fast because of small template size [5].

VC is a recently developed mechanism used for security of images. In this scheme the Image is separated into many pieces "shares" in order to be distributed among participants, decryption of VC only overlaps the share images in order to have original image. The first model was only used for the binary images and then developed for Color Images [6, 7].VC is cryptographic mechanism used for encryption visual information because the decryption

process is done by human visual system [8, 9]. Let's now see how visual cryptography algorithm works; each pixel P in the secret image is split into two sub pixels in each of two shares as shown in figure (1) [10].

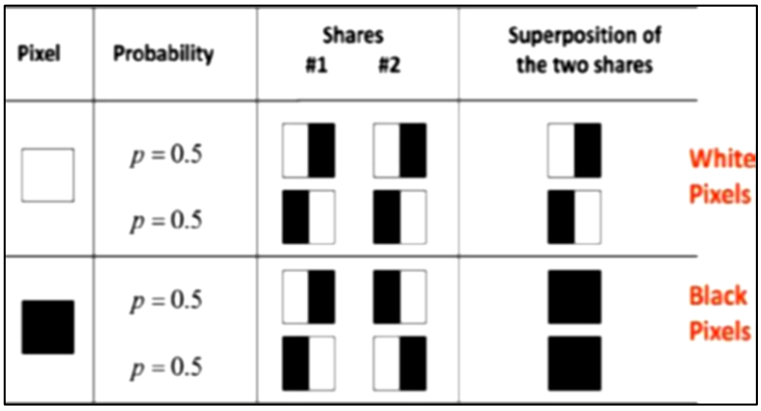

Figure (1) Extractions (2, 2) VC Scheme

- If P is "white" then randomly choose any one from first two rows in figure (1) i.e. if the choice is first row then the two sub pixels in both two shares are ("white", "black"). If the choice is second row then both of them will be ("black", "white"). In this case when P is white we have one "black" sub pixel and one "white" sub pixel when overlapping the two shares.
- If P is " black" then choose randomly any one from second two row in figure (1), this means if the choice is first row then the two sub pixels in first share will be ("white", "black") and second share will be ("black", "white") . while if the choice is second row then two sub pixels in first share will be ("black", "white") and second share will be ("white", "black"), so when overlapping the two shares we can get two "black" sub pixels.

Image Fusion is a method of combinations the pertinent information from multiple images to produce one image, the result image will have more informative than all input images. Important applications of the image fusion are medical imaging, remote sensing, and robotics [11, 12].The image fusion process can done

by using wavelet transform, the general process is as follows [13], Create wavelet lower decomposition by implementing discrete wavelet transform on both input images. Apply fusion rules to fuse each decomposition level. Apply Inverse Discrete Wavelet Transform to fused decomposed level in order to reconstruct the fused image. The quality of fused image can be assessed by using quality metrics which are; Peak Signal to Noise Ratio (PSNR) which is the ratio between the maximum power of a signal and the power of corrupting noise that creates distortion of image. The Entropy (EN) is used to evaluate the information quantity in an image. High value after fusing indicates that the information increases and this will improve performances. Mean Squared Error (MSE), is a measure of image quality index. The high value of MSE indicates poor quality of image [13, 14].

2. Related Works

- In 2014, Nanaware et al.; suggested new method for anti-phishing by authentication system using visual cryptography which is implemented with the combination of one time password, which is password used only for one session to avoid the problem of static password and it is not vulnerable to replay attacks, that means potential intruder who wants to send the user a message via e-mail. Merchant server sent share1 to user for verification process. User stacked share1 with share2 to get the image in order to get OTP from this image and use it to validate with the bank server through the merchant server [15].
- In 2014, Jose et al.; suggested a new method for anti-phishing by using authentication system using image based visual cryptography and to improve the security they use "Blowfish algorithm" to split original image captcha into many blocks and rearrange them, also they use split and rotate algorithm to rotate the rearranged blocks. This proposal provides three levels of security, first level verifies if website is secure or not, second level image captcha can be read only by human user and not by machine user, the third level prevents attacks on the account of the user by intruders [16].

- In 2014, Soradge et al.; solved the problem of phishing by using VC scheme to produce the privacy of an image of user choice and breaking down this image into two shares that are kept in different database servers where original image can be revealed when both shares are accessible. In order to increase the security on server site the share in this side is further decomposed into multiple shares and stored in different servers. The proposal preserves sensitive information of user in two stages of security, first stage can determine if a website is a genuine or phishing website because phishing website can't show the original image. Second stage by using image captcha (which is text inside image only humans can read but machine user can't read), where only humans who access the site can read the captcha [8].
- In 2015, Patil et al.; proposed in their work wavelet transform based fusion algorithm and they studied principles and characteristics of discrete wavelet transform, the result of experiment explains that wavelet transform is a good method for image fusion. Also they used MAX, MIN and MEAN methods for fusion purpose. Also they used information entropy in order to evaluate the fusion quality, which means how much average information of fusion image [17].
- In 2015 Hamsalekha et al.; made a review of different image fusion techniques like average method, select Min, select Max, discrete wavelet transform and PCA. Also they gave the performance measure like mean square error, entropy, normalized cross correlation. And they made comparison of all these techniques, and explained the spatial domain provides high resolution, but it has main drawback which is spectral distortion, therefore transform domain is done [14].

3. General Description of the Proposal

The proposed system consists of two main phases: Registration phase and Identification phase (login phase), as shown in figures (2) and (3). In registration phase the user will enter the key and fingerprint image, pattern recognition process will be done

to generate user template and store it in server database. On server site, the server will select unique virtual fingerprint for that user. These two fingerprint images are fused together by using image fusion technique to produce one fused fingerprint image. A copy of this fused image will be sent to the user to be used during login phase. The next step uses (2, 2) visual cryptography scheme to generate two shares, one of them will be kept in user database and the other will be stored in server database. This process will protect biometric data that are stored in centralized database because they are vulnerable to eavesdropping and attacks.

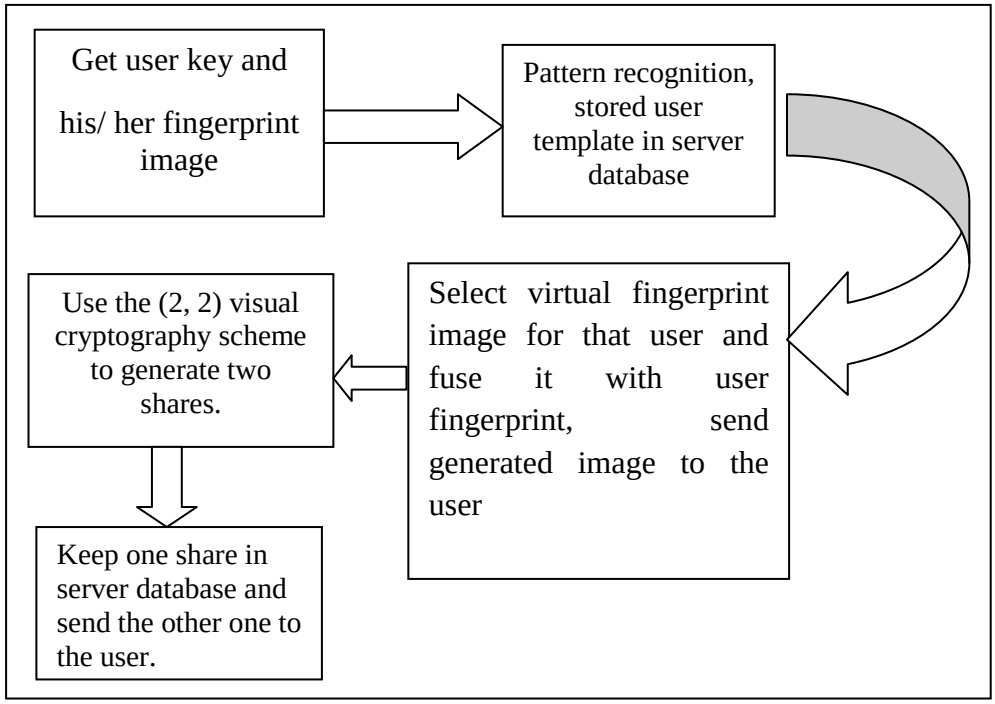

Figure (2) Block diagram of registration phase

The user can log in by entering his key in order to use his account. Then he will be asked to enter his fingerprint, pattern recognition process will be done in order to compare the generated 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 must enter the share

with him. So the users share and server share are stacked together in order to get fused image. This image will be shown to the user, so he can determine if displayed image matches the image that was created during registration time. If it doesn't match, the user will know that this is a phishing website. While if there is a match the user must enter the text displayed in the image captcha, the user can log in into the website. This process can prove if the website is genuine or a phishing website and can also prove if the user is a human user or machine user.

Let's explain if a hacker user can access in any way the stored share, when stacking these two shares he will get the fused image which is still fingerprint image but he doesn't know it is fused image. So when he tries to login to the system he will enter this image, the server will do pattern recognition process on these image and compare it with the stored template in database and no match will occur and a hacker user cannot login to the system.

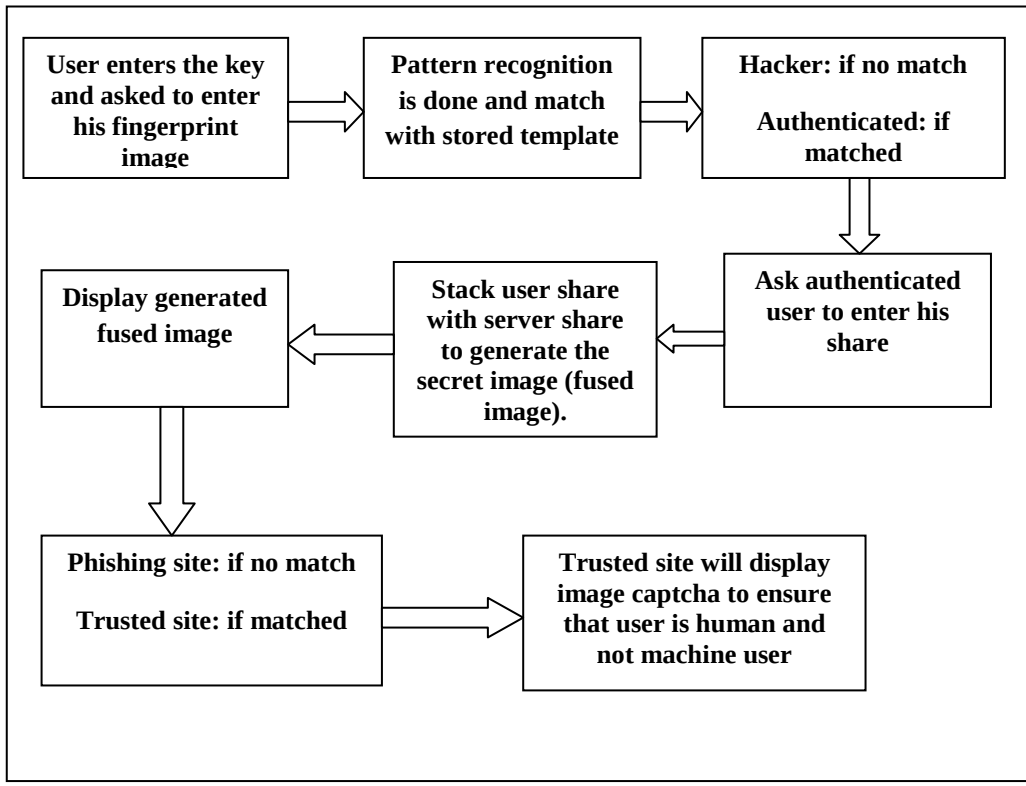

Figure (3) Block diagram of login phase/ authentication

On the other hand trusted user will not be a victim to any phishing website because server share is stored in trusted website database and when stacking with trusted user share will produce fused image, the user can match it with stored image in its database and know it is genuine website and not phishing website, this is anti-phishing process.

This proposal uses two data sets, each of them contains 100 fingerprint images and both of them have the same name for their images, the first data set contains users' fingerprint and the other one contains virtual fingerprint images. When the fingerprint of the user has the name "101.bmp", the serve will search in data set2 for fingerprint image with the same name and retrieve it, both of these two fingerprint images (real and virtual) will pass to image fusion routine to produce the fused image.

3.1 Standard Fingerprint Recognition

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

1. Preprocessing

- Image Enhancement, This step uses combination in spatial domain and frequency domain in order to use the complete advantages of each domain. So in this step histogram equalization is used in spatial domain and Gabor filter in frequency domain. In this paper Gabor filter is used because the "Gabor filter" is (Gaussian * Fourier).
- Image Binarization, In this step threshold must be chosen. And the value of image over the threshold value becomes 1 (black) and value less than threshold value will be 0(white). By experience threshold value is equal to 0.8.
- Image Segmentation, (A) Block direction, the horizontal and vertical values (gx, gy) must be computed for all pixels in the enhanced image by applying Sobel mask to both directions (vertical and horizontal). Gradient magnitude and

gradient direction are computed. When applying this process to each block, the unnecessary blocks will be discarded.(B) Region of interest, In this step dilation is applied followed by erosion to reduce the image, this is done by using Close operation. And then erosion is applied followed by dilation; 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.

2. Minutia Extraction

- Thinning, In this process all the ridges will be thinned to be one pixel wide. This is done by checking the eight neighborhoods of every pixel in binarized image and checking if the pixel needs to be thinned or not.
- Minutia Specifying, this process will use (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 represented as a bifurcation, while if the central pixel has value of "1" with a unique "1" value pixel as a neighbor then the pixel is determined as a termination. The resulting thinned image may contain some of unnecessary spikes and breaks and these should be removed because they may lead to recognition of false minutia.

3. Minutia Post-Processing

- False minutia could be removed by calculating the average distance between any two neighborhoods minutia. This distance is considered as a threshold value. For a given raw the sum of the value of its pixel will be calculated and then the average distance is found by dividing the sum by the number of pixels for this raw. For a given two bifurcation and termination or two terminations or two bifurcations, if

the distance is less than the previous average distance (threshold) both of them will be removed.

- Fingerprint Matching, Fingerprint minutia matcher is based on ridge alignment which consists of choosing any two pairs of minutia as a reference pair and calculating 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.

3.2 Image Fusion

Image fusion is a method for combining two or more images in order to produce single image. In our proposal, image fusion is used for fusing real fingerprint image that entered by the user with the virtual fingerprint image that is selected from server site in order to provide more security for the stored user fingerprint image because the stored biometrics in database are vulnerable to eavesdropping and attack. The proposal uses "discrete wavelet transform (DWT)" which converts the input image from spatial domain to frequency domain and divides image by vertical and horizontal lines in order to separate four parts that is "LL1, LH1, HL1, and HH1". Algorithm (1) explains main steps of image fusion process.

Algorithm (1) Image fusion process
Input: images to be fused Output: fused image
Process Input the two fingerprint images (mask, bust) Apply wavelet decomposition by discrete wavelet transform to both input images Choose fusion rule and apply it to fuse each decomposition level Apply "inverse discrete wavelet transform" to get the fused image End process

First we explain step1 which is discrete wavelet transform (DWT). The first DWT was Haar wavelet where the input should be a multiple of 2n, where n is the number of levels.

The Haar transform takes pairs of data items from the signal and performs two steps of calculation which are [18]:

$$L_i = \frac{X_{2i} + X_{2i+1}}{2} \quad \dots\dots\dots\dots\dots (1)$$

$$H_i = \frac{X_{2i} - X_{2i+1}}{2} \dots\dots\dots\dots\dots\dots (2)$$

Where Li: low sub band and Hi: high sub band.
The formula of inverse Haar transform is:

$$X_{2i} = \frac{L_i + H_i}{2} \dots\dots\dots\dots\dots\dots\dots (3)$$

$$X_{2i+1} = \frac{L_i - H_i}{2} \dots\dots\dots\dots\dots\dots\dots (4)$$

The DWT of input signal X is calculated by passing it through sequence of filters, the sample will pass through "low pass filter" (g) and then decompose using a "high pass filter" (h), see the following equations:

$$Y_{low} = (X * g) \downarrow 2 \dots\dots\dots\dots\dots (5)$$

$$Y_{high}(X * h) \downarrow 2 \dots\dots\dots\dots\dots\dots (6)$$

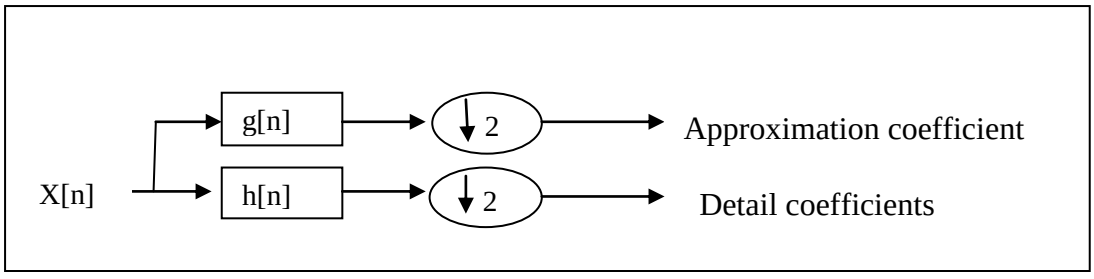

Figure (4) Block diagram of filter analysis

The filter output is then sub sampled by 2 as shown in figure (4) [18]. The process of Haar DWT is explained in algorithm (2).

Algorithm (2) Haar DWT
Input: input fingerprint image with size (n*n) Output: decomposed image

Process
For i=0 to n/2 do
For j=0 to n/2 do
Output image [i, j]=input image[i, j*2]+input image[i, j*2+1] /2
Next j
Next i
For i=n/2 to n do
For j=n/2 to n do
Output image [i, j]=input image[i, j*2] – input image[i, j*2+1] /2
Next j
Next i
End process

After applying decomposition to the two images by using DWT, second step will apply fusion rule like (MAX, MIN, MEAN), which uses the "minimum, maximum and mean" values for the transform coefficients.

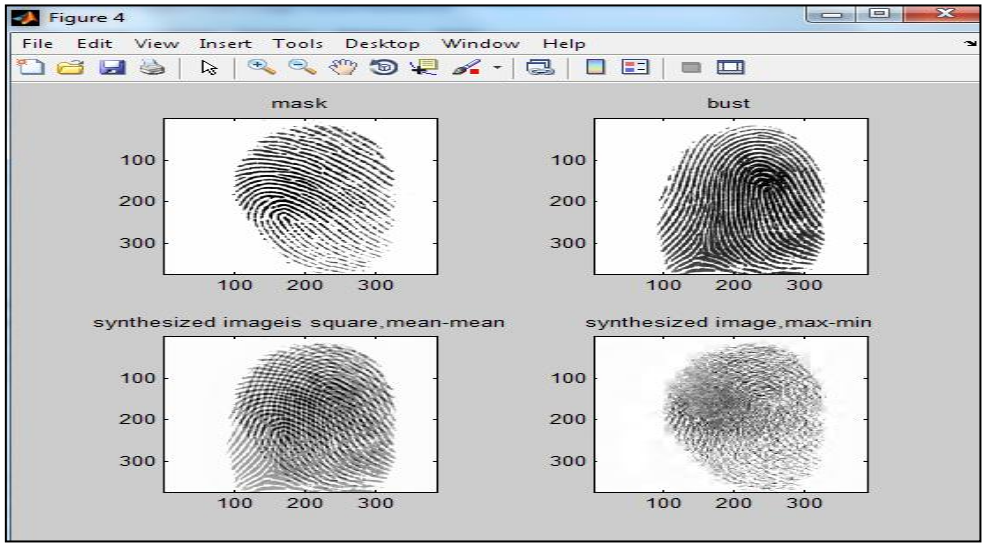

Figure (5) Image fusion

Third step of image fusion will apply "inverse wavelet transform" in order to reconstruct the fused image. Figure (5) explains how to fuse two fingerprint images from wavelet decomposition at "level 5" and "db2" by applying two methods of fusion, first by applying the mean for both approximations and details; second by applying the maximum for approximations and the minimum for the details.

3.3 Visual Cryptography

Protecting the template file that's stored in database is considered as a challenging task in biometric system because it is weak to eavesdropping and attack, so other protection mechanisms need more security; many researches are done to protect the biometric data like stenography and watermarking. In this proposal the VC technique is suggested to protect biometric template (fingerprint) in order to provide more security from attack, and also as an extra layer of authentication for the users.

In the proposal after applying image fusion technique to the real fingerprint image from the user and virtual fingerprint image from the server, the resulting fused image will pass to (2,2) visual cryptography scheme to generate two shares, one of them will be saved in the user database and the other will be saved in server database. Any one of these two shares can't give any details about the fused image, only when two shares are overlapped together can you get the original image. And this is a type of secret sharing. Algorithm (3) explains how to generate two shares from the binary fused image.

The following example will explain how to decompose the fingerprint image into two shares and how to overlap these two shares. Figure(6) shows the secret image, This secret image will be input to the (2, 2) visual cryptography to produce two shares as shown in figure (7) which shows share1 and figure (8) which shows share2. Figure (9) explains how can get the secret image when stacking the two shares.

Algorithm (3) "(2, 2) visual cryptography scheme"
Input: binary fused image Output: two shares

Process
For each pixel (P) in binary image do
If P is "white" then set two sub pixel in both share as ("white", "black") or
("black", "white")
Else
If P is "black" then choose one of the following options:
Option 1: set two sub pixels in first share as ("white", "black") and second as ("black", "white").
Option 2: set two sub pixels in first share as ("black", "white") and second share as ("white, black").
End for
End process

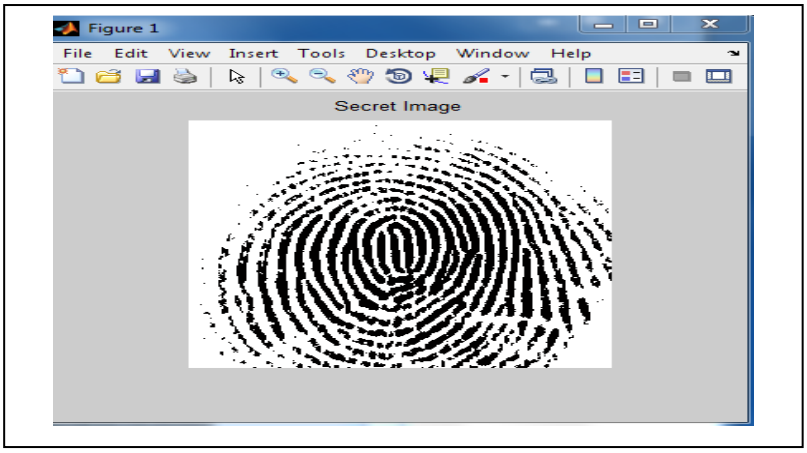

Figure (6) The secret image

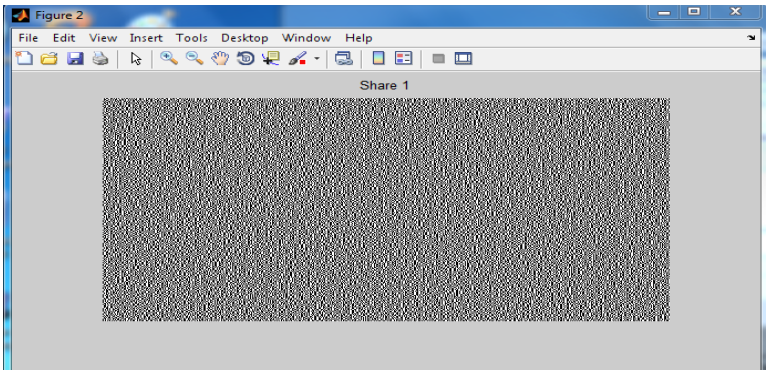

Figure (7) Share1 of secret image

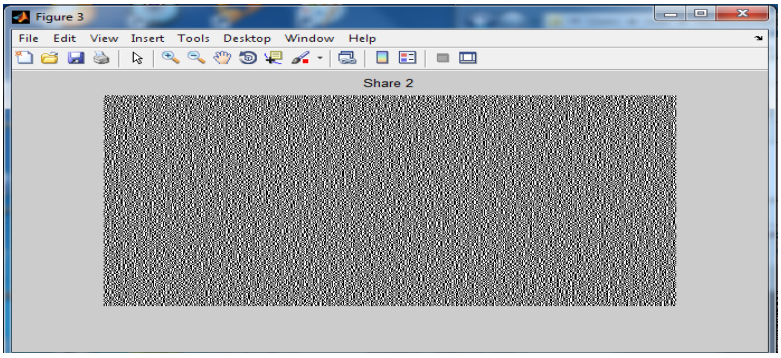

Figure (8) Share2 of secret image

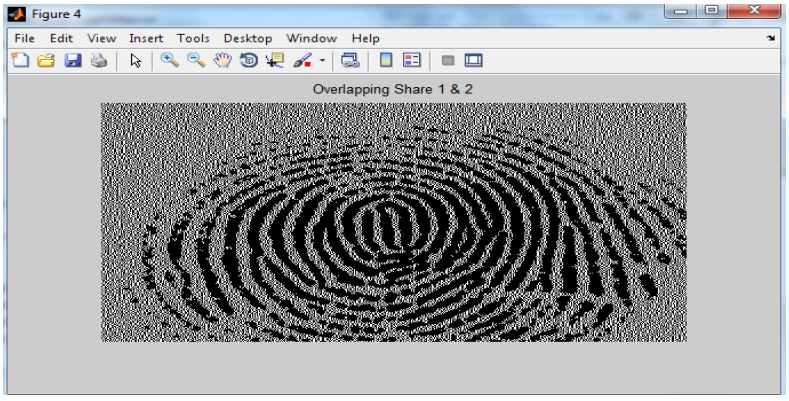

Figure (9) Overlapping share1 and share2

4. Experimental Works

This proposal depends on data set of (100) fingerprint images in order to evaluate the proposed system. Enrollment process will be done for all these entries in order to store template file for each fingerprint image. From the fusion experiment on fingerprint image the result are reached which are shown in table (1). The table can explain the result values are so close to each other although different wavelet functions are used. In this work there is no wavelet basis, which is better than other ones. But it can be proved that the entropy which is a measure of the information quality contained in an image, where two fingerprint images are taken and the entropy is calculated for each image, and then the entropy is calculated for the fused image, and the result is explained in table (2).

Table (2) explains high value of entropy after fusing images which indicates that the information increases and this will improve performance.

Table (1) Measures of fused images

Wavelet function	Level	Operator	Entropy	PSNR	MSE
db2	5	Max-min	8.5469	13.8203	40.1503
db2	5	Mean	8.4939	14.9207	17.1198
Haar	4	Max-min	8.1137	13.8071	60.5253
Haar	4	Mean	8.2113	14.9207	17.1198
db1	5	Mean	8.2025	14.9207	17.1198
db1	5	Max-min	8.123	13.7464	59.2099
Sym2	5	Mean	8.5469	14.9206	17.1180
Sym2	5	Max-min	8.4239	13.8203	30.4150

Table (2) Entropy for individual and fused images

Fingerprint image 1	Entropy = 5.0933
Fingerprint image 2	Entropy = 6.8015
Fused image	Entropy = 8.5469

When the program has been run the time of the used techniques in this proposal was as follows:-

Table (3) Time of execute the used techniques

Process	Tim in second
Fingerprint template extraction	5
Fingerprint template extraction + image fusion	7
Fingerprint template extraction + image fusion +VC	9

5. Conclusions

The proposal provides authentication system for anti-phishing system which consists of many layers of security in order to authenticate both sides (user and website) to each other. The techniques that are used in this proposal give it high level of security because the server can trust the user when he enters his fingerprint and the share that's stored with him, also by using "image captcha" that's displayed by the server which can be read only by "human user" and not read by "machine user". On the other hands the user can trust the server and know its trusted site and not phishing site when the stacking share and the display image will matches with the stored fused image that stored with him.

References

[1] Dhmij R., Tyger J.D., Hearst, "Why Phishing Works", Proceeding Of CHI-2006: Conference on Human Factors in Computer Systems, ACM 1-59593-178, April2006.

[2] Chhikara J., Dahiya R., Garg N., Rani M., "Phishing & Anti Phishing Techniques: Case Study", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 5, May 2013.

[3] William F.P., "Protect Yourself from Email Phishing Attacks", Multi-State Information Sharing And Analysis Center, Vol. 8, Issue 4, April 2013.

[4] Chuan Y., Haining W., "Bogus Biter: A Transparent Protection against Phishing Attacks", ACM Transaction on Internet Technology, Vol.10, No. 2, Article 6, May 2010.

[5] Kaur G., VermaCh. K., "Comparative Analysis of Biometric Modalities", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.4, Issue 4, April 2014.

[6] Archna B. D.,Nitin J. J., "An Implementation of Algorithm in Visual Cryptography in Images", International Journal of Scientific Research Publications, Vol. 3, Issue 3, March 2013.

[7] Revenkar P.S., Anisa A., Gandhare W.Z., "Secure Iris Authentication Using Visual Cryptography", International Journal Of Computer Science And Information Security, Vol. 7, No. 3, 2010.

[8] Soradge N., Thakre K.S., "A Novel Anti Phishing Framework on Cloud Based On Visual Cryptography", Proceedings of 12th IRF International Conference, 29th June, 2014.

[9] Gaurav P., Shekhar J., Ashutosh M., Vishal D., Baj.S, "An Enhanced Anti-Phishing Framework Based On Visual Cryptography", International Journal Of Emerging Research In Management &Technology, Vol.3, Issue 3, March 2014.

[10] James D., Philip M., "A Novel Anti Phishing Framework Based On Visual Cryptography", International Journal of Distributed and Parallel System, Vol.3, No. 1, January 2012.

[11] Sahu D., K. Parsai M.P., "Different Image Fusion Techniques-A Critical Review", International Journal Of Modern Engineering Research, Vol. 2, Issue.5, Sep.-Oct., Pp-4298-4301, 2012.

[12] Umaamaheshvari A., Thanushkodi K., "Image Fusion Techniques", IJRRAS 4 (1), July 2010.

[13] Rani K., Reecha S., "Study on Different Image Fusion Algorithm", International Journal Of Emerging Technology And Advanced Engineering, Vol. 3, Issue 5, May 2013.

[14] Hamsalekha R.,Rehna V.J., "Analysis Of Fusion Techniques With Application To Biomedical Image: A Review", International Journal Of Emerging Engineering

Research And Technology, Vol. 3, Issue 1, PP70-78, January2015.

[15] Nanaware K., Kanade K., Bhat M., Patil R. And Deokar A.S., "Malicious Website Detection Using Visual Cryptography and OTP", International Journal of Current Engineering and Technology, Volume 4, No. 5, 2014.

[16] Jose A., Lakshmi V., "Web Security Using Visual Cryptography Against Phishing", Middle-East Journal Of Scientific Research 20 (12):2626-2632, 2014.

[17] Patil A., Tibdewal M.N., "Wavelet Transform Based Medical Image Fusion with Different Fusion Methods", Journal of Engineering Research and Application, Vol. 5, Issue 3, Part-3, Pp. 10-14, March 2015.

[18] Gupta D. , Choubey S., "Discrete Wavelet Transform for Image Processing", International Journal of Emerging Technology and Advanced Engineering, ISO 9001:2008 Certified Journal, Volume 4, Issue 3, March 2015.

مقترح هجين من بصمة الاصبع وتقنيات دمج الصور والتشفير المرئي لمكافحة التصيد

م.م.رجاء كاظم حسون
rajaamena@yahoo.com
الجامعة التكنولوجية - قسم علوم الحاسوب - بغداد العراق
أ.م.د.سكينة حسن هاشم
soukaena.hassam@yahoo.com
الجامعة التكنولوجية - قسم علوم الحاسوب - بغداد العراق
أ.م.د.رحاب فليح حسن
surorh@yahoo.com
الجامعة التكنولوجية - قسم علوم الحاسوب - بغداد العراق

المستخلص:

هذا البحث يقترح نظام مكافحة صفحات التصيد بواسطة الخطوات التالية: طور التسجيل حيث يقوم المستفيد بادخال اسم المستخدم وكلمة السر وبصمة الاصبع اما في جهة الخادم سوف يختار صورة لبصمة اصبع افتراضية، يتم تطبيق دمج الصور وذلك لدمج بصمة الاصبع الحقيقية مع البصمة الافتراضية. الصورة المدمجة سوف تكون ادخال الى تقنية التشفير المرئي لتكون جزئين احدهما يحفظ مع المستفيد بالإضافة الى الصورة المدمجة. والجزء الثاني يحفظ عند الخادم. الخطوة الثانية هي طور التخويل حيث يقوم المستفيد بادخال كلمة السر ثم يطلب منه ادخال بصمة الاصبع حيث يتم تشغيل تمييز الانماط لتحديد فيما اذا كان مهاجم او مستخدم مخول، عندما يقبل الخادم بصمة الاصبع يتم طلب الجزء المخزون لدى المستفيد حيث يتم دمج جزء المستفيد مع جزء الخادم لعرض الصورة الناتجة. المستفيد سوف يحدد فيما اذا كانت صفحة تصيد ام لا اعتمادا على الصورة المعروضة (بعد مطابقتها مع الصورة الذي تشارك بها مع الخادم خلال طور التسجيل).

عدة اعمال تجريبية اجريت على النظام المقترح ولاحظنا القوة كانت متمركزة في دمج الصور. حيث ان صورة بصمة الاصبع الناتجة من الدمج تمتلك جودة عالية اكثر

من صورة بصمة الاصبع المفردة، وهذا يزيد من عشوائية اجزاء التشفير المرئي والمشتقة من بصمة الاصبع المدمجة.

الكلمات الرئيسية: بصمة الاصبع، هجوم التصيد، التشفير المرئي، دمج الصور.