UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

A Grid-based Invisible Watermarking for .Jpeg Images Using Least Significant Bit

Kushalinni Nair Radakrishnan & Hazinah Kutty Mammi
School of Computing, Faculty of Engineering
Universiti Teknologi Malaysia
81310 UTM Johor Bahru, Johor, Malaysia
kushalinninair173@gmail.com

Submitted: 15/07/2019. Revised edition: 16/03/2020. Accepted: 17/03/2020. Published online: 20/05/2020
DOI: https://doi.org/10.11113/ijic.v10n1.235

***Abstract*—Internet is a one stop centre for users to download any media file such as image, audio and even videos. It is an excellent distribution system for digital media as it is inexpensive, eliminates warehousing and stock and user-friendly. However, there is an issue where user may copy or share the data illegally which eventually can increase the risk of privacy level of the media. Digital watermarking is introduced in order to solve the issue where it can provide copyright protection of the media and also to provide ownership that can be used to protect data from piracy. An efficient scheme of invisible watermarking is that it has to be able to overcome attacks on social media such in a way where when people download and crop any image from social media, the owner of the image can proof that the image is rightfully his. The loss of synchronization caused by geometrical modifications of an image, such as cropping, increases the difficulty of watermark detection, especially for invisible watermarking schemes. In this research, the Spatial Domain technique based algorithms were considered and two experiments were conducted in where one is text-based watermark embedding and another is image-based watermark embedding, The text-based watermarking method preserved the watermark after being uploaded and download to social media but decreases in terms of size of image. For the case of image-based watermark, the watermark was preserved for images with minimal colours or solid colours. It has also survived the watermark originality once being uploaded to social media.**

***Keywords*—Digital Watermarking, Cropping, Invisible Watermarking, Social media, Image-based, Text-Based**

I. INTRODUCTION

Currently, creating and embedding watermarks in an image faces many limitations and constraints, particularly reduced robustness against threats and reduced capacity to hide a large volume of watermark due to the originality of the image content. There have been numerous researches on this subject where researchers have proposed algorithms to hide large amount of watermark data in an image. image. Unfortunately, these algorithms only apply to certain languages, only achieve small hiding bit data capacity and are not strong enough to survive attacks. Thus, increasing the capacity for watermark hiding and prevent copyright and ownership attacks are the main goals of watermarking applications for storing the copyrighted data of the images. There have been previous researches to embed watermarks but only for text images in where there is very much reduced robustness in the algorithms now as it is prone to many attacks (Al-Maveri, 2016).

The main issue here is how do people get the images, were those images captured by themselves or downloaded illegally by just cropping out the little identity of the watermark present in the image. All data are digitalized in these days which provides easy access for intruders to plagiarize on an image and claim it is theirs.

II. LITERATURE REVIEW

A. *Image Types*

An image, digital image, or still image is a binary representation of visual information such as drawings, pictures, graphs, logos, or individual video frames. Digital images can be saved electronically on any storage device. In social media, people tend to upload all kind of images ranging from enormous sized to small sized pictures. It doesn't seem to matter whether a picture is uploaded as .PNG or .JPEG format, the upload drastically reduces the size of the image, thus reducing the quality of the image. The loss of quality is especially noticeable with text portions of an image. JPEG is generally used for images with blended tones, like photos, and GIF and PNG are better for images of flat tones, like logos, text, and graphics. Table 1.1 below shows the varieties of image format and widely used in various fields.

TABLE 1.1. Types and Comparison of Image Format

Type	Characteristics	Used in
TIFF, file types ending in .tif	Large files that contains many detailed images.	Photo software (Photoshop)
JPEG (also known as JPG), file types ending in .jpg	Compressed images that is stored in small file.	Photographs on the web
GIF, file types ending in .gif	Lossless compression.	Used for animations.
PNG, file types ending in .png	Open format replacing GIF.	Used almost exclusively for web images.
Raw image files	Unprocessed raw files where the data is from a digital camera.	Used for further editing.

B. Invisible Watermarking

Invisible watermarking is useful for secret communication and copyrights. A secret data hiding in a medium so that no one will guess its existence into this medium is called invisible watermarking. The research issues of invisible watermarking system are increasing the imperceptibility and robustness. There are many techniques proposed by researchers for increasing the strength of watermarking system. In order to sustain antipiracy technologies, firm anti-piracy legal laws are needed for support of all these applications because no extra system and mechanism is incorporated in these devices when a person can be caught making illegal use of it. The conscious concealment of data within another image is called image watermarking. Another way is to store and transmitting data in a form in order to make it secure from unintended recipients or use is called cryptography, but cryptography does not hide the doubt of secret hiding. Invisible watermarking approach is classified into spatial domain watermarking and frequency domain watermarking. Frequency domain watermarking shows better robustness than spatial domain watermarking. Makbol Nasrin *et al.,* (2012) has suggested block level DWT image watermarking system and analyzed the performance of robustness. In a digital image, information is imbedded into noisy area of image for hiding secret watermark in less perceptible parts of image and for this varying block level image watermarking scheme is suggested and analyzed. Visible watermarking provides security by overlaying images or text in front of the image. This has reduced robustness towards attacks and has triggered to the formation of invisible watermarking.

C. Spatial Domain

Least Significant Bit (LSB) under the working domain of Spatial Domain is the method that will be used in this research. It is the unsophisticated technique that implements steganography. As per the usual steganographic method, it embeds any data such as file or image and text into the cover so it cannot be detected by any naked eye. This method works in a way by substituting of information in a certain pixel with information from the data to be embedded. On the other hand, where it is feasible to embed data into any bit-plane of an image, LSB is all about embedding it into the least significant bit. This limits the variation in colors that the embedding makes. For instance, inserting into the least significant bit changes the color rate by 1. Second bit plane of embedding would then change the color rate or value into 2.

D. Grid Lines

(Kutter, 1999) proposed a method to achieve self-registration for watermark detection. In his scheme, a pattern is embedded at shifted locations in the image such that generalized geometrical transformation can be reflected by applying autocorrelation to the investigated image. Four patterns consisting of pseudo-random numbers are embedded in the image. The four patterns are not totally different but linearly shifted copies of each other. The initial pattern is a two-dimensional random number array. The second pattern is then formed by horizontally shifting the first pattern by six columns. Similarly, the third pattern is formed by vertically shifting the first pattern by. Finally, the fourth pattern is formed by shifting the first pattern by five horizontally and vertically. The four patterns are embedded in an interleaved way.

III. METHODOLOGY

There are four phases that must be completed, and the phases would have to obey the restrictions of the objectives:

A. Phase 1:Review and Study on Technique

In doing this research, a study on the related field was conducted and from that findings, there are three domains for this research according to the research objectives, which includes watermarking, splitting image, and social media. Thus, a study on the type of watermarks, several types of watermarking techniques, different formats of images must be done. In watermarking itself there are two methods, visible and invisible but in this research, it is more focused on invisible watermarking. Next, for the scope of grid lines, studies were done on knowing methods to divide the watermark accordingly. A literature review of books, articles and journals together with review on existing algorithms that uses spatial domain technique is required. The aim of reviewing the literature is to find more information about image watermarking. Furthermore, the robustness of the technique based on LSB against image attacks is identified.

Besides, the existing techniques based on LSB is compared to know which technique gives better robustness against image.

B. Phase 2: Design,Develop and Design Experiment

In this phase, after detailed study on the above domains, the watermarking techniques have been decided. The chosen working domain is Spatial Domain technique in which LSB is in. The algorithm would be created and modified from previous research and from the present techniques that have been studied. In performing the watermarking process, the inputs required are a cover image, text watermark and image watermark. Watermark embedding process is performed on the cover image to hide the watermark. Then the extraction or decoding process is done to show whether or not the watermark still exists.

C. Phase 3: Data Collection and Analysis

This research is mainly focused on Joint Photographic Expert Group (JPEG) types of images because most of the social media uses this format of image. Thirty images are planned to be experimented and at the end of the experiment, the quality of the image and the originality of the watermark would be tested. Also, in this phase, analysis of detection of the watermarked images must be done. The detection works in a way where to check is the watermark still embedded on the image and quality of the watermarked image would be the parameters on testing the image. All the images that has been watermarked has to be downloaded and cropped of a particular section and be uploaded to social media and then downloaded back to see if there is any changes in the watermark.

IV. RESEARCH DESIGN AND IMPLEMENTATION

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

A. Proposed Solution

As mentioned in previous chapters, the solution to the problem that has been discussed is embedding watermarks of text and image form and testing whether the watermark is still present or not. The purpose of the method proposed in this experiment is to test on the parameters that have been set for this study.

After a successful watermarking process, the watermarked image must be uploaded into four different kind of social media, including Facebook, WhatsApp and also Gmail. It is required in order to answer the research aim. It is a success if the embedded watermark is not been detected and altered by social media uploading process.

There are two experiments, Experiment A, Text-based Watermarking, shown in Fig. 1.2 and Experiment B, Image-based Watermarking, shown in Fig. 1.3. Fig. 1.1 below shows the design of the experiment.

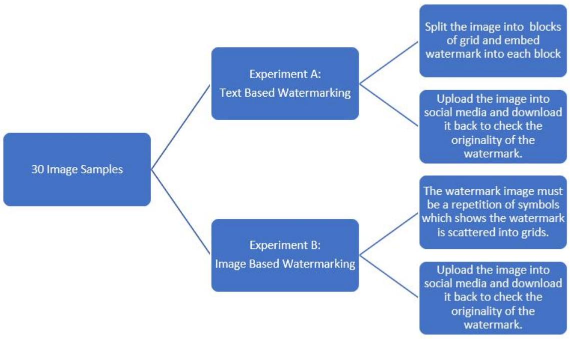

30 Image Samples
Experiment A: Text Based Watermarking
Split the image into blocks of grid and embed watermark into each block
Upload the image into social media and download it back to check the originality of the watermark.
Experiment B: Image Based Watermarking
The watermark image must be a repetition of symbols which shows the watermark is scattered into grids.
Upload the image into social media and download it back to check the originality of the watermark.

Fig. 1.1. Design of the experiment

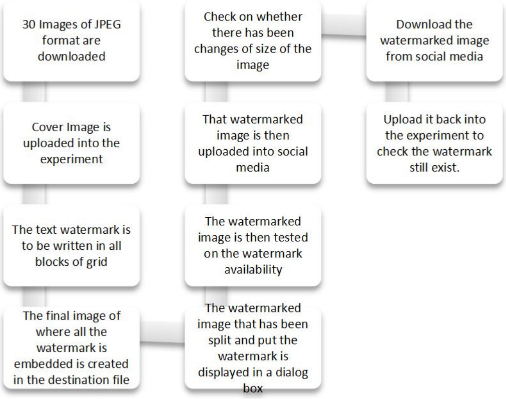

30 Images of JPEG format are downloaded
Cover Image is uploaded into the experiment
The text watermark is to be written in all blocks of grid
The final image of where all the watermark is embedded is created in the destination file
The watermarked image that has been split and put the watermark is displayed in a dialog box
The watermarked image is then tested on the watermark availability
That watermarked image is then uploaded into social media
Check on whether there has been changes of size of the image
Download the watermarked image from social media
Upload it back into the experiment to check the watermark still exist.

Fig. 1.2. Experiment A (Text-based Watermarking)

The steps below explains the figure.

(a) Cover Image is uploaded into the experiment.
The image which was downloaded earlier is uploaded to the experiment named as host image. Host image is the image before it is being watermarked.

(b) The text watermark is to be embedded in all blocks of grid.
This part of the experiment is where the user is prompted to enter the text-based watermark to be embedded on the image. There are nine blank boxes where the user has to fill each and one of it Each box indicates one-part block of the image.

(c) The final image of where all the watermark is embedded is created in the destination file.
The image that has been watermarked is saved in the destination file of the user. The image is saved as final_out.jpg.

(d) The watermarked image that has been split and put the watermark is displayed in a dialog box.
To show the user that the image has been watermarked in each block that has been split, a dialog box is featured

for user to view the image which has been split and watermarked.

(e) The watermarked image is then tested on the watermark availability.

All watermarked media must be checked on the watermark availability before running any process to it. This is to prove that the watermark has been successfully embedded to the image and if the watermark is gone after a certain process, it should be the algorithm of the process which does not allow the watermark to survive.

(f) The watermarked image is uploaded into social media

In order to check whether the image can survive any process done by social media, the image saved as final_out.jpg is uploaded to three different mediums of social media.

(g) Check on whether there has been changes of size of the image.

The size of the image is then compared to check whether there have been any changes to the original image and after being watermarked.

(h) Download the watermarked image from social media.

The image which was uploaded to the social media is then downloaded back to check whether the originality of watermark still exist or not.

(i) Upload it back into the experiment to check the watermark still exist.

The image that has been downloaded from social media has to be once again uploaded into the experiment to check on the availability of the watermark.

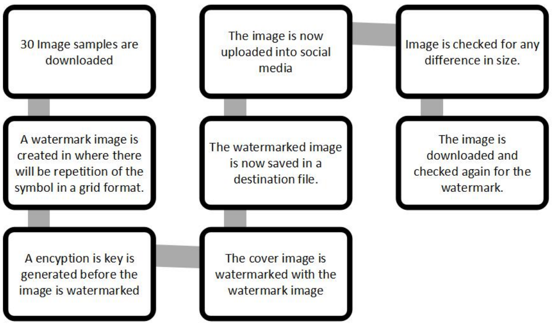

30 Image samples are downloaded
A watermark image is created in where there will be repetition of the symbol in a grid format.
A encyption is key is generated before the image is watermarked
The cover image is watermarked with the watermark image
The watermarked image is now saved in a destination file.
The image is now uploaded into social media
Image is checked for any difference in size.
The image is downloaded and checked again for the watermark.

Fig. 1.3. Experiment B (Image-based Watermark)

The steps below explains the figure:

(a) A watermark image is created in grid format.

An image is created where there is grid embedded to it and the watermark would be a symbol which is repeated in each grid block. The image is created using Canva and downloaded using the JPEG format because the experiment only accepts images in JPEG format.

(b) An encryption key is generated before the image is watermarked.

An AES generated encryption key is generated once the cover image and image to be watermarked is chosen. The watermark image is now embedded into the cover image.The key is used as authentication when the image is to be uploaded and downloaded to check the watermarkavailability.

(c) The cover image is watermarked with the watermark image.

The image is watermarked when the user has already generated the encryption key. This process take a while before the watermarked image pops up.

(d) The watermarked image is saved in destination file.

The image that has been watermarked is now saved in a destination file as per user's preference.

(e) The downloaded image is uploaded to social media.

As per Experiment A, this experiment also requires the image to be uploaded to social media to be checked on their survival of the watermark.

(f) The image is checked for any difference in size.

The image that has been watermarked is compared with original size and also after being uploaded and downloaded to social media.

(g) The downloaded image is checked again for watermark.

The image that has been uploaded to social media is then downloaded again to check the survival of the watermark.

B. *Parameters and Testing Method*

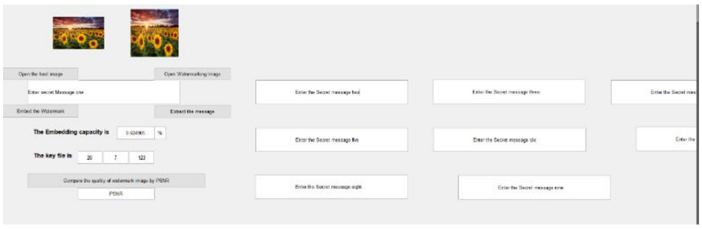
For Experiment A, Text-based watermark (refer Fig. 1.4) all the cover images are tested with the same text to be exact of the test result. The same goes for Experiment B, Image-based Watermark (refer Fig. 1.5) in where the same size and design image is used to be embedded in the 30 cover images.

1) Size of the Image After Watermarked

The image is tested to be whether in the same size or not after being embedded with the watermark. The JPEG images would be tested by checking the properties of the image. The size is also checked again after being uploaded and downloaded to social media.

2) Readability of the Watermark

The image is tested again in the experiment on whether the watermark is still present or not after being downloaded from the social media. The image is also to be cropped of a certain part to check the availability of the watermark.



Open the host image
Open Watermarking image
Enter secret Massage one
Enter the Secret message two
Enter the Secret message three
Enter the Secret mes
Embed the Watermark
Extract the message
Enter the Secret message five
Enter the Secret message six
Enter the
Compare the quality of watermark image by PSNR
PSNR
Enter the Secret message eight
Enter the Secret message nine

The Embedding capacity is 0.624905 %

The key file is 26 7 123

Fig. 1.4. Experiment A (Text-based watermark)

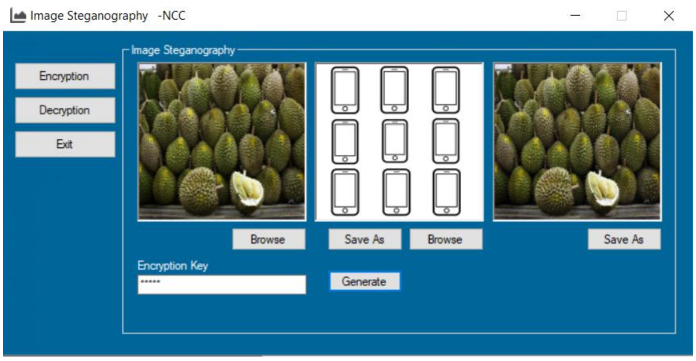


Image Steganography -NCC

Encryption Key *****

Fig. 1.5. Experiment B (Image-based Watermark)

V. RESEARCH ANALYSIS AND DISCUSSION

1) *Text Based Watermarking*

There has been significant change in the size of the image when it is watermarked.As can be seen in Table 1.2, the original size of the images, and the watermarked size of the image in where it means that the size of the image after being watermarked has decreased significantly.

TABLE 1.2. Text-based Watermark Image Analysis

Image Texts	Original Image Size	Watermarked Image Size	Difference		
			Comparison	Size Difference	
				Kilobytes	Percentage
1	32.5 KB	2 KB	Smaller	30.5	93.84%
2	189 KB	9.66 KB	Smaller	179.34	94.89%
3	148 KB	21.3 KB	Smaller	126.7	85.60%
4	211 KB	5.89 KB	Smaller	205.11	97.21%
5	961 KB	6.55 KB	Smaller	954.45	99.3%
6	95.4 KB	9.10 KB	Smaller	86.3	90.46%
7	7.62 MB	14.7 KB	Smaller	7.08	99.8%
8	692 KB	8.51 KB	Smaller	683.49	98.77%
9	1.11 MB	15.4 KB	Smaller	1121.24	98.7%
10	1.76 MB	12.5 KB	Smaller	1789.74	93.1%
11	459 KB	10.1 KB	Smaller	448.9	97.80%
12	80.2 KB	14.0 KB	Smaller	66.2	82.54%
13	945 KB	6.39 KB	Smaller	938.61	99.32%
14	177 KB	11.8 KB	Smaller	165.2	93.33%
15	4.35 MB	20.7 KB	Smaller	4433.7	99.5%
16	882 KB	14.5 KB	Smaller	867.5	98.36%
17	138 KB	19.0 KB	Smaller	119	86.23%
18	447 KB	10.5 KB	Smaller	436.5	97.65%
19	110 KB	20.9 KB	Smaller	89.1	81%
20	808 KB	17.1 KB	Smaller	790.9	97.88%
21	507 KB	9.89 KB	Smaller	497.11	98.05%
22	60.5 KB	7.59 KB	Smaller	52.91	87.45%
23	220 KB	8.80 KB	Smaller	211.2	96%
24	127 KB	8.92 KB	Smaller	118.08	92.98%
25	261 KB	15.7 KB	Smaller	245.3	93.99%
26	445 KB	17.0 KB	Smaller	428	96.18%
27	253 KB	6.42 KB	Smaller	246.58	97.46%
28	115 KB	14.9 KB	Smaller	100.1	87.04%
29	3.23 MB	12.6 KB	Smaller	3294.92	99.6%
30	885 KB	12.5 KB	Smaller	872.5	98.59%
			Average	**947.27**	**94.42%**

2) *Image Based Watermarking*

There has been significant rise in the size of the image after being image watermarked. The percentage of the image mostly increased beyong 100% and this has caused degradation of the quality of the image.

TABLE 1.3. Image Based Watermark Image Analysis

Image	Original Image Size	Watermarked Image Size	Difference		
			Comparison	Size Difference	
				KiloBytes	Percentage
1	32.5 KB	153 KB	Larger	120.5	370%
2	189 KB	2.02 MB	Larger	1879	994%
3	148 KB	1.50 MB	Larger	1388	937%
4	211 KB	1.59 MB	Larger	1417	671%
5	961 KB	2.58 MB	Larger	1680.9	174%
6	95.4 KB	0.78 MB	Larger	703.32	737%
7	7.62 MB	8.03 MB	Larger	8818.8	5.38%
8	692 KB	4.94 MB	Larger	4366.5	247%
9	1.11 MB	4.42 MB	Larger	3389.4	298%
10	1.76 MB	12.2 MB	Larger	10690.5	593%
11	459 KB	4.07 MB	Larger	3708.6	807%
12	80.2 KB	904 KB	Larger	823.8	1027%
13	945 KB	5.84 MB	Larger	5035.2	532%
14	177 KB	1.10 MB	Larger	949.4	536%
15	4.35 MB	15.8 MB	Larger	11724.8	263%
16	882 KB	5.92 MB	Larger	5180.1	587%
17	138 KB	1.00 MB	Larger	886	642%
18	447 KB	3.34 MB	Larger	2973.2	665%
19	110 KB	1.98 MB	Larger	1917.52	994%
20	808 KB	4.07 MB	Larger	3359.7	415%
21	507 KB	805 KB	Larger	298	58%
22	60.5 KB	458 KB	Larger	397.5	657%
23	220 KB	0.99 MB	Larger	793.76	360.8%
24	127 KB	2.30 MB	Larger	2228.2	999%
25	261 KB	2.79 MB	Larger	2595	994%
26	445 KB	3.33 MB	Larger	2694	666%
27	253 KB	263 KB	Larger	10	3.9%
28	115 KB	1.06 MB	Larger	970	843%
29	3.23 MB	10.9 MB	Larger	7854.1	237%
30	885 KB	8.61 MB	Larger	7931	896%
			Average	**3226.1**	**573.6%**

The experiments were conducted to answer the research question as per in Chapter 1. The significance of this research is to identify and study the technique based on grid lines in invisible digital watermarking whether it gives robustness against image attacks in order to achieve copyright protection. This is in line with the objectives of this research as stated in Chapter 1. The research aim is to know how much watermark can be embedded in the grid lines, but in this case of experiment, as the image is divided into blocks of grids, it shows that it can be divided into 9 blocks the smallest. How to make the grid lines is where one method is to break the image into grid blocks and another one is to embed a grid-based image as a watermark itself. The other research aim would also be to investigate whether or not the watermark would still exist in the image after being cropped out of being plagiarized for other purposes. As per the analysis, for Experiment A, Text based Watermarking, after uploading and downloading back from 3 chosen social media, only Facebook recorded changes in the quality of the image but still had watermark present after downloading back, but Whatsapp and Gmail retained the quality of the image and still has the watermark present in it after being downloaded back. As for Experiment B, Image based Watermarking for Facebook and Whatsapp respectively, the quality of the image reduced and the watermark presence varied according to the image type. Only images with less colours survived the watermark after being downloaded. Nevertheless, for Gmail, there has been no changes in the quality of the image and the watermark is still present in the image after downloaded.

As been mentioned, the compression technique used by the social media above are still unclear because only a few researches have been done on it which cannot seem to support the is research analysis. In accordance to that, future research on this topic should be done in order to know what are the modification which are being done to the image which causes the alteration of the watermark.

It can be concluded from the table above that both methods are feasible in their own ways. For text watermarking, the LSB algorithm used survived all social media modification to the image and preserved the watermark but with degradation of the size of the image. In image watermarking, the LSB algorithm used could only protect images which has minimal colors as the embedding capacity is higher, Furthermore, for those images where the watermark was present, when the cropping test was done, it was proven that the watermark still exists even after being uploaded to social media. This shows that the technique is feasible but with restriction for the type of image.

As a conclusion, the concept of ownership and proving the originality of image can be done via text watermarking but degradation on the quality of the image. As for image watermarking, the method is only feasible for media owners with minimal color.

REFERENCES

[1] Akram M. Zeki. Khedher. (2006). Digital Watermarking Implementation.

[2] Preceedings of the Postgraduate Annual Research Seminar. 2006, Faculty of Computer Science and Information System, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia, 197-198.

[3] Rui, Y., Huang, T. S., & Chang, S. F. (1999). Image Retrieval: Current Techniques, Promising Directions, and Open Issues. *Journal of Visual Communication and Image Representation,* 10(1), 39-62.

[4] Furht, B., Muharemagic, E., & Socek, D. (2006). *Multimedia Encryption and Watermarking* Springer Science & Business Media. Vol. 28.

[5] R. G. van Schyndel, A. Z. Tirkel and C. F. Osborne. (1994). A Digital Watermark. *Proceedings of 1st International Conference on Image Processing, Austin, TX.* 2, 86-90.

[6] Kaur, M. (2015). An Existential Review on Text Watermarking Techniques, 120(18), 29-32.

[7] M. S. Kankanhalli, Rajmohan and K. R. Ramakrishnan. (1999). Adaptive Visible Watermarking of Images. *Proceedings IEEE International Conference on Multimedia Computing and Systems, Florence, Italy*. 1, 568-573.

[8] F. Hartung and M. Kutter. (1999). Multimedia Watermarking Techniques. *Proceedings of the IEEE*. 87(7): 1079-1107.

[9] Makbol, N. M., & Khoo, B. E. (2013). Robust Blind Image Watermarking Scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition. *AEUE-International Journal of Electronics and Communications,* 67(2):102-112. https://doi.org/10.1016/j.aeue.2012.06.008.

[10] Sumathi, C. P., Santanam, T., & Umamaheswari, G. (2013). A Study of Various Steganographic Techniques Used for Information Hiding, 4(6), 9-25.

[11] Mandal, J. K., & Das, D. (2012). Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain, 2(4), 83–93

[12] Moghaddasi, Z., Bt, A., & Manaf, A. (2012). Secure Genetic Based Image Steganography System in Frequency Domain, 4(6), 7-11.

[13] Aslam, M., & Alkhaldi, A. H. (2015). A Novel Method of Audio Steganography using Advanced Encryption Standard, 4(3), 155-159. https://doi.org/10.1515/nleng-2015-001.

[14] Chan, C., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution, 37, 469–474. https://doi.org/10.1016/j.patcog.2003.08.00.

[15] Wang, Y., Member, S., Doherty, J. F., Member, S., & Dyck, R. E. Van. (2002). A Wavelet-based Watermarking Algorithm for Ownership Verification of Digital Images, 11(2), 77-88.

[16] G. Eason, B. Noble, and I. N. Sneddon. (1955). On Certain Integrals of Lipschitz-Hankel Type Involving Products of Bessel Functions. *Phil. Trans. Roy. Soc. London*, A247: 529-551.