VOL 1 (2017) NO 4 - 2

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

A Digital Image Watermarking System: An Application Of Dual Layer Watermarking Technique

Ch'ng Chen Phin[#], Nurul Hidayah Ab Rahman[#*], Noraini Che Pa[**]

[#] *Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Malaysia.*
[*] *Information Security Interest Group, FSKTM, Universiti Tun Hussein Onn Malaysia, Malaysia.*
[**] *Faculty of Computer Science and Information Technology, Universiti Putra Malaysia*

E-mail: hidayahar@uthm.edu.my

***Abstract*— Watermarking is a method to digitally sign a product to provide authentication and prevent copyright infringement to proving the ownership of a product and provides integrity for companies to protect their product. In this study, dual layer watermark that applies two different watermarking techniques at each layer is presented. The first layer applies the LSB Substitution technique while the second layer uses the Discrete Wavelet Transform (DWT) technique. This implies greater integrity as it contains of two signatures in providing authentication.**

***Keywords*— LSB, discrete wavelet transform, watermarking; integrity, copyright.**

I. INTRODUCTION

Digital watermarking technique is originally used in the photography market as a way of identifying the copyright owner of digital photos [1]. With the advancement of the digital media, the technique is increasingly being adopted with the motivation to protect intellectual property rights, information hiding and fingerprinting. For instance, in January 2009, the photograph on which Fairey allegedly based the design was revealed by the Associated Press as one shot by AP freelancer Mannie Garcia — with the AP demanding compensation for its use in Fairey's work [2]. In a case of theft or misusing images, there are no proof that the image is being misused by unauthorized party and claims that image is provided by authorized party since there is no 'signature' inside a digital image to provide authentication, copyright of digital images.

In this study, dual layer digital image watermarking is, therefore, proposed to protect the ownership of digital image. The objectives of this study are in two-fold:

- To design a watermarking system that prevent image being theft or misused by unauthorized party
- To develop a dual layer watermarking that provides greater integrity

Dual layer digital image watermarking refers two watermarks techniques to be applied into the digital image. The process is separated into two steps: (1) digital image watermarking process uses LSB Substitution Technique; (2) inserting watermark by applying Discrete Wavelet Transform Technique on digital image. Using two layers of watermarks increase the integrity strength as it contains two signatures to provide authentication.

II. BACKGROUND OF STUDY

A. Digital Image

Digital images are electronic snapshots taken from a scene or scanned from documents, such as photographs, manuscripts, printed texts, and artwork [12]. When these snapshots are taken or while the documents were scanned, it went through a process called digitization. Digitization is the process of transforming images, text, or sound from analogue media into electronic data that we can save, organize, retrieve, and restore through electronic devices into perceptible surrogates of the original works.

B. Bitmap Images

BMP (Bitmap) format image is digital image composed of a matrix of dots. When viewed at 100%, each dot corresponds to an individual pixel on a display [13]. In a standard BMP image, each dot can be assigned a different colour. Together, these dots can be used to represent any type of rectangular picture.

BMP supports graphic files inside the Microsoft Windows Operational System. Typically, BMP files data are not compressed which results in big size files. The main advantage of this format is it simplicity and broad acceptation. While most BMP file format have a relatively large file size due to lack of any compression, many BMP file format can be considerably compressed with lossless data compression algorithms.

C. Digital Watermarking

A digital watermark is data embedded into digital intellectual property to identify where it provides copyright protection to digital intellectual property, which includes images, sound recordings, videos and etc. [3]. Digital watermarks are cannot be see through naked eye but it can serve as signals when copyrighted materials are downloaded or reproduced. There are two main types of digital watermarking which is visible watermark and invisible watermark.

A visible watermark is a visible semi-transparent text or image overlaid on the original image [4]. It allows the original image to be viewed, but it still provides copyright protection by marking the image as its owner's property. Visible watermarks are more robust against image transformation. Thus they are preferable for strong copyright protection of digital intellectual property.

An invisible watermark is an embedded image which cannot be perceived with human's eyes. Only electronic devices or specialized software can extract the hidden information to identify the copyright owner [5]. Invisible watermarks are used to mark a specialized digital content, for example text, images, audio to prove its authenticity [6].

D. Watermarking Techniques

Watermarking can be used for solving many objectives like tamper detection, data authentication, security, copyright protection. Watermarking is done by using some particular, strong and appropriate algorithms which plays an important role in watermarking [7]. This is because if the technique which is used in watermarking process is strong, efficient and effective, then the embedded watermark cannot be easily extracted. These algorithms can be categorized into two domains which are frequency domain and spatial domain.

In frequency domain, the watermark is embedded in the spectral coefficient of the image. The generally used algorithms in frequency domain are Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT). The watermarking in frequency domain is widely applied because spectral coefficients can capture characteristics of the Human Visual System (HVS) more efficiently [9]. In this study, DWT is applied as the technique is widely used in digital signal processing, image compression, watermarking and etc. This technique uses wavelet filters to transform the image and the transforms are based on small waves which called wavelet that varies frequency and limited duration [8].

Spatial domain manipulates an image representing an object in space to enhance the image for a given application [9]. Spatial domain digital watermarking algorithms directly load the raw data into the original image. It can also be applied using colour separation. The algorithm was based on direct embedding of watermark into the image pixels. Least Significant Bit (LSB) is the technique under spatial domain that is applied in this study. In this technique watermark is embedded into the LSB of pixels. This method is easy to implement but it is not very robust against attack which means the watermark may be destroyed. The watermarking is done by choosing a subset of image pixels and substituting the LSB of each of the chosen pixels with watermark bits [10].

III. SYSTEM DEVELOPMENT

This study involves five phases of development, namely: (1) planning, (2) analysis, (3) design, (4) implementation, and (5) system testing (see Table 1).

MATLAB programming language is chosen to develop the proposed system that comprises two main modules that are: (1) watermark insert module and (2) watermark extract module. The first module involves selection of two cover images for the watermarking process while the latter involves watermark extraction where users need to insert the received watermarked image and subsequently obtained the 2 watermark image (see Figure 1). The image used in this study is in `.bmp` format.

TABLE I
PHASES OF PROJECT DEVELOPMENT

Phase	Activities	Result
Initial Phase	- Planning - Analysis	- Detailed Proposal - Gantt Chart - Analyzed Existing System - Analyzed Project Background
Phase I	- Analysis I - Design I - Implementation I - System Version I	- User Interface - Coding - UML Diagram - Implement System - System Testing
Phase II	- Analysis II - Design II - Implementation I - System Version II	- Better User Interface - Modified Coding - Implement System - System Testing
Phase III	- Analysis III - Design III - Implementation III - Final Version	- Upgraded Interface - Bugless Coding - Implement System - Complete Version of System

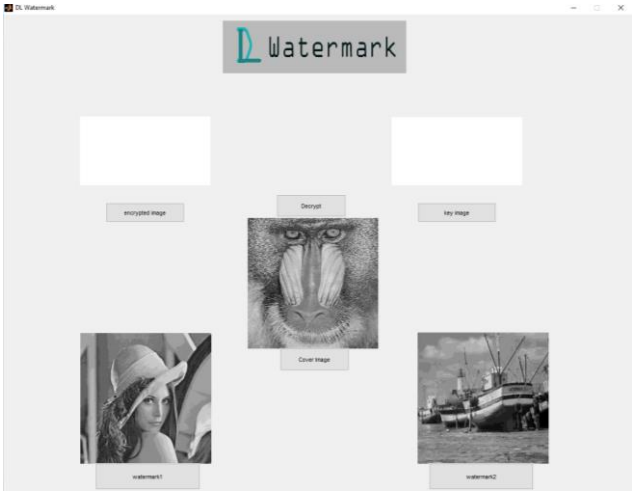

Fig 1 Example of extract watermark screenshot

Initial phase is the earliest phase where the whole project starts. This phase contains of 2 processes which Planning process and Analysis process.

Phase I is the phase where the whole project runs for the first time with whole complete processes and outcome the first version of system. This phase contains of 4 processes which is Analysis I, Design I, Implementation I and System Version I.

Phase II is the phase where the whole project runs for the second time with whole complete processes and improves the first version of system. This phase contains of 4 processes which is Analysis II, Design II, Implementation II and System Version II.

Phase III is the phase where the whole project runs for the last time with whole complete processes and improves the second version of system. Hence, producing the final version of the system. This phase contains of 4 processes which is Analysis III, Design III, Implementation III and Final System Version.

IV. IMPLEMENTATION OF DUAL LAYER WATERMARKING TECHNIQUE

Dual layer digital image watermarking technique is separated into two steps in which the first layer uses LSB Substitution Technique and inserting watermark in the second layer uses DWT on digital image.

After the selected watermark image by users is converted and exported, the image in the MATLAB base workspace will capture the value in the global variable `im2` and `im3`. The eighth, seventh, sixth and fifth bit value at position bit in variable `im3` which is the watermark image will be returned. The value of `im2`, denotes the cover image will be returned with bit position 4th, 3rd, 2nd and 1st set to the value returned by position bit in `im3`. The process is basically substituting the LSB of the cover image by using the MSB of the watermark image. The watermarked image will then be saved. Example of source code for LSB Watermarking insert module is presented in Figure 2.

```
function LSB_Callback(hObject, eventdata,
handles)
    global im2;
    im2=evalin('base','im1');
    im3=evalin('base','im3');
    im2=bitset(im2,4,bitget(im3,8));
    im2=bitset(im2,3,bitget(im3,7));
    im2=bitset(im2,2,bitget(im3,6));
    im2=bitset(im2,1,bitget(im3,5));
    axes(handles.axes3)
    imshow(im2,[])
    imwrite(im2,'out1.bmp');
```

Fig. 2 Source Code for LSB Substitution Watermarking Insert Module

The output image of LSB Substitution Watermarking Technique will be selected and rescaled. Subsequently, the wavelet decomposition of output image of LSB Substitution Watermarking Technique is obtained (i.e. Haar Wavelets) and coefficient matrices are computed. After users select the watermark image for this watermarking technique, the image will be converted to grayscale and rescaled.

```
function DWT_Callback(hObject, eventdata,
handles)
rgbimage=imresize((imread('out1.bmp')),[512
512]);
[h_LL,h_LH,h_HL,h_HH]=dwt2(rgbimage,'haar');
dec2d = [...
        h_LL,     h_LH;     ...
        h_HL,     h_HH      ...
        ];
assignin('base','h_LL',h_LL)
assignin('base','h_HH',h_HH)
assignin('base','h_LH',h_LH)
assignin('base','h_HL',h_HL)
[f p fi]=uigetfile({'*bmp'},'Select the
image');
if isequal(f,0) || isequal(p,0)
   ;
else
    rgbimage=imread([p f])
    if size(rgbimage,3)==3
        rgbimage=rgb2gray(rgbimage);
    else
        rgbimage=rgbimage;
    end
    rgbimage= imresize(rgbimage,[512,512]);
    axes(handles.axes4)
    imshow(rgbimage)
    assignin('base','rgbimage',rgbimage)
end
[w_LL,w_LH,w_HL,w_HH]=dwt2(rgbimage,'haar');
dec2d = [...
        w_LL,     w_LH;     ...
        w_HL,     w_HH      ...
        ];
figure,imshow(uint8(dec2d));title('DWT2 of
Watermark image');
assignin('base','w_LL',w_LL)
assignin('base','w_LH',w_LH)
assignin('base','w_HL',w_HL)
assignin('base','w_HH',w_HH)
newhost_LL = h_LL + (0.05*w_LL);
rgb2=idwt2(newhost_LL,h_LH,h_HL,h_HH,'haar');
figure;imshow(uint8(rgb2));title('Watermarked
image');
imwrite(uint8(rgb2),'Watermarked.bmp');
```

Fig. 3 Source Code for DWT Watermarking Insert Module

Wavelet decomposition of watermark image is obtained and coefficient matrices are computed. These wavelets obtained are also Haar Wavelets. A new matrix is formed by multiplication and addition between the matrix of watermark image and output image from LSB Substitution Watermarking Technique. Wavelet reconstruction will then be done by using the new matrix that based on Haar Wavelets. Example of source code for DWT Watermarking insert module is presented in Figure 3.

In system testing phase, functional and non-functional testing of proposed system is carried out. Functional testing is a software testing process that checks software to ensure that it has all the required functionality that is specified within its functional requirements. This is to ensure the functions work properly by adding the input and examine the output. Functional testing for this system is divided into two according to the module which is Dual Watermarking Insert Module and Dual Watermarking Extract Module. Table 2 shows the functional testing for both Watermarking insert and extract module.

Non-functional testing is the testing of a software application or system for its non-functional requirements. Non-functional testing is concerned with the non-functional requirements and is designed specifically to evaluate the readiness of a system according to the various criteria which are not covered by functional testing. Non-functional testing for this system is divided into two according to the module which is Encryption Module and Decryption Module. Table 3 shows the non-functional testing for both encryption and decryption module.

TABLE 2
FUNCTIONAL TESTING FOR WATERMARKING INSERT AND EXTRACT MODULE

No.	**Test Cases**	**Expected Output**	**Actual Output**
1	User click "Start LSB Watermarking" button to watermark cover image using LSB Substitution Watermarking Technique.	Cover image is watermarked using the technique stated.	As Expected
2	User click "Insert Image and Start DWT Watermarking" button to watermark cover image using DWT Watermarking Technique.	Cover image is watermarked using the technique stated.	As Expected
3	User does not input watermark images.	Watermarking process does not proceed.	As Expected
4	User skip LSB Substitution Watermarking Technique and proceed to DWT Watermarking Technique.	Warning message is displayed.	As Expected.
5	User attempt to cancel before input watermark image.	Reminder message is displayed.	As Expected.
6	User click "Watermark 2" to obtain watermark image embedded using LSB Substitution Watermarking Technique.	Watermark image is extracted.	As Expected
7	User click "Watermark 1" to obtain watermark image embedded using DWT Watermarking Technique.	Watermark image is extracted.	As Expected
8	User does not input cover images.	Watermarking process does not proceed.	As Expected
9	User skip watermark extraction that uses DWT Watermarking Technique and proceed to watermark extraction that uses LSB Substitution Watermarking Technique.	Warning message is displayed.	As Expected.
10	User attempt to cancel before input cover image.	Reminder message is displayed.	As Expected.

TABLE 3
NON-FUNCTIONAL TESTING FOR ENCRYPTION AND DECRYPTION MODULE

No.	Test Cases	Expected Output	Actual Output
1	User click "Encrypt" to encrypt the cover image using the key image selected.	Cover image is encrypted.	As Expected
2	Encrypted image obtainable.	Encrypted image is obtained.	As Expected
1	User click "Decrypt" to decrypt the cover image using the key image selected.	Cover image is decrypted.	As Expected
2	Decrypted image obtainable.	Decrypted image is obtained.	As Expected

Acceptance testing is provided and carried out with 35 students in UTHM. These student are required to give feedback on two user acceptance test which is the system functionality test and user friendly test. Figure 4 shows the feedback of students towards the system functionally tests.

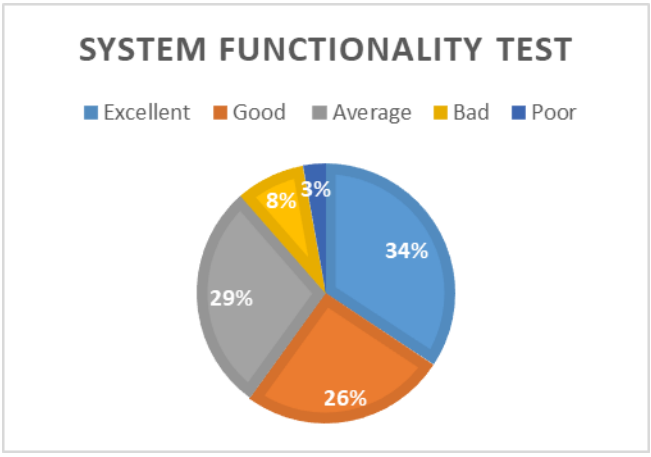

Fig. 4 System Functionality Test

34% of students think that this system function excellently and able to reach their expectation. Only 3% of students are dissapointed with the system as they are unable to retrieve their watermark image. Watermark image can only be retrieve when user input BMP format image. There are 29% of students feel that the system is just average compared to other system.

V. CONCLUSIONS

By providing two different watermarking techniques in embedding the into a cover image, this study is therefore has achieved its objective. It further suggests that the system is able to provide authentication and copyright protection to the owner of the digital image by allowing user to embed their signature which can prove their ownership. The developed system is however, only supports BMP format of and grey scale digital images. It would be promising for future works to support more variety of digital images format (e.g. JPEG and PNG) and colour images.

ACKNOWLEDGMENT

The authors express appreciation to the Universiti Tun Hussein Onn Malaysia (UTHM). This research is supported by Gates IT Solution Sdn. Bhd. under its publication scheme. Thanks to anonymous reviewer for valuable comments.

REFERENCES

[1] Calhoon, S., Rodriguez, T. F., & Conwell, W. Y.: U.S. Patent Application No. 15/063,381. (2016)
[2] Artist Sues The A.P. Over Obama Image, http://www.nytimes.com/2009/02/10/arts/design/10fair.html
[3] Nyeem, H., Boles, W., & Boyd, C.: Digital image watermarking: its formal model, fundamental properties and possible attacks. EURASIP Journal on Advances in Signal Processing, (1), 135 (2014)
[4] Bhatt, S., Ray, A., & Ghosh, A.: Image steganography and visible watermarking using LSB extraction technique. In: 9th IEEE International Conference on Intelligent Systems and Control (ISCO), pp. 1—6 (2015)
[5] Agarwal, H., Raman, B., & Venkat, I.: Blind reliable invisible watermarking method in wavelet domain for face image watermark. Multimedia Tools and Applications, 74, 6897--6935 (2015)
[6] Dhiman, S., & Singh, O.: Analysis of Visible and Invisible Image Watermarking: A Review. International Journal of Computer Applications, 147, (2016)
[7] Gupta, V., & Barve, M. A.: A review on image watermarking and its techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 4, 92--97 (2014)
[8] Ali, M., Ahn, C. W., & Pant, M.: A robust image watermarking technique using SVD and differential evolution in DCT domain. Optik-International Journal for Light and Electron Optics, 125, 428--434 (2014)
[9] Ram, B.: Digital image watermarking technique using discrete wavelet transform and discrete cosine transform. Int. J. of Advancements in Research & technology, 2, 19--27 (2013)
[10] Parashar, P. & Singh, R.K.: A survey: digital image watermarking techniques. Int. J. Signal Process. Image Process. Pattern Recognit, 7, 111--124 (2014)
[11] Kaur, G., & Kaur, K.: Image Watermarking Using LSB (Least Significant Bit). International Journal of Advanced Research in Computer Science and Software Engineering, 3, (2013).
[12] Amiri, D. M. (2011). Digital Image Proceessing, 5.
[13] Burger, W., & Burge, M. J. (2016). Digital image processing: an algorithmic introduction using Java. Springer.