ROBUST WATERMARKING USING HAND GESTURE FOR ENHANCED AUTHENTICATION

Woo Chaw Seng, Leong Lai Fong, Ng Liang Shing, Saied Ali Hosseini Noudeh
Department of Artificial Intelligence
Faculty of Computer Science and Information Technology
University of Malaya, Malaysia
Email: cswoo@um.edu.my, lsng@um.edu.my

ABSTRACT

According to Bell Lab's finding, a large percentage of passwords chosen by users were easy to decode in a short period of time. As users realize the importance of security and privacy, there is a rapid increment of higher security demand in authentication systems. In this work, a gesture authentication system built with a robust watermark algorithm is presented. This biometric authentication system is divided into two modules, which are watermark embedding module and watermark detection module. For watermark embedding module, the first level of DWT is applied to the host image. Hand gesture image (watermark) is embedded into a host image using LSB and the redundant embedding method. For watermark detection module, the watermarked image will be processed and the majority voting method is used to retrieve the watermark from watermarked image. Non-blind watermarking is emphasized in watermark detection module. Various tests have been evaluated in both modules. Firstly, the effectiveness and fidelity tests are evaluated for watermark embedding module and both results are pass. Secondly, all the detection effectiveness test (pass) and robustness test using JPEG Compression (98.34%), Gaussian Noise (98.34%), Median Filtering (85.48%) and Contrast Adjustment (98.34%) have satisfying results. As conclusion, this algorithm is suitable to be applied in any type of image authentication system.

Keywords: Watermarking, Robust, Authentication, Hand Gesture, Biometrics, DWT, LSB

1. INTRODUCTION

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.", Mark Weiser's idea on pervasive computing [1]. This concept is highly implied in watermarking technology, as properties of watermarks are watermark messages which are hidden during normal use and only visible during a special viewing process in which watermarks carry information about an object that is the identity of the object [2].

In business and personal life today, security protection system play an essential role in various application domains, including: (a) personal and public safety; (b) computer and network security (terminal user verification); (c) transaction protection (client verification); (d) access control (key or keyless) [3]. However, most of the authentication systems today are static-single-password-based. According to Bell Lab's finding, a large percentage of passwords chosen by users were easy to decode in a short period of time [3]. Hence, more secure and effective authentication methods are now in great demand. In this paper, we presented an innovative idea – combining biometric (hand gesture) with the watermarking technique in authentication system.

The objective of this research is to develop a robust watermark algorithm which can be implemented in authentication systems with the digital watermarking and biometric method. The motivation behind this research is that human are easier to remember image compare to text. The problem that users forgetting their passwords can be overcome by using hand gesture images to replace the password. Besides that, watermark has been used in many applications such as broadcast monitoring, owner identification, proof of ownership, transaction tracking and authentication.

For this system, users are allowed to select any image to be the validation key for the authentication system. For instance, user could capture a host image with camera as his/her login password. Human face image will be used as an example in this authentication system. Although the human face image is changed differently with different expression and orientation. A hand gesture could be chosen as the second validation key by considering the hand geometric and the observed gesture. The hand gesture is the password for login. Verification performance could be improved by using hand gestures as a validation key. Host images and hand gestures will act as a biometric authentication method in which login password will be replaced with traditional authentication methods. Digital

watermarking is a way that is used to embed hand gesture images in host image which will be used during authentication.

One of the assumptions made in this research is that the hand gesture image is monotone, as it is important to have a high contrast between the background image and the object as the hand gesture image. Thus, the hand gesture image must be a black and white (0-255 grey level, but not RGB) image during watermark embedding and watermark detection processes. Besides that, the dimension of watermark must be smaller than host image.

This paper is divided into five sections. Section one describes about the problem statement, the project scope, the project objective and some of the project assumptions. Section two focuses on the related literature about digital watermarking and biometric. Section three investigates about the algorithm of digital watermarking. Watermark embedding and watermark detection processes are discussed here. Section four is about all the testing and experiment result analysis for the embedding and detection processes. Robustness and fidelity of watermark will be discussed in this section. Lastly, section five includes summary and recommendations for this research finding.

2. BACKGROUND

In this section, we will discuss on 2.1 What is digital watermark?; 2.2 Discrete Wavelet Transform (DWT); 2.3 What is biometric?; 2.4 Current watermarking technologies.

2.1 What is Digital Watermark?

Watermark can be divided into two categories [4]: (a) visible watermark – a translucent layer of message overlaid on the primary object and is hard to be removed from the primary object; (b) invisible watermark – a hidden secret message in the primary object that changes the Least Significant Bit of the primary object.

There are three types of watermarking methods: (a) robust watermark – usually used in the system that strictly prevents someone to remove the watermark in the primary object, is perceptual transparency, high pay load, resist to signal processing operation, resist to geometric attack, against collusion attack and computational simplicity; (b) fragile watermark – usually used in protecting data by detecting the content modifications, but become undetectable after minor modifications to the object; (c) semi-fragile watermark – has the combination of both robust and fragile watermark characteristics, as it is very fragile to certain modifications while robust to others.

2.2 Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform (DWT), a combination of spatial domain and frequency domain technique, consisting irregular and asymmetric spatial and frequency information. DWT provides a good localization method to stationary signal, as every wavelet coefficient is calculated at every level of decomposition to ensure optimum identification for all watermark image regions. In this transform method, every image pixel is analyzed and decomposed into different scales and locations. Thus, it is a useful transform when dealing with image attacks in this research.

2.3 What is Biometric?

Biometric is a human identification technique by using validation key, which can be categorized as (a) physiological – the shape of human body such as the shape or geometric of a hand, fingerprint, iris, face and other parts of body; (b) behavioral – relates to human's behavior such as signature and voice. Every biometric has its advantages and limitations. Considering the low resolution of the camera phone, hand gesture is determined as a suitable biometric authentication method in this research.

2.4 Current Watermarking Technology With Biometric

Biometric techniques have inherent advantages compared with conventional single static password authentications. However, there are also concerns on security and privacy of biometric data, as it is impossible to replace it as in case of a credit card or ID when a person's biometric data is stolen. This problem can be solved by embedding watermark into the biometric host image, as to add another layer security into the biometric data.

In fact, researches have been worked on combining biometrics and watermarking algorithm [5-10]. Previous works have been undertaken on biometric data hiding involving the face and fingerprint images. Jain et.al. [11,12] proposed an effective way hiding eigenface into a fingerprint image. Besides that, Ratha et.al. [13] described a data hiding method applicable to wavelet compressed fingerprint images. However, the drawback of these approaches is that the robustness impacted when compressing the watermarking before insertion. Pantanti and Yeung [14] developed a fragile watermarking for fingerprint images verification, as their watermarking technique does not lead to a significant performance loss in fingerprint verification. In Minerva et.al. [7], watermark is extracted using local-

based 5x5 cross-shaped neighborhood. This spatial domain based method has severe weakness against blurring attack. Other than that, Jaehyuck Lim et.al. [15] suggested the invertible watermarking algorithm based on compressed Regular and Singular (RS) bit stream. Although this method can detect the manipulation positions of watermarked biometric data, but it also suffers from various attacks specifically blurring and cropping. All previous work including fingerprint and face template protection[16] embeds biometric data in a robust manner but they lack the flexibility that allows the user to determine a unique input for watermarking. In our work, we allow the user to select a specific hand gesture for watermarking. In addition, this also increases the practical usage because we do not need to have specialized device to capture fingerprint image.

3. METHODOLOGY

There are 3 sub-sections discussed here, including: 3.1 System overview; 3.2 Image acquisition; 3.3 Watermark embedding process; 3.4 Watermark detection process.

3.1 System Overview

The watermarking authentication system includes two main modules which are watermark embedding process and watermark detection process.

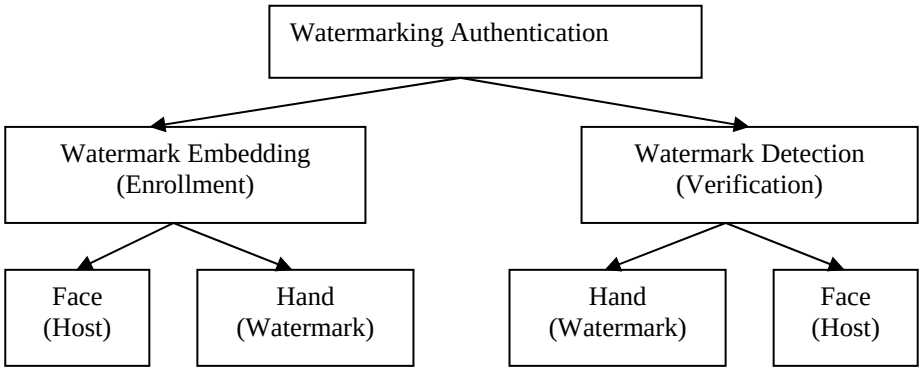

Figure 3.1: Watermarking Authentication System Overview

Watermark embedding process is taken place during user account enrollment to embed hand gesture image into edge of a host image. Watermark detection process is implemented in the verification step where the hand gesture image is retrieved from the edge of the original host image and then is compared with the original hand gesture image. The details of these two modules will be discussed in the following section.

3.2 Image Acquisition

Watermarking involved two color images which are host image and hand gesture image. Firstly, the user chooses any image to be the host image, which acts as the username for user. We use face as host image here. At the same time, a hand gesture image is captured by the user. This hand gesture image acted as the password for user to log in the authentication system. Users are allowed to capture different gestures - different styles and postures of hand. In this way, the probability for password to be known by others is decreased making it hard to be hacked.

Below are samples of host image and gesture images.

(a) (b) (c)

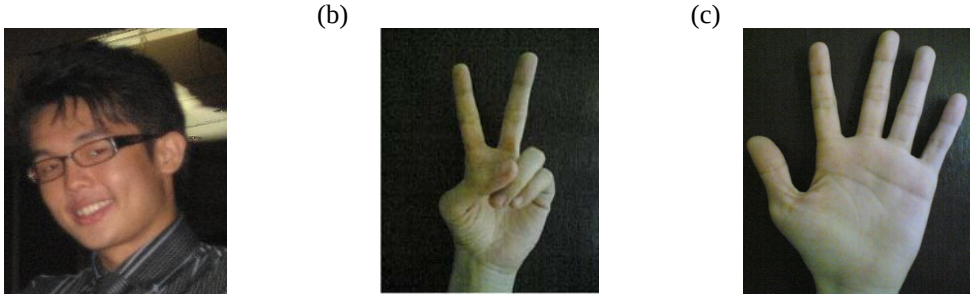

Figure 3.2 (a) shows a sample of host image while figure 3.2 (b) and 3.2 (c) show samples of different hand gesture images.

3.3 Watermark Embedding Process

The following figure shows the flow of the watermark embedding process.

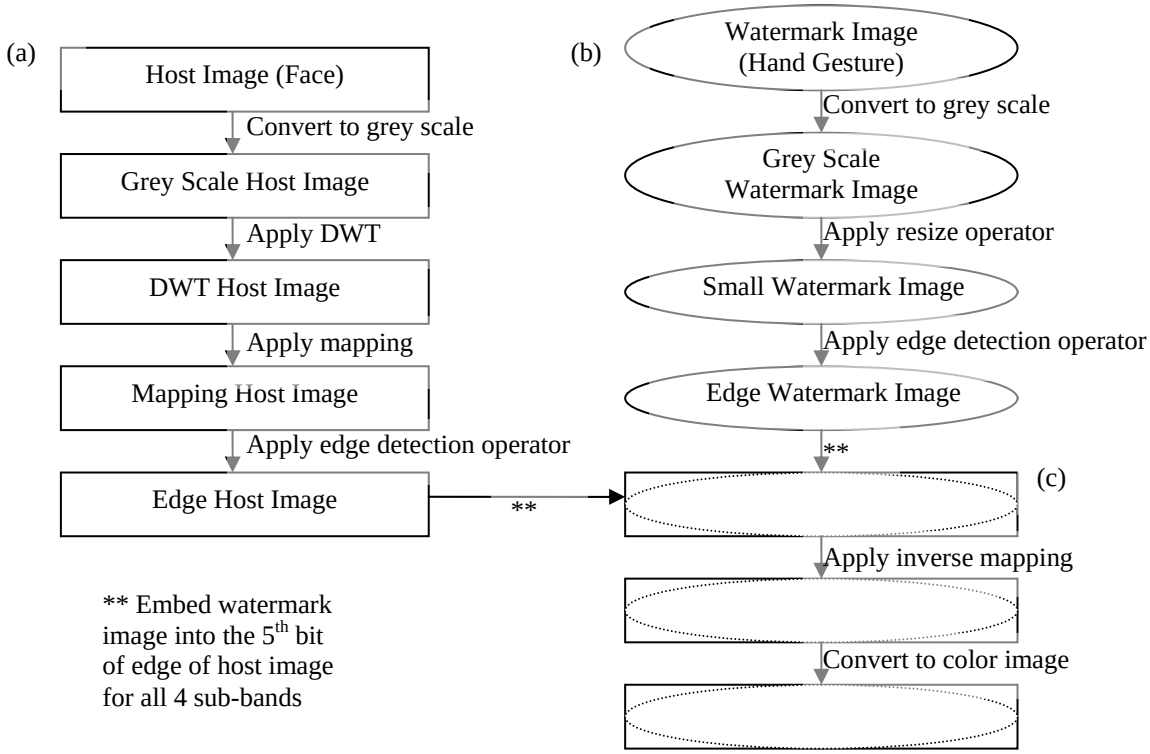

Figure 3.2: Watermark Embedding Process – (a) Host image embedding pre-processing, (b) Watermark image embedding pre-processing, (c) Watermark embedding process

(a) Host image embedding pre-processing

Host image is converted into grey scale image. The reason for this is because grey scale images have pixel value that ranges between 0-255. Then, the grey scale host image is decomposed into four sub-bands with equal sizes, so that the image pixel values become very small. After the completion of the first level of DWT, a mapping process will be done on the whole image. This is to ensure that the range of pixel value of DWT image will fall in the range of 0-255. Host image is always a 8-bit image. The mapping factor formula is shown below:

$$\text{map factor} = \frac{255}{\max(\max(I))} \qquad (1)$$

where i indicates the image's pixel value. After that, the edge of grey scale host image from the first sub-band will be detected. The reason of the detection of edge for the first sub-band is because the edge is the active image location. These edge locations will be used to embed the hand gesture image information.

The reasons that edge will be chosen as the embedding location because the human eye perception is less sensitive to the edge. If above the edge of an image is modified, human are not easy discover it.

(b) Watermark image embedding pre-processing

Hand gesture image is also converted to grey scale image and then went through the first level DWT. In order to ensure that the hand gesture image could be embedded into host image, the size of hand image must be smaller than the host image. A formula will be created to ensure that the hand image size is always smaller than host image. This formula is very useful during the process of watermark detecting. Formula is show below:

$$size = sqrt(numel(find(e == 1))) \quad (2)$$

where size is the resize hand gesture image and e is the edge of host image. numel and find function are used to find the edge of an image.

After resizing of the hand gesture image, edge detection applied to the image. Then a black and white 1 bit hand gesture image is gained.

(c) Watermark embedding process

Edge host image and edge hand gesture image will undergo embedding process. 1 bit of hand gesture image is embedded one by one into the edge of host image. The embedding process consists of embedded hand gesture image to all sub-bands. The embedding process is repeated four times. First is the embedding between hand gesture images with low sub-bands (approximation sub-bands or LL sub-bands). Then the hand gesture image embedded with the second sub-bands which is the LH sub-bands. The process is repeated four times until all the four sub-bands are embedded successfully. The reason to embed a watermark to all four sub-bands is because of the redundancy property will make it robustness. If one of the sub-bands of face image is attacked, there is another sub-band which contains important information of the hand gesture image. Formula below shows the embedding for all four sub-bands:

$$watermarked^{\theta}(r,c) = host^{\theta}(r,c) + hand^{\theta}(r,c) \quad (3)$$

where θ is sub-bands value from 0-3, r is row of sub-band and c is column of sub-band. “watermarked” is the watermarked image. “host” is the original host image. “hand” is the hand gesture image. If value θ is 0, it is indicates that this belongs to the LL sub-band or approximation sub-band. If θ is 1, it belongs to LH sub-band which is the horizontal sub-band. If θ is 2, it belongs to HL sub-band which is the vertical sub-band. If θ is 3, it belongs to HH sub-band which is the diagonal sub-band.

The 1 bit of hand gesture image will be embedded into the 5th element of 8 bit host image. All the positions are tested. The 5th position would give the best performance compare to other bit positions in host image. This process will continue until all the hand gesture image is embedded into host image. A watermarked image is gained. Figure 3.3 shows that a host image consists of 8 bit for each pixel value. Hand gesture image is 1 bit for each pixel value. The bit positions are showed. The embedding process is embedded the 1 bit hand gesture image into the 5th position of a host image.

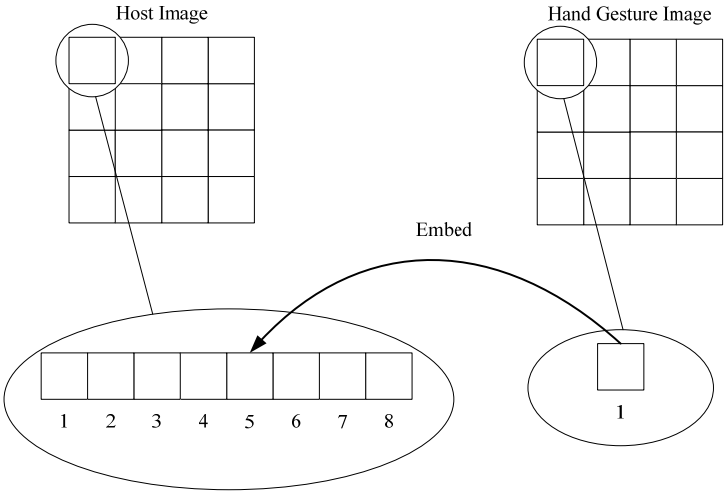

Figure 3.3 Embedding Process

Then IDWT (Inverse Discrete Wavelet Transform) will be applied to the watermarked image. A reverse mapping process will be done onto the pixel value of watermarked image. This is a reconstruction process that convert image to original signal without loosing information. After that the watermarked image will be converted into color image and store it at a location for the watermark detecting process. Watermark embedding process is successful. Figure 3.4 shows the example of watermarked image.

Figure 3.4: Example of Watermarked Image

The following figure shows that the process of embedding a hand gesture image into host image and a watermarked image is obtained.

Figure 3.5: Example of Embedding Process

Comparison between original host image and the watermarked image is made. From the perceptual of human vision, it is very difficult to differentiate the differences between these two images. Left hand side is the original host image; right hand side is the watermarked image which is the original host image with the watermark; middle is the watermark image or hand gesture image.

The figure below shows the edge detection of hand gesture image which will be used in the following process. Figure 3.6 is an example of watermark.

Figure 3.6 Example of Watermark

3.4 Watermark Detection Process

Watermark detection process involved the process of extracted the watermark and then compare it with the original hand gesture image to verify the authentication. The following figure shows that the watermark detection process:

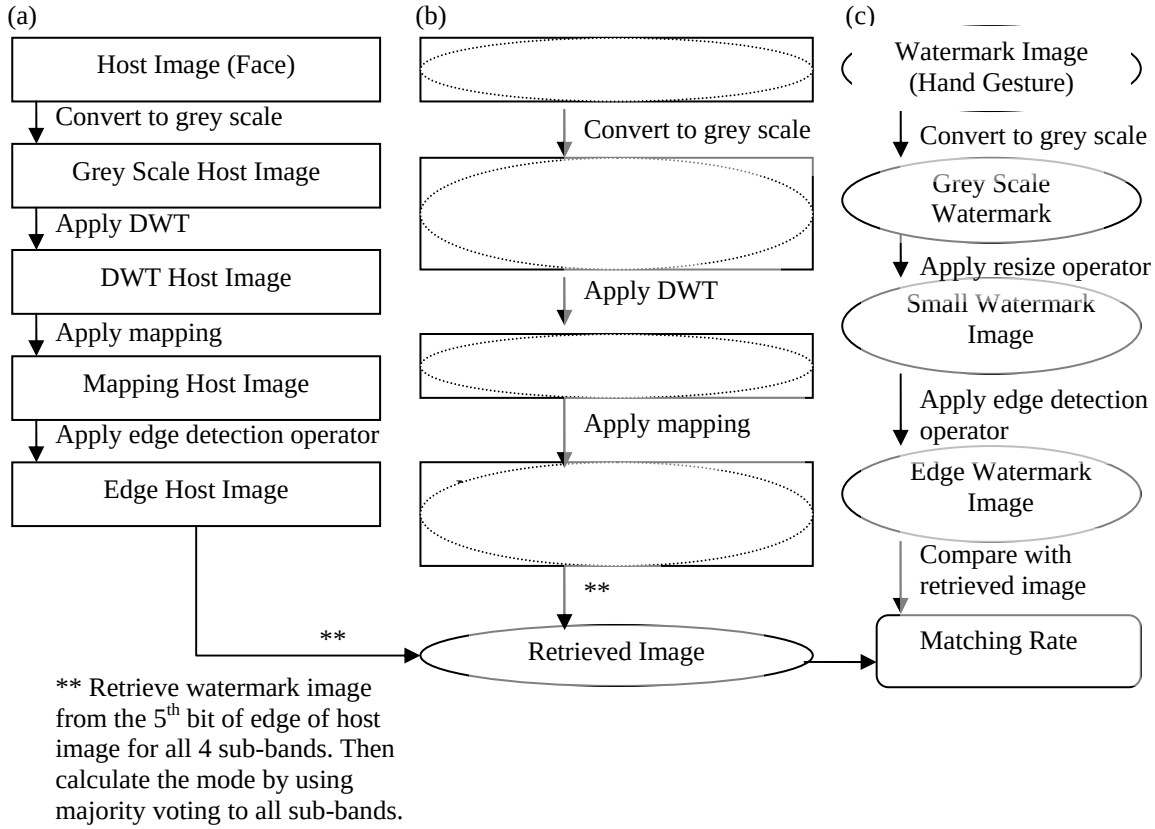

Figure 3.7: Watermark Detection Process – (a) Host image detection pre-processing, (b) Watermark detection pre-processing, (c) Watermark verification process

(a) Host image detection pre-processing
The original host image will went through the same process as watermark embedding process.

(b) Watermark detection process
Firstly, color watermarked image will converted into grey-scale image and then DWT operator is applied. After that is mapping process and the edge of host image is detected. The edge of the original host image is detected because edge will be used as the reference to retrieve the hand gesture image which already embedded in watermark embedding process. According to the edge location, the actual watermark would be retrieved correctly.

The watermark hand gesture image will retrieved from the 5th bit of edge of original host image. This process will repeated four times for all sub-bands. A majority voting formula is created to calculate the

majority voting for each of the sub-bands. Firstly, first pixel value for each sub-band will be retrieved. Then the majority voting formula is used to obtain a major vote of pixel value. This pixel value will store in temporary memory. This process is repeated until gone through all the pixel value of the image. Finally, a retrieve watermark image is obtained. For the approximation sub-band, it will be given the highest voting compare to the other three sub-bands. It is because this sub-band is the downscale version of the original host image. This sub-band consists of the most important information for original image. Hence, it contains the highest voting compared to other sub-bands.

The formula below is used to calculate the majority voting for all sub-bands.

$$\text{majority voting} = \text{mode}(s^0 + s^0 + s^1 + s^2 + s^3) \quad (4)$$

where majority voting is the pixel value which will be used to form retrieve watermark image and then will compared with the original hand gesture image. s^0 is pixel value for approximation sub-band, s^1 is pixel value for horizontal sub-band, s^2 is pixel value for vertical sub-band and s^3 is pixel value for diagonal sub-band. mode is a function to calculate the most frequency pixel value of an image. The pixel value that used in this stage is either 0 or 1. The voting value is associated to only one pixel. This formula will be applied to all the pixel values of an image. All this voting value will be cumulate to form a hand gesture image. Table below contains some examples to calculate the vote.

Table 3.1 Example of Majority Voting

S0	S0	S1	S2	S3	Majority Voting
1	1	1	1	1	1
1	1	1	1	0	1
1	1	1	0	0	1
1	1	0	0	0	0
0	0	0	0	0	0

From the calculation, the entire majority voting for each pixel for an image is cumulated to form a retrieve watermark image. Figure below shows that the retrieved hand gesture image.

Figure 3.8: Retrieved Hand Gesture Watermark

(c) Watermark verification process

After that is the verification process. In order to compare the retrieved hand gesture image with the original hand gesture image, a similar process as watermark embedding will be applied to both of the images. The hand gesture image will went through the grey scale operator, resize operator and edge detection operator. When a watermarked hand gesture image is retrieved, it compared with the original hand gesture image.

Figure 3.9 shows that the comparison between the original hand gesture image (watermark) with the retrieved hand gesture image.

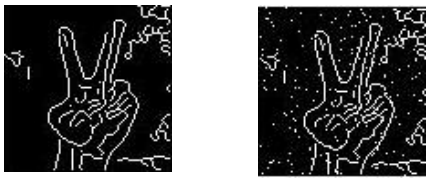

Figure 3.9: Retrieved Watermark Compare with Original Watermark

If there are perfect matches between the original hand gesture image with the retrieved hand gesture image, authentication is successful. If not matching is found, authentication process will consider fail. The comparison formula to determine the matching rate is show below:

$$\text{matching rate} = \frac{\text{compare}(\text{edge}^r, \text{edge}^o)}{\text{totaledge}^o} \times 100\% \quad (5)$$

where edge^r is edge of retrieved hand gesture image , edge^o is edge of original hand gesture image. totaledge^o is the total number of edge of original hand gesture image. compare is a function used to compare the edge of retrieved hand gesture image with edge of original hand gesture image.

Matching rate is also known as the percentage of watermark detected correctly. Total number of watermark is calculated. Comparison between the edge of retrieved hand gesture image and edge of original hand gesture image is the determinate for the matching rate. If both images have high comparison value, the matching rate is also high.

4. ANALYSIS OF EXPERIMENT RESULTS

This section provides the experiment results for the authentication algorithm in both the watermark embedding module and watermark detection module (as in section three). Firstly, testing properties in watermark embedding process that to be tested are effectiveness and fidelity. Secondly, testing properties in watermark detection process that to be tested are detection effectiveness result with respect to non-blind watermark and robustness. (Fridrich. J. & Goljan. M.).

4.1 Watermark Embedding Experiment Result Analysis

(a) Embedding Effectiveness Test Result Analysis

The definition of effectiveness of an embedding watermark process is the percentage of the output of embedder will be watermarked. According to Cox, I. J. (2002), embedding effectiveness is the probability of detection after embedding. Result of effectiveness might not get 100% because the result is depended on application. The performance of watermark embedding process is considered with respect to other properties such as fidelity.

For watermark embedding process, a hand gesture image is embedded into a host image. After the embedding process, a test is done to verify whether the embedding process is successful. Verification for the successful rate of embedding process is done by comparing the original host image with the watermarked image. In the comparison process, an edge detection operator is applied to the host image and all the edge pixels are compared. If the result shows a positive embedding, the percentage of getting correct watermark is recorded.

Figure 4.1(a) shows the original host image, Figure 4.1(b) shows the watermarked image and Figure 4.1(c) shows the absolute difference between original host image and watermarked image. The watermark is hidden only in the edge of host image which is categories as high activities region of an image.

(a) (b) (c)

Figure 4.1: (a) Original Host Image, (b) Watermarked Image and (c) Absolute Difference between Original Host Image and Watermarked Image.

(b) Embedding Fidelity Test Result Analysis

Fidelity means there is no difference between original image and watermarked image that could be seen by using human eye perception. For different application, fidelity will be used to cater the robustness of system. For this watermark system, the balances between robustness and fidelity must be achieved. So, a small distortion will not affect the coefficient value of image.

Referring to Figure 4.2, it has been proven that from human perception, we are not able to detect the difference between both images. Two images from Figure are the same images from Figure. The left hand side image is the original host image. The right hand side image is the watermarked image which contains the hand gesture image (watermark image) in it. According to the experiment from section 4.1.1, it has proven that both images have a very big difference. The high activity region of host image is embedded with hand gesture information. From human perception, we are not able to distinguish. With the used of watermarking system, the differences is very obvious. Conclusion, this experiment shows that watermarked image had passed the fidelity test.

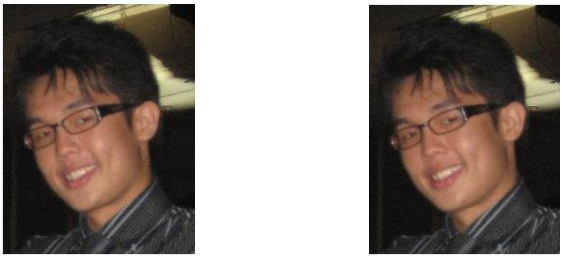

Figure 4.2: Fidelity Testing

4.2 Watermark Detection Experiment Result Analysis

(a) Detection Effectiveness Test Result Analysis

For detection process, two processes will be done which are retrieved watermark and compare watermark image with original image. Non-blind detection is used in this watermark detection process. Original host image and original hand gesture image are available during detection process. This could improve the performance of detector because the original host image could subtract from watermarked image and then the watermark could retrieve. Original image could used to face attack from different type of digital processing.

Firstly, watermarked image will compare with original host image. Then watermark which is a hand gesture image will be retrieved from watermarked image and then compare with the original hand gesture image. In order to verify the successful of the comparison between original hand gesture image with retrieved hand gesture image, a matching rate equation is used to determine the matching rate. The result is about 98.34%. This result shows that there is minor difference between the original hand gesture image and the retrieved hand gesture image. This is because during the process of converting the image to color image or the process of converting the image from color image, the coefficient could be varied from the actual coefficient value. In addition, converting from color image to grey-scale image or grey-scale image to color image, DWT and mapping processes would cause some noise to the image.

Figure 4.3(a) presents the original hand gesture image and Figure 4.3(b) presents retrieved hand gesture image from watermarked image. Comparison between both images is shown as below. There is much noise in retrieved hand gesture image compare to the original. The successfully rate for this detection process is about 98.34%.

(a) (b)

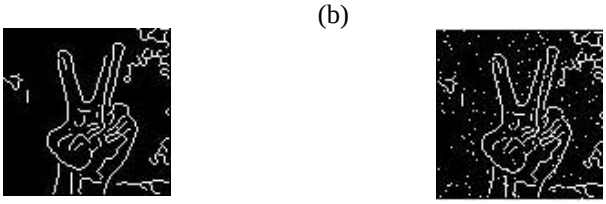

Figure 4.3: (a) Original Hand Gesture Image and (b) Retrieved Hand Gesture Image.

Another hand gesture image is tested with the same algorithm to verify the percentage of watermarks detected correctly. The result shows that this algorithm provides a very high and accurate of authentication rate. The percentage of watermarks detected correctly is about 97.18%. Figure 4.4 shows the comparison between original hand gesture image with retrieved hand gesture image. This is another gesture image compare to the previous.

(a) (b)

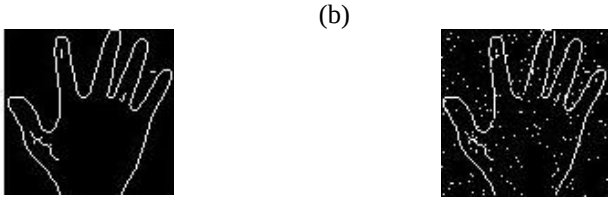

Figure 4.4: (a) Original Hand Gesture Image and (b) Retrieved Hand Gesture Image.

From both of these results, it shows that with different hand gesture image or password to login, the authentication process still able to get very good result. This algorithm is able to detect and identify the users' identity in a very high accurate rate.

(b) Detection Robustness Test Result Analysis

A lot of robustness tests are done to examine the robustness of watermarked image or watermarked image such as JPEG compression, apply Gaussian noise, apply median filtering and apply contrast adjustment. All this tests are considered as attacks to the image. All this tests will do above the watermarked image. Comparison is done between original watermarked image with the watermarked image after applying attacks. The difference between both images will be measured using equation (5). Matching rate in equation (5) is same as the percentage of watermarks detected correctly.

JPEG CompressionTest

JPEG compression attack is simulated on watermarked image when data is lost during compression. The highest the number of quality factor means that the better the quality of image, because the image experience low image degration by the compression. Table 4.1 shows that watermarked image is tested with different quality factor.

Table 4.1: Result of Apply JPEG Compression

Quality Factor	100%	85%	70%	55%	25%
Percentage of watermarks detected correctly	**98.34%**	72.48%	68.20%	64.18%	51.45%

Gaussian Noise Test

Gaussian Noise is an insertion of noise to the intensity of image by varying the variance values and it is wary to analyze. The robustness of watermark is investigated by adding Gaussian noise with zero mean and increasing variance to the watermarked image. Watermarked image was start distorted with variance of 0 and then variance is increased 20% each time. Table 4.2 shows the result of this robustness test.

Table 4.2: Result of adding Gaussian Noise

Variance of Gaussian Noise	0.0000	0.0002	0.0004	0.0006	0.0008	0.0010
Percentage of watermarks detected correctly	**98.34%**	79.67%	76.21%	69.71%	67.50%	68.60%

Median Filtering Test

Median filtering is an enhancement method to reduce noise without blurring or decreasing the sharpness of an image, by considering the median of neighboring pixel values. Application of median filtering is depend on the energy of watermark message in each frequency. A robust watermark may design the watermark to have most energy in frequency to minimize the filter changes. In the median filtering test, we investigate the robustness of watermark using 3x3 median filtering and 5x5 median filtering. Table 4.3 shows the results of applying 3x3 median filtering and 5x5 median filtering to the watermarked image.

Table 4.3: Result after applying Median Filtering

Median filtering Type	3x3	5x5
Percentage of watermarks detected correctly	**85.48%**	**85.48%**

Both results show the same percentage of watermarks detected correctly, which is 85.48%. The same result indicates that the affected location is only on the center of each 3x3 block or 5x5 block, where the center value is replaced by median value of 3x3 block or 5x5 block respectively.

Contrast Adjustment Test

Contrast adjustment is used to change the intensity of an image to become brighter or darker comparing to the original image, as to sharpen an image or remove noise from the image. The contrast of image could be adjusted using gamma correction factor. The default value for the gamma correction factor is 1.0 which means that it is an original image without applying any contrast adjustment on it. The image will become brighter for gamma correction lower than 1.0, while it will become darker for gamma correction higher than 1.0. Table 4.4 shows the results of applying 0.5 and 1.5 gamma correction factor to the watermarked image.

Table 4.4: Result of Contrast Adjustment

Gamma Correction Factor	0.5	1.0	1.5
Percentage of watermarks detected correctly	77.18%	**98.34%**	72.20%

From the table result, it has shown that the percentage of watermarks to be detected correctly is above 70% after contrast adjustment. This indicates that contrast adjustment to an image would probably change the image.

5. CONCLUSION

As conclusion, we have built an authentication algorithm system by using digital watermarking and biometric. In our research, the authentication algorithm consists of two main modules which are embedding and detection to enhance the security of authentication. Hand gesture image is embedded into host image in the embedding module; while the hand gesture image is detected in host image in the detection module. Experiments and testing have done and the results (as in section four) had proven that the image had passed the robustness and fidelity test. A watermark with balance robustness and fidelity is gained. Our work allows flexibility of choosing hand gesture as opposed to most other methods that used fingerprint as watermark.

However, a few interesting areas for further enhancement are identified. We suggest incorporating facial watermark in watermarking system, multimodal biometric method, locating center of gravity (CoG) to improve the verification performance and implementing this algorithm in mobile platform.

Acknowledgement

We thank the researcher, Miss Hon Pue Kuan for her contribution in programming work of this research.

Reference

[1] Norbert Streitz, Achilles Kameas, Irene Mavrommati, "The Disappearing Computer: Interaction Design, System Infrastructures and Applications for Smart Environments", Springer Publisher, 2007, pp12.

[2] I.J.Cox, M.L. Miller and J.A. Bloom, Digital watermarking. San Francisco, Morgan Kaufmann Publishers.

[3] S.Y.Kung, M.W.Mak, S.H.Lin, Biometric Authentication – A Machine Learning Approach, Prentice Hall.

[4] C.I.Podilchuk, E.J.Delp, Digital Watermarking: Algorithm and Applications, IEEE Signal Processing Magazine, pp 33- 46.

[5] H.Lin and K.J.Anil, Integrating faces and fingerprints for personal identification, IEEE Trans. On Pattern Analysis and Machine Intelligence, Vol 20, No. 12, pp 1295-1307, 1998.

[6] K.J.Anil, U.Umut and H.Rein-Lien, Hiding a face in a fingerprint image, Proc. Of Int. Conf. on Pattern Recognition, Vol 3, pp 756-759.

[7] M.Minerva and P.Sharath, Verification watermarks on fingerprint recognition and retrieval, Proc. Of SPIE Conference on Security and Watermarking of Multimedia Contents, Vol 3657, 1999.

[8] DongMei Sun, Qiang Li, Tong Liu, Bing He and ZhengDing Qiu, A secure multimodal biometric verification scheme, IWSBRS 2005, LNCS 3781, pp 233-240, 2005.

[9] Kang Ryoung Park, Dae Sik Jeong, Byung Jun kang and Eui Chul Lee, A study on iris feature watermarking on face data, ICANNGA 2007, Part II, LCNS 4432, pp 415-423, 2007.

[10] Gui Feng and QiWei Lin, Iris feature based watermarking algorithm for personal identification, Proc. Of SPIE, Vol 6790, pp 45, 2007.

[11] A.K.Jain and U.Uludag, Hiding fingerprint minutiae in images, Proc. Of 3rd Workshop on Automatic Identification Advanced Technologies, pp 97-102, 2002.

[12] A.K.Jain and U.Uludag, Hiding biometric data, IEEE Trans. On Pattern Analysis and Machine Intelligence, Vol 25, No. 11, 2003.

[13] N.K.Ratha, J.H.Connel and R.M.Boll, Secure data hiding in wavelet compressed fingerprint images, Proc. Of ACM Multimedia Workshops, pp 127-130, 2000.

[14] Pankanti S and Yeung M.M., Verification watermarks on fingerprint recognition and retrieval, Proc. Of SPIE, Vol 3657, pp 66-78, 1999.

[15] Jachyuck Lim et.al, Invertible watermarking algorithm with detecting locations of malicious manipulation for biometric image acquisition, LNCS, Vol 3832, pp 763-769, 2006.

[16] M. Vatsa et al.,Robust Biometric Image Watermarking for Fingerprint and Face Template Protection, IEICE Electronics Express, Vol.3, No.2, pp.23-28, 2006