WATERMARKING AND ANALYSING DIGITAL IMAGE APPLICATION.

Norhaiza Ya Abdullah
Universiti Kuala Lumpur
UniKL MIIT, Jalan Sultan Ismail
Kuala Lumpur, Malaysia
norhaizaya@unikl.edu.my

Herny Ramadhani Mohd Husny
Universiti Kuala Lumpur
UniKL MIIT, Jalan Sultan Ismail,
Kuala Lumpur, Malaysia
herny@unikl.edu.my

Siti Wan Mazidah Binti Wan Hassan
Universiti Kuala Lumpur
UniKL MIIT, Jalan Sultan Ismail,
Kuala Lumpur, Malaysia
wmazidah69@gmail.com

Wan Hazimah Wan Ismail
Universiti Kuala Lumpur
UniKL MIIT, Jalan Sultan Ismail,
Kuala Lumpur, Malaysia
wanhazimah@unikl.edu.my

Abstract— Uploading and sharing pictures on Internet seems to be common things to do nowadays and these pictures eventually will be downloaded back or repeatedly sharing among the user making the pictures less secure and easier to be manipulated for other purpose. One of the ways to protect these pictures is by using watermark. Watermark is capable of carrying information as authentication or authorization codes, or a legend essential for image interpretation. The capability is envisaged to find application in image tagging, copyright enforcement, counterfeit protection and controlled access. Nevertheless, by embedding the watermark itself is not going to strengthen the security, thus the ability to analyse the modified pictures are well demanded. By analysing the pictures, it can verify the content and detect the differences between two images or in other context; which are original digital image and modified digital image. Therefore, a system is proposed to combine both watermark and analysing ability features in one system to enhance security to the pictures. We conducted analysis on digital image from various format of image's metadata. It is hope that the proposed combination methods can be one of the method to ensure digital image is more secure and reliable.

Keywords— Digital Image, Watermark, Image Analyse, Metadata

I. INTRODUCTION

Watermarking is a technique by embedding a secret imperceptible signal, a watermark, into the original data in such a way that it is always remains present [2]. In watermarking a media is embedded with data for the purpose of authentication and protection. Watermarking techniques are divided into two categories; which are Spatial-domain technique and Frequency-domain technique. Spatial-domain technique works by slightly modifies the pixels of one or two randomly selected fraction subsets of image. Modifications might include flipping the lower order bit of each pixel. The inserted information may be easily detected using computer analysis. Frequency-domain technique or sometimes called transform domain works by altering the values of certain frequency rather than making it appear in original frequency. These frequency alternations are done in the mid-frequency components [12].

There are four different approaches to analyse images according to [5] which are is Observation, Basic Image Enhancement, Image Format Analysis and Advance Image Analysis. Observation and Basic Image Enhancement are simple method and not a good choice for making tools analysis. In other hands, Image Format Analysis and Advance Image Analysis are good choice because of its advance and precise method.

In this paper, we present the techniques used in generate watermark and method used in analyzing digital image in one application system. In order for making a good combination of proposed system, Spatial-Domain technique and Image Format Analysis were choose based on how these two can works on pixels and affect each other to show nature abilities of each methods. The reason might be that there are so many images available at Internet without any cost, which needs to be protected.

The rest of the paper is organized as follows: In section 2, we review some literatures in digital image properties and techniques in analyzing image. Section 3 describes results of implementation of proposed system and discussion and finally section 4 summarizes the paper and future work.

II. RELATED WORKS

According to [12], since watermarking can be applied to various types of data, the imperceptibility constraint will take different forms depending on the properties of the recipient such as human sense. Furthermore, researchers [7][8] conclude from many studies and listed some ideal properties of a digital watermark which are:

- Perceptual transparency - watermark should be transparent so not as to affect the viewing experience of the image nor it should degrade the quality of picture content.
- Undetectable - watermark must be difficult to remove without degrading the host signal.
- Robustness – watermark must be difficult to remove or any attempt to destroy it by adding a noise that degrade the perceptual quality of the host data so as to render it unusable. The mark should resist to common signal processing.
- Security - this is a description of how easy it is to intentionally remove a watermark example by deleting, modifying or buying of the watermark in another illicit one.
- Data capacity - refers to the amount of information that can be stored within the watermark content.

A. Spatial-domain Technique (Algorithm).

Spatial-domain techniques [4] is a part of main categories of digital watermarking. An example of Spatial-domain technique are Least Significant Bits (LSB) and Spread Spectrum Modulation Based Technique (SSM). Generally, the watermark is inserted directly by modifying the pixel value of the host images [13]. Although Frequency-Domain technique are gaining more popularity because its complexity and robustness towards most watermark attacks. Spatial-Domain technique is flexible and suitable on handling data capacity of watermark content but still provide security and perceptual transparency when embedded into pictures. One main advantage of Spatial- Domain technique used in this proposed system is the ability to be detect easily for analyse purpose.

B. Frequency-Domain Technique.

Frequency-Domain technique [9] employs various transform, either local or global. The target of this technique is to insert the watermark in the spectral coefficient of the image. The reason alternation done on mid-frequency component is because the low frequency tends to be highly sensitive to any distortion while high-frequency component can be removed without significantly affecting the original image quality [12]. An example of widely recognize Frequency-Domain technique are Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [13].

Table 1 Comparison between Two Main Techniques

Technique (s)	*Spatial-Domain Technique*	*Frequency-Domain*
Description	*Modifies the pixels of one or two randomly selected subsets of an image.*	*Altering the values of certain frequency rather than making it appear in*
Example	*LSB and SSM*	*DCT and DWT*
Advantage	*Embedded watermark is easy to extract and suitable for a small image*	*More robust and secure than Spatial-Domain technique.*
Disadvantage	*Less robust than Frequency domain technique.*	*Not much data capacity can be embed because host image quality will be*

C. Analyze Images.

Based on [5], there are four main different approaches to analyse image. Below are the description approaches to analyse image.

- Observation – Many times forgeries or modified images can be identified through direct observation. No image analysis tools are required.
- Basic Image Enhancement – Through common algorithm such as sharpening, blurring, scaling, and re-colouring, attributes within the image can be more distinct.
- Image Format Analysis – Changes to images alter the file format. In the case of JPEGs and other lossy image formats, changes to image can be detected.
- Advance Image Analysis – Signal analysis can be detecting manipulation. Approaches range from error level analysis to Principle Component Analysis (PCA) and wavelet transformations.

D. Image Format Analysis.

Images can be stored [6] in a variety of format such as RAW that contain only pixel data while JPEG, GIF, PNG or TIFF can be as informative as the image. Changes to the image yield changes to the file format. For example, JPEG files contain a well-define feature set thus changes to the image will modify the feature set. The feature set for JPEG includes metadata, quantization table for image compression, lossy data compression and subdivided image processing using 8 x 8 pixel cells [5]:

i. Metadata analysis – Most pictures include a significant amount of metadata [11] that describe the source of the image. For example, a JPEG from a digital camera usually includes the camera type, resolution, focus settings, and other features.
ii. Quantization fingerprinting – known as ballistics, it's provides a method to detect images that do not match the specific metadata. The JPEG algorithm uses a set

of quantization matrices to control image compression and quality. The format type image like JPEG algorithm uses a set of quantization matrices to control image compression and quality. Images can be converted from RGB to YCrCb. One quantization matrix handled the luminance (Y) and a second matrix handled the chrominance for both red (Cr) and blue (Cb) [5].

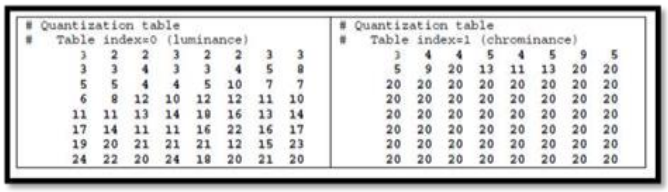

Figure 1 Example of Quantization Table Fingerprinting (source: Dr. Neal Krawetz, "A Picture's Worth...",)

Each quantization table contain 64 bytes. The first byte is the DC and acts as a scalar value. The remaining 63 bytes are the AC and define compression by frequency. The algorithm developed by [4] Hacker Factor Solution for approximating the quality of an image format

iii. Quality detection - When saving an image, most tools allow the selection of the image quality. In general, lower quality results in a smaller image. Although a known quantization table allows the identification of the tools as well as the quality, the quantization table may not always match a known application or camera. In this situation, the quality of the image must be approximated [10].

III. RESULTS AND DISCUSSION

In the proposed system, there two option which is to generate watermark and analyse image. First watermarked is added in the original image then the same image we analyze to compare the difference between the original and the watermarked image. The source image is shown in Figure 2 and Figure 3 shows the watermarked image and the difference between the original and the watermarked image. It also shows the analysis part of both images.

Figure 2 Watermark have been added to into the original image .

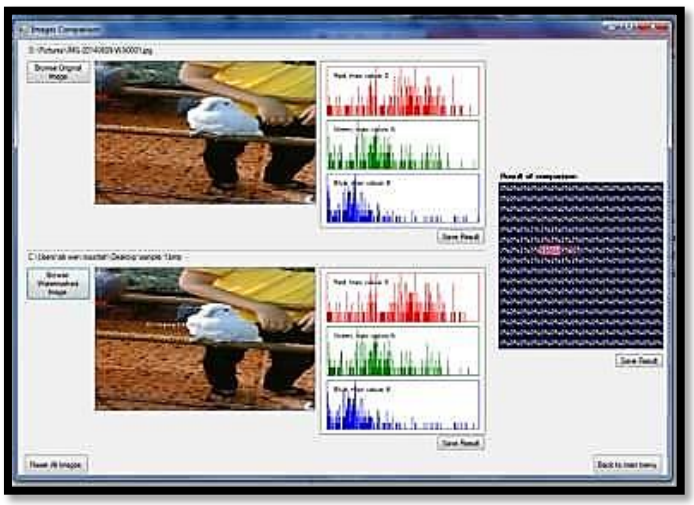

Figure 3 Comparison and Analysis of Both Images

User Acceptance Testing (UAT) have been done to ensure the system is usable to the user. There are three features that have been tested: 1) Usability and user-friendly, 2) Functionality and 3) Security. The testing has been conducted by a group of user (31 persons) from different background study.

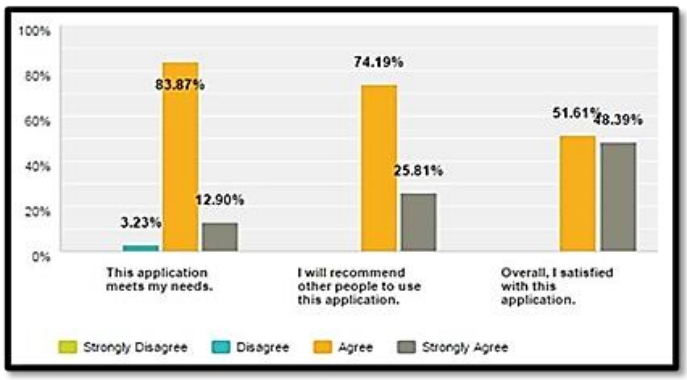

Figure 4 Chart of Usability

Based on Figure 4 above, it is proven that the proposed system is useful for the potential client who will use this application system.

Those respondents said that this Digital Image Watermark Analyse System is useful in order to protect pictures by embedding the watermark before upload it on Internet. Some of the respondents feel this application system is very useful for them and will recommend it to other peoples. Moreover, respondents claimed that this system is easy to use for the potential client who will use this application system. Furthermore, those respondents are satisfied with Digital Image Watermark Analyse System but still have room for improvement and future enhancement.

IV. CONCLUSION.

In this paper, we have presented the techniques used in generating watermark and analysis of digital image watermarking using Spatial-Domain technique and Image Format Analysis. The performance of the algorithm is analyzed in this work. Moreover, the testing of the proposed system shows the combination of both watermark and analysing ability features in one system, able to enhance security to the digital image.

The technique is useful in a way such that user can ensure the authenticity of the image. With the increase of the application of digital media communication through Internet it has now become more difficult to secure the authenticity of communicated media. Thus, involvement of the watermarking system, like the one presented in this paper, hope can be helpful to setup a secure data communication. Watermarking [1] can also be used to store the data to avoid its use by malicious users. Moreover, there are some future enhancement needs to take action for improvement of Digital Image Watermark Analyse System which as the following:

i. Create more attractive Graphical User Interface (GUI) to make the system more interactive and understandable to help the unexperienced user easy to use.

ii. Add another helpful features like such as zoom in/out and add another metadata information of other format digital image.

V. REFERENCE

[1] Ankita..P & Poonam, " Image Data Authentication using Watermarking Scheme by DWT based Data Embedding Approach" Intyernational Journal of Advanced Research in Elecrical , Electronics and Instrumentation Engineering" Vol 4, Issue 12 December 2015.

[2] I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[3] Bender, W., Gruhl, D., Morimoto, N., & Lu, A. "Techniques for data hiding." IBM systems journal (1996)., 35(3.4), 313-336.

[4] Digimarc. (n.d.), from http://www.digimarc.com/digimarc-for-images

[5] Dittmann, J., Steinebach, M., Wohlmacher, P., & Ackermann, R. " Digital watermarks enabling e-commerce strategies: conditional and user specific access to services and resources". EURASIP Journal on Applied Signal Processing, 2002(1), 174-184.

[6] Dr. Neal Krawetz, "A Picture's Worth...", Black Hat conference, Caesars Palace" - Las Vegas, retrieved 08/01/07 2007, http://blackhat.com/html/bh-usa-07/bh-usa-07- speakers.html#Krawetz

[7] Gaurav, J., & T. Srinivas, C. (n.d.). "Digital image watermarking: An overview". Retrieved from http://web.iiit.ac.in/~gaurav/watermark.pdf

[8] Kim, H. J., Xiang, S., Yeo, I. K., & Maitra, S. "Robustness Analysis of Patchwork Watermarking Schemes. Digital Audio Watermarking Techniques and Technologies: Applications and Benchmarks." . (2008).

[9] Meerwald, P.. "Digital watermark detection in visual media content." Retrieved from www.wavelab.at/papers/Meerwald10d.pdf (2010)

[10] Mustafa Osman Ali, Elamir Abu Abaida Ali Osman and Rameshwar Row, "Invisible Digital Image Watermarking in Spatial Domain with Random Localization", International Journal of Engineering and Innovative Technology, November 2012,Volume-2 Issue-5, pp. 227-231,.

[11] Mriganka, G., Koushik, M., H.M.Khalid, R. B., Dibya, J. D., & Ankita, D. " Image and video based double watermark extraction spread spectrum watermarking in low variance region". International Journal of Advanced Computer Science and Applications (IJACSA), (2013)4(6), doi: 10.14569/IJACSA.2013.040615.

[12] Nixon, A. "Watermarks: An in-depth discussion". SANS Institute InfoSec Reading Room, (2012).Retrieved from https://www.sans.org/reading-

room/whitepapers/detection/watermarks-prevent-leaks-34087

[13] Qureshi, M. A., & Tao, R. "A comprehensive analysis of digital watermarking." Information Technology Journal, 5(3) (2006)., 471-475.

[14] Shantikumar, S., B. Pushpa, D., & Kh. Manglem , S. "A review of different techniques on digital image watermarking scheme."(2013). International Journal of Engineering Research, 2(3), 193-199.