Image Fusion-based Fingerprint Authentication System

التخويل باستخدام بصمة الابهام المعتمد على تقنية دمج الصور

Rajaa K. Hasoun Soukaena H. Hashem Rehab F. Hasan
Computer Science Department, University of Technology, Baghdad/Iraq

Abstract

This paper proposes deception to secure storing fingerprint in server site, that by image fusion system; it is carried out by fusing the fingerprint image that's entering from the user with the virtual fingerprint image that's selected from server site. So the user template will be stored in server database, while the fused image will be stored in server database and user database in order to be used by the user to compare the stored fused image with the displayed image from the server site to ensure this site is trusted and not phishing site.

The contribution of this proposal is using image fusion technique to cheat the attacker in database of server. The results obtained from the proposal are; detecting best fusion technique which gives clearer image and best entropy.

Keywords: image fusion, DWT.

المستخلص

هذا البحث يقترح نظام خداع يتضمن دمج للصور عن طريق دمج صورة بصمة الاصبع المدخلة من المستفيد مع البصمة الافتراضية التي يتم اختيارها من الخادم. بحيث ان القالب التابع للمستفيد يتم خزنه في قاعدة بيانات الخادم اما الصورة المدمجة يتم خزنها في كل من قاعدة بيانات المستفيد والخادم من اجل ان يتم استخدامها من قبل المستفيد وذلك عن طريق مقارنة الصورة المخزونة لديه مع تلك التي تعرض من قبل الخادم لكي يتأكد بان تلك الجهة هي موثوقة وليست جهة تصيد. القوة في هذا البحث تتركز في استخدام تقنية دمج الصور لذلك سيتم بيان قياس كمية المعلومات التي تحتويها الصورة وكذلك توضيح افضل تقنية والتي تعطي صور اكثر وضوحا.

الكلمات المفتاحية: دمج الصور، تحويل الموجات

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].In this paper will use image fusion to fuse real fingerprint from the user with the virtual fingerprint that selected from the server to produce the fused image in order to be used as a form of secret sharing between the authenticated user and the trusted site. Image fusion is a method of combination the pertinent information from multiple images to produce one image, the result image will has more informative than all input images. Image fusion applications are robotics , medical imaging, and remote sensing [5, 6].

2. Related Works

The following related work will present fusion techniques as much as related to the proposal:

- In 2010, Zhenget al.; In this work they compared 2916 kind of wavelet based function method and use similarity measure as evaluation criteria and they summarized the best wavelet, best wavelet decomposing level and the best fusion operator. Where they analyses and compares 54 wavelet bases, six kinds of decomposition level and 9 kind of fusion operator [7].
- 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 [8].

- 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 [9].

3. Image Fusion Techniques

Techniques of image fusion can enhance image without harming it.There are two types for the ways of enhancement"spatial domain and frequency domain".The first method immediately deals with pixels of input images.These method like "simple maximum,simple minimum, averaging, principal component analysis (PCA)" consider as spatial domain approaches. While in the second method , image must be transferred to frequency domain. As example for these method the DWT [10].

3.1 Simple Maximum Method

The resultant fused image of this image fusion method is resulted by choosing from input image the maximum intensity of pixels [11, 12].

$$E(i,j) = \sum_{i=0}^{M} \sum_{j=0}^{N} max \;\; C(i,j)D(i,j) \;\ldots\ldots\ldots\ldots\ldots\ldots \; (1)$$

$$Where, C\;(i,j), D\;(i,j) \; are \; input \; images \; and \; E\;(i,j) \; is \; fused \; image.$$

3.2 Simple Minimum Method

This method work by selecting the minimum intensity of pixels from both the input images [10, 13].

$$E(i,j) = \sum_{i=0}^{M} \sum_{j=0}^{N} min \;\; C(i,j)D(i,j) \;\ldots\ldots\ldots\ldots\ldots\ldots \; (2)$$

$$Where, C\;(i,j), D(i,j) \; are \; input \; images \; and \; E(i,j) \; is \; fused \; image.$$

3.3 Simple Average Method

The resultant fused image is calculated by taking the average intensity of corresponding pixels from both the input images [10, 12].

$$E(i,j) = {}^{(C(i,j) + D(i,j))}/_{2} \;\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$Where, C(i,j), D(i,j) \; are \; input \; images \; and \; the \; fused \; image \; is \; E(i,j)$$

3.4 Discrete Wavelet Transform Method (DWT)

(WT) are tools of multi-resolution image decomposition, DWT transform the image from the "spatial domain" to "frequency domain". The image is splited by horizontal and vertical lines to represents the1st order of DWT, and the image can be separated with four parts those are "LL1, LH1, HL1 and HH1" [7, 13]. As shown in figure (1).

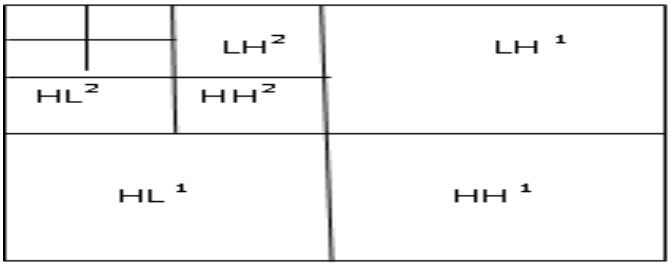

Figure (1) Wavelet decomposition

The image fusion process which is based on wavelet transform is shown in figure (2), which explain example of two images A and B are the original images needed to be processed; F is the result of fused image. The general process is as follows [12];

1. Create wavelet lower decomposition by implementing discrete wavelet transform on both input image.
2. Apply fusion rules to fuse each decomposition level.
3. compute "Inverse Discrete Wavelet Transform" to rebuild the fused image F.

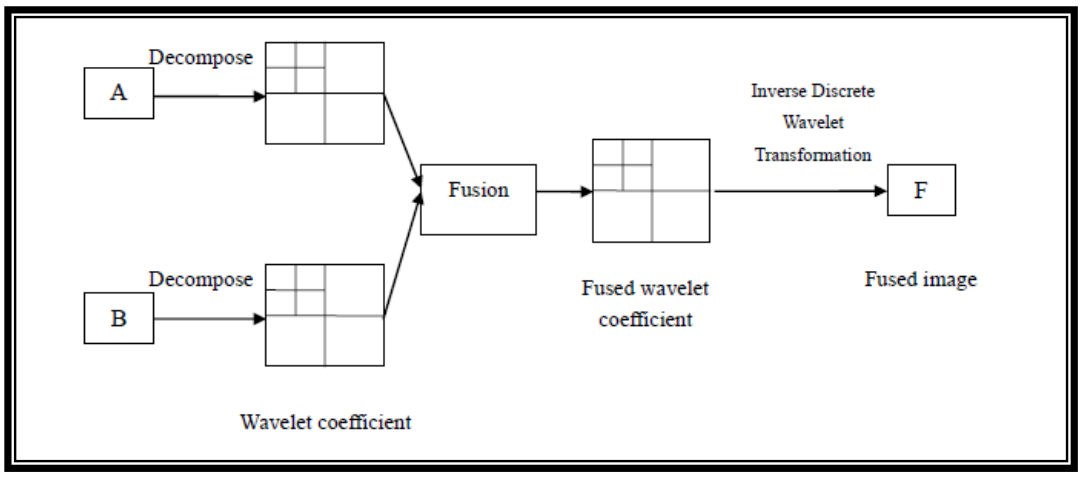

Figure (2) Wavelet based image fusion.

The first DWT was Haar wavelet where the input must be a multiple of 2^n, where n is the number of level [14]. The Haar transform take pairs of data items from the signal and perform two steps of calculation which is:

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

$$H_i=\frac{X_{2i}-X_{2i+1}}{2} \dots\dots\dots\dots\dots\dots (5)$$

Where L_i: low sub band and H_i: high sub band

The formula of inverse Haar transform is:

$$X_{2i}=\frac{L_i+H_i}{2} \quad \dots\dots\dots\dots\dots\dots\dots (6)$$

$$X_{2i+1}=\frac{L_i-H_i}{2} \dots\dots\dots\dots\dots\dots\dots (7)$$

The DWT of input signal X is calculating by passing it through series of filter, first the sample will pass through "low pass filter" (g) and then decomposed using a "high pass filter" (h) see equations (8) and (9). The filter output are then sub sampled by 2 as show in figure (3) [14].

$$Y_{low} = (X * g) \downarrow 2 \ \ldots\ldots\ldots\ldots\ldots (8)$$
$$Y_{high} = (X * h) \downarrow 2 \ldots\ldots\ldots\ldots\ldots\ldots (9)$$

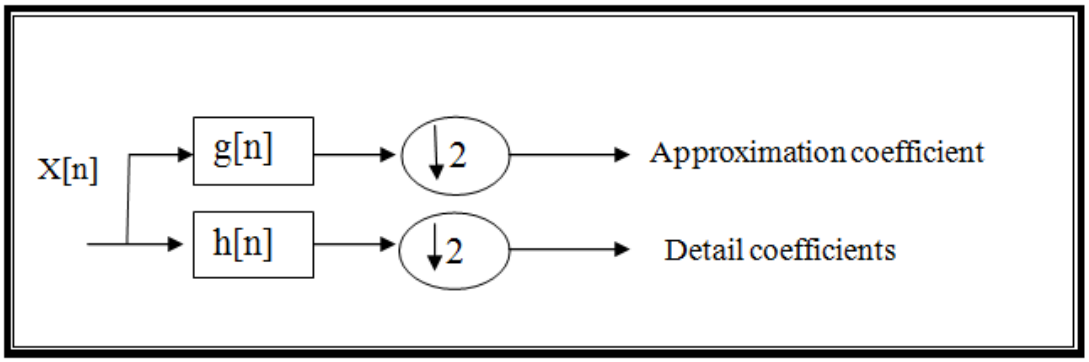

Figure (3) Block diagram of filter analysis

4. The general description of the Proposal

The proposed system used fingerprint to authenticate the user and consist of two phases (registration phase and authentication phase) . When the user enters his/her fingerprint image during the registration phase, pattern recognition process will be done to extract the user template and store it in server database. Server will select virtual fingerprint image for that user and apply fusion process to fuse the two fingerprint images (real and virtual). The result fused image will be stored in server and user databases to be used during the login phase as a type of secret sharing to authenticate that site . Figure (4) explain the block diagram for the registration phase. So when the user try to enter the system during the login phase will enter his/her fingerprint image to the server and pattern recognition process will be done to extract the user template and match it with the stored template, when a match accord that's means the user is authenticated, the server will display the fused image that's share it with that user during the registration phase, the user will compare the displayed image with the stored image with him, if match is accord this mean that's the site is trusted and not phishing site. Figure (5) explain the block diagram for the login phase. Algorithm (1) explain the image fusion process while algorithm (2) explain *Haar DWT*.

When the attacker can access in any way to the fused image that's stored in user and server databases may believe that this image is real fingerprint image because the fused image is still fingerprint and cant recognized as fused image and may use it to enter the system, but when pattern recognition process is done for that's image the server will know that this is fused image and not real fingerprint because it doesn't contains any minutia where the fusion process destroyed all minutia in the two images.

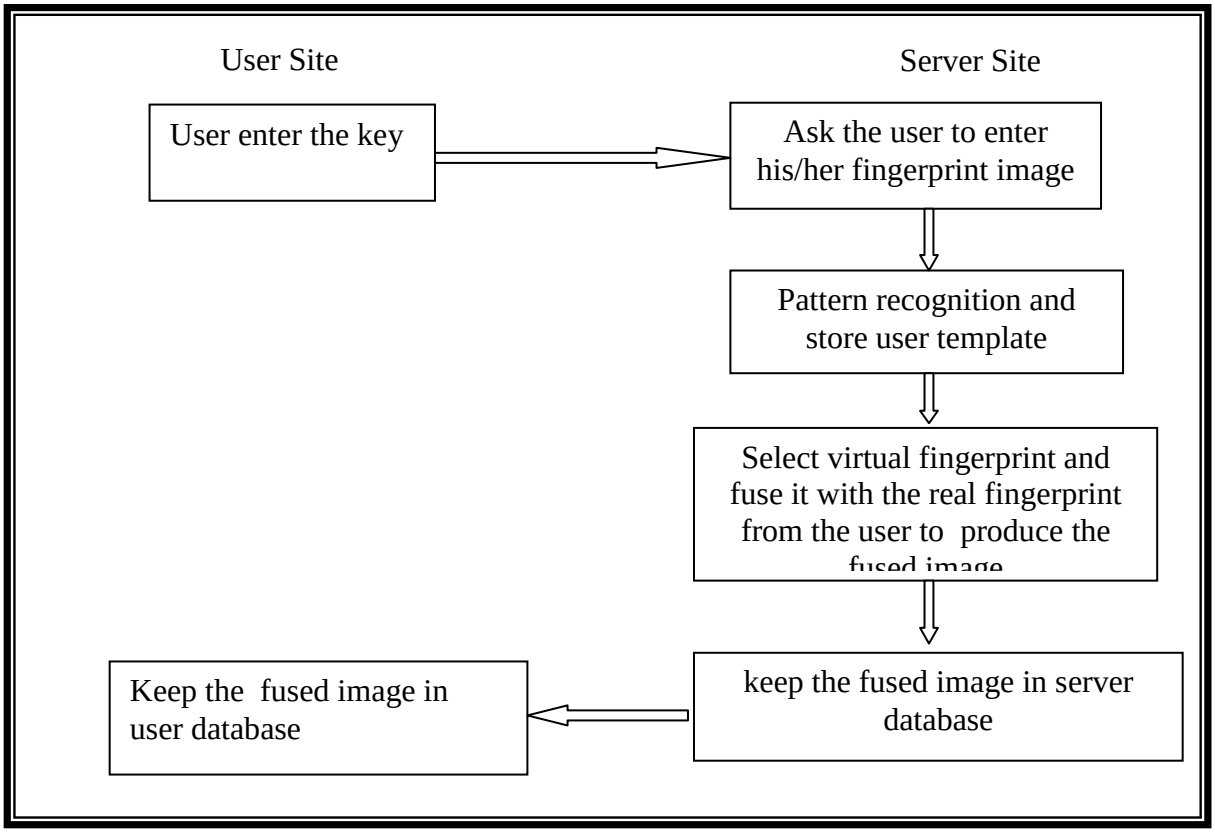

Figure (4) The block diagram of registration phase

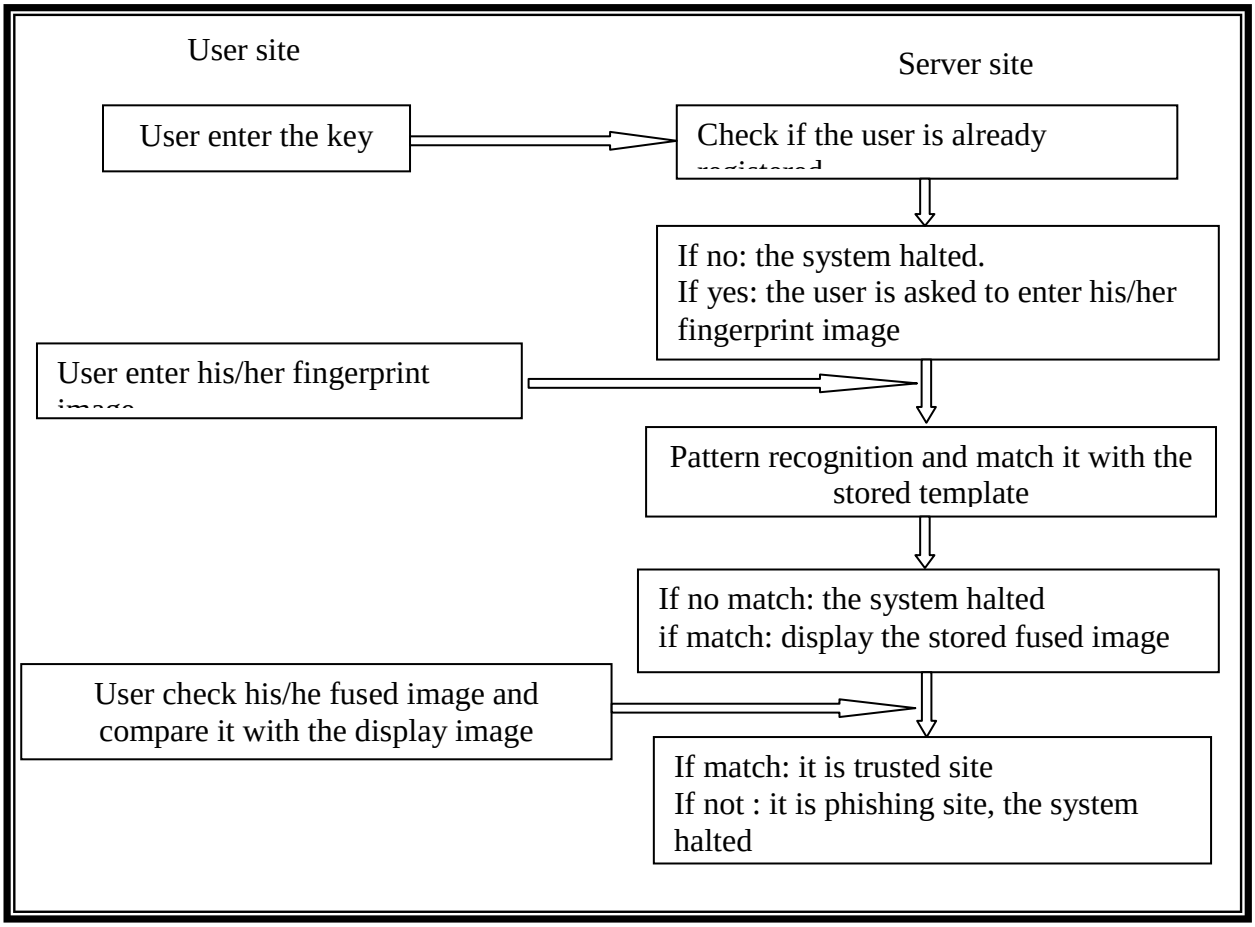

Figure (5) The block diagram of login phase

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 using Haar DWT on both input image see algorithm (3.10) Choose fusion rule and apply it to fuse each decomposition level Apply "inverse discrete wavelet transform" to get the fused image End process

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 for the two images by using DWT, second steps will be applying fusion rule like (MAX, MIN, MEAN) which is described in section (3) that is use the minimum, maximum and mean values for the transform coefficients. Third steps of image fusion will be applying inverse wavelet transform in order to reconstruct the fused image.

Figure (6) explain how to fuse two fingerprint images (mask image on the top left and bust image on the top right) where decomposition at "level 5" using "Haar" DWT and fusion by using the mean for both approximations and details (fused image on the lower left); fusion by using the maximum for approximations and the minimum for the details (fused image on the lower right).

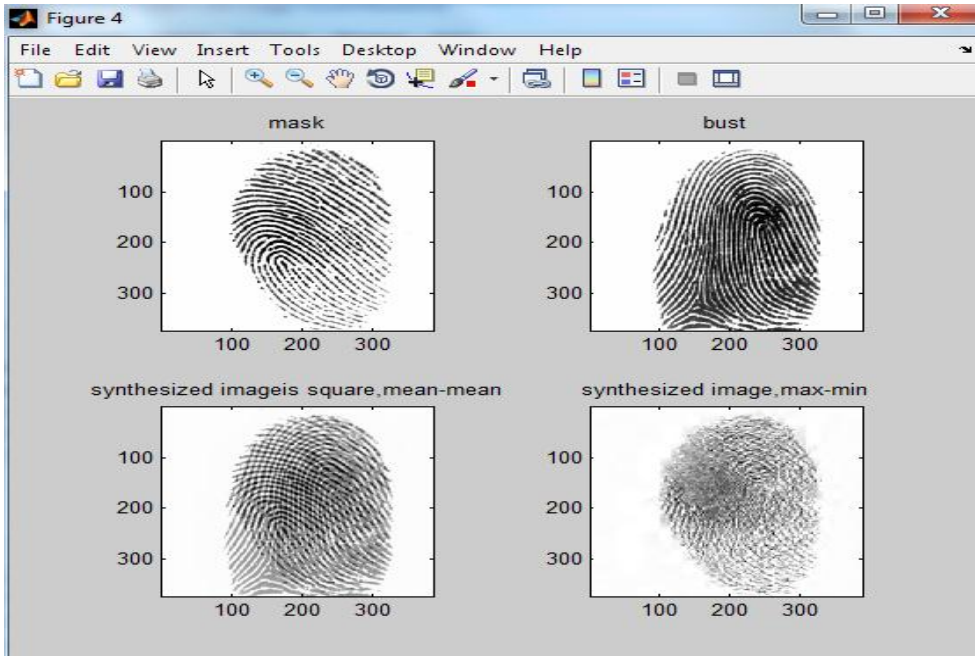

Figure (6) Show the result of image fusion technique

5. Experimental works and results

In this paper take 20 fingerprint images as reference image and fuse every two fingerprint images to produce 10 fused images. Now, will explain the results for some of the image quality metrics to assess the quality of fused image. Table (1) will explain entropy for each fingerprint image in addition to the fused image, the entropy is used to evaluate the information quality contain in an image. We can see high value of entropy for all fused images which is higher than all other images that used in the test which indicate that the information increase and this will improve performance.

Also the table explains PSNR and RMSE. From the result can see that high values of PSNR and small values of RMSE which is indicator for better fused image .

Table (1) Entropy for Reference and Fused Image

Entropy of image1	Entropy of image2	Entropy of fused image	PSNR	RMSE
5.3108	6.1511	8.4988	2.295	0.246
3.2247	5.1432	8.4913	2.088	0.223
4.387	6.8476	8.5078	3.200	0.243
6.2198	6.1792	8.4748	2.750	0.160
5.2479	5.1758	8.4618	3.626	0.224
5.963	6.848	7.583	2.938	0.166
4.723	5.464	7.082	2.427	0.158
5.176	6.649	7.346	2.441	0.183
6.223	6.876	7.611	2.998	0.204
4.824	7.019	7.389	3.524	0.148

Figure (7) show the graph for the entropy value for the reference images and the fused images, it's clear from the graph the high value of entropy for all fused images when compared with their reference images.

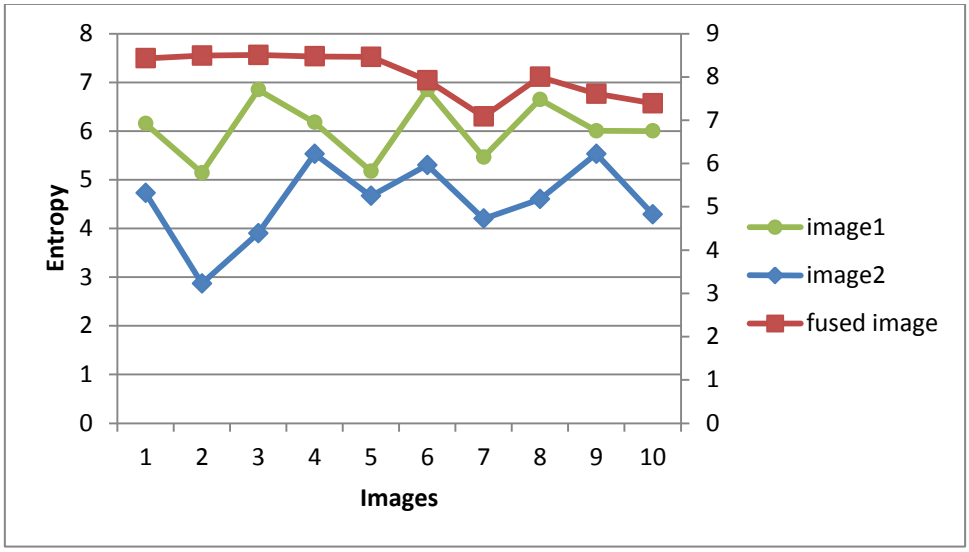

Figure (7) Entropy of reference images and the fused image

Table (2) will use the same samples of fingerprint image in table (1) but use different wavelet functions, level of decomposition and fusion operators. For these parameters will find value of entropy, PSNR and RMSE for the fused images and the result were as follows:-

Table (2) Measures of Fused Images

Wavelet function	Level	Operator	Entropy	PSNR	RMSE
db2	5	Max-min	8.5469	2.320	0.240
db2	5	Mean	8.4939	2.207	0.260
Haar	4	Max-min	8.1137	2.750	0.216
Haar	4	Mean	8.2113	2.295	0.246
db1	5	Mean	8.2025	3.098	0.223
db1	5	Max-min	8.123	2.910	0.169
Sym2	5	Mean	8.5469	3.630	0.224
Sym2	5	Max-min	8.4239	3.784	0.270

In table (2) used four different wavelet function which is (db2, Haar, db1 and sym2) but it's so clear, the result values 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. These wavelet functions belongs to large collection of wavelet transforms discovered by Daubechies. The Daubechies wavelet transforms are defined in the same way as the Haar wavelet transform and differs in how scaling functions and wavelets are defined.

by experiment find the "mean" fusion operator give best result when compared with the "max and min" operators where the mean give clear fused image as will show in the following example to fuse two images as shown in figures (8) and (9) which show the mask and bust images, while figure (10) show the fused image when using "mean" operator and figures (11) and (12) explain the fused images by using the "max" and "min". In this example used Penguins images not fingerprint images in order to clarify which operator gives best results because fingerprint consists of ridge and valley and can't recognize the best operator well.

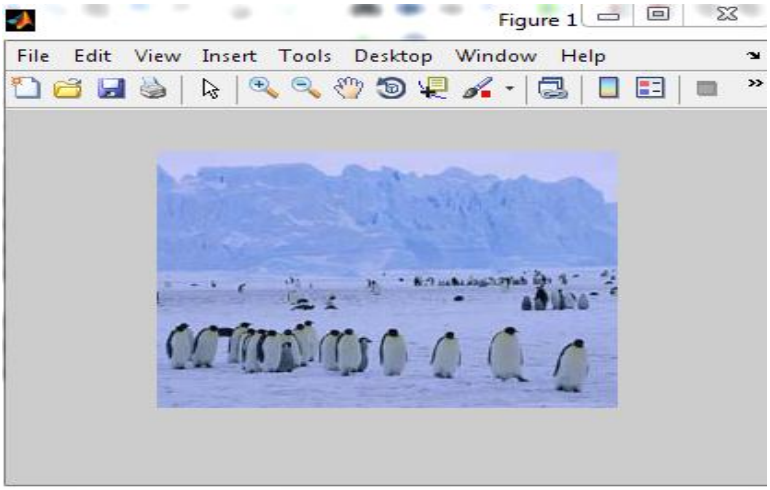

Figure (8) Show the mask image for fusion technique

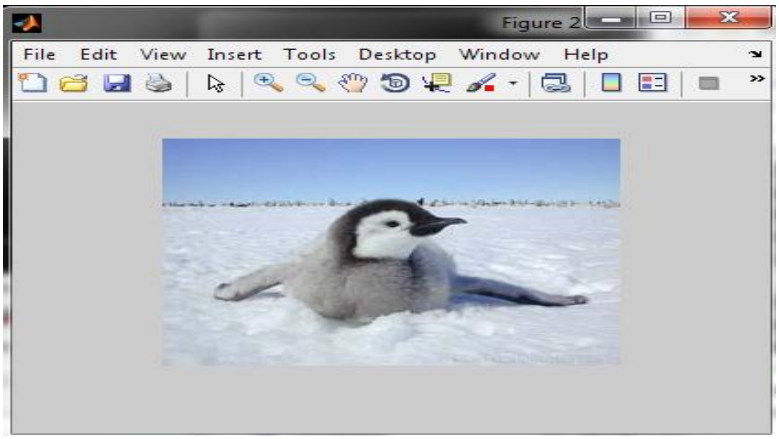

Figure (9) show the bust image for fusion technique

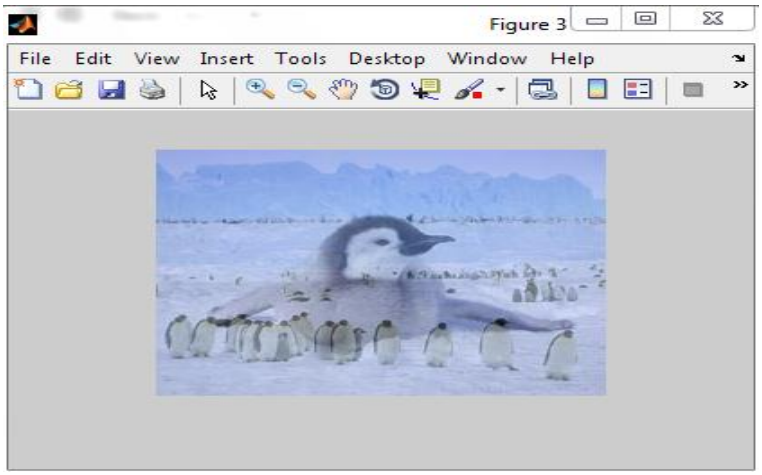

Figure (10) show the fused image by using "mean" for details and approximation

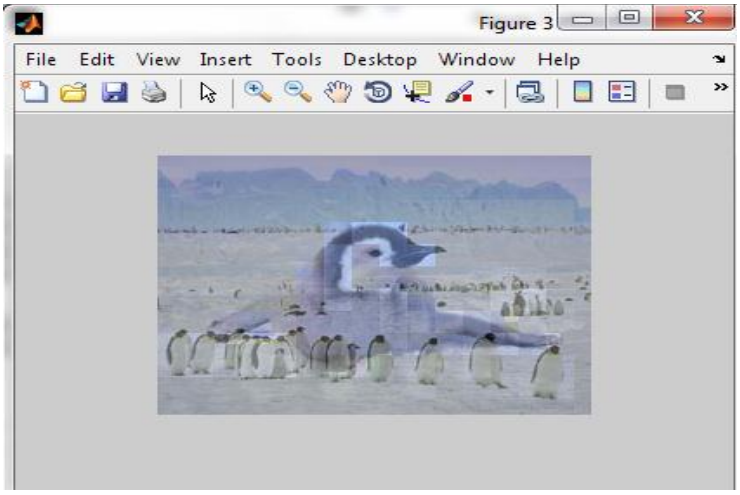

Figure (11) show the fused image by using "max" for details and approximation

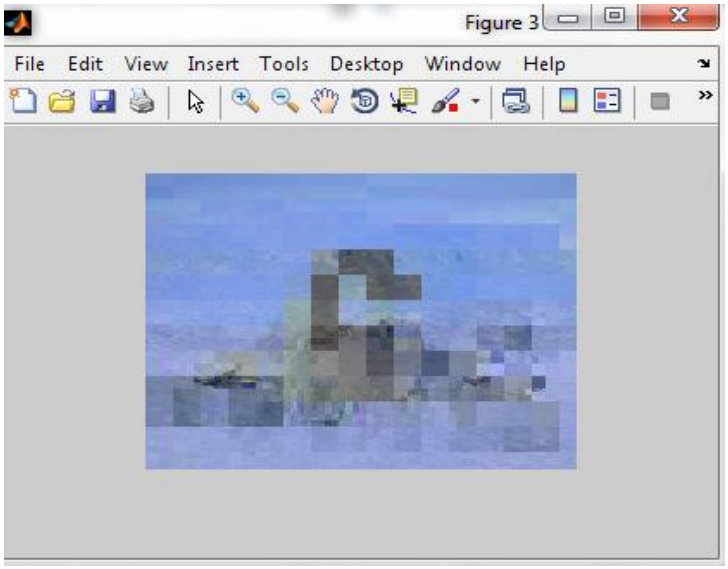

Figure (12) show the fused image by using "min" for details and approximation

6. Conclusions

In traditional authentication techniques, such as username and password are not secure, so the proposal provides authentication system against phishing attacks by using two layers of security (biometric and image fusion) in order to authenticate both sides (user and website) to each other. The image fusion technique that are used in this proposal give the fused image high value of entropy which make the images more informative and cheating the attacker. When using different wavelet functions the result values of entropy, PSNR and RMSE so close to each other, this indicates to there is no wavelet basis, which is better than others, Finally proposal proves the "mean" operator give the best result (clear fused image) among the others operators but the value of PSNR and RMSE still close to other operators.

References

1. Dhmij R., Tyger J.D., and Hearst M. "Why Phishing Works", Proceeding Of CHI-2006: Conference on Human Factors In Computer Systems, ACM 1-59593-178, April 2006.
2. Chhikara J., Dahiya R., Garg N., and Rani M., "Phishing & Ant 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., and Haining W., "Bogus Biter: A Transparent Protection against Phishing Attacks", ACM Transaction on Internet Technology, Vol.10, No. 2, Article 6, May 2010.
5. Sahu D. K. and Parsai M. P., "Different Image Fusion Techniques-A Critical Review", International Journal of Modern Engineering Research, Vol. 2, Issue.5, Sep.-Oct., 2012.
6. Umaamaheshvari A., and Thanushkodi K. "Image Fusion Techniques", International Journal of Research and Reviews in Applied Sciences (IJRRAS), Vol. 4**,** Issue 1, July 2010.
7. Zheng H., Zheng D., Yanxing H., and Sheng L., "Study On The Optimal Parameters Of Image Fusion Based On Wavelet Transform", Journal Of Computational Information Systems, January 2010.
8. Patil A., and 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.
9. Hamsalekha R., and 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.
10. Hamsalekha R. and 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, January2015.
11. Sahu D. K. and Parsai M. P., "Different Image Fusion Techniques-A Critical Review", International Journal of Modern Engineering Research, Vol. 2, Issue.5, Sep.-Oct., 2012.
12. Rani K. and Reecha S., "Study on Different Image Fusion Algorithm", International Journal of Emerging Technology and Advanced Engineering, Vol. 3, Issue 5, May 2013.
13. Patil A. and 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, March 2015.
14. Gupta D. and Choubey S., "Discrete Wavelet Transform for Image Processing", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 3, March 2015.