International Journal of Applied and Physical Sciences
volume 4 issue 3 pp. 103-109 doi: https://dx.doi.org/10.20469/ijaps.4.50004-3

Invisible Watermarking on Grayscale Image

Mohd Shahrir Abd Rahim[*]
Department of Polytechnic Education,
Ministry of Education Malaysia,
Putrajaya, Malaysia

Nabilah Hasanah Binti Shaari
Universiti Malaysia Perlis,
Arau, Malaysia

Nur Hafizah Binti Ghazali
Universiti Malaysia Perlis,
Arau, Malaysia

Abstract: Digital watermarking is a procedure to embedded watermark or logo into an image to avoid copyright and protect the image from being manipulated by others without owner approval. In the Technical and Vocational Education and Training (TVET) sector, the main challenge in watermarking is how to achieve high imperceptibility or visual quality and robustness without sacrificing the capacity of the cover image. In addition, the watermark should be ably extracted without any distortion. As for that, spiral scan embedding technique is used to overcome this issue. The performance of the proposed project is evaluated by comparing the results of extracting process using spiral scan technique with sequence technique, while the imperceptibility of the cover image is measured using Peak Signal Ratio (PSNR) and robustness of the watermarked image is measured using Normalized Cross Correlation (NCC). The eesult shows that the proposed technique obtains high imperceptibility and robustness.

Keywords: *TVET, watermarking, Matlab, PSNR, NCC*

Received: 17 July 2018; ***Accepted:*** 18 September 2018; ***Published:*** 14 November 2018

I. INTRODUCTION

Nowadays achievement of the worldwide web and accessibility of affordable device and high tech tool make information and data stored on the internet easy to acquire and duplicate with the same quality. This lead to a major problem to the metadata such as video, music, and picture producer in these industries if there are no methods to secure the right of ownership and also avoid unapproved replicating. Something should have to be encoded in the metadata to avoid unapproved entry to metadata. But encoding also has constraints in ensuring the protected right of ownership in light of the fact that once digital data get decoded, then there is nothing to keep an unauthorized TVET client to duplicating the data. A Better innovation is clearly demanded to authorize and secure the right of ownership, also trail the data use, guarantee approved entry, encourage data verification and avoid unlawful duplication.

This problem forced a research group pulled into consideration to a production of another data embedded structure that is Digital Watermarking. Fundamental thought of digital watermarking is to create data consist of a secret message, and then shroud the data inside desired metadata. The data can be embedded into different forms, for example, binary image pattern or character string. First of all, the data is installed into its bit stream representation then after that shroud in the watermark, the arrangement of same sort and element from the cover work, the digital data that have to be secured.

Lastly, the watermark is embedded into the cover work where it ought to be imperceptible. The watermark ought to be high in robustness to hold not only distortions

[*]Correspondence concerning this article should be addressed to Mohd Shahrir Abd Rahim, Department of Polytechnic Education, Ministry of Education Malaysia, Putrajaya, Malaysia. E-mail: shahrir@mohe.gov.my

brought on by spiteful assault but also most of the normal flag distortions.

II. LITERATURE REVIEW

This chapter discusses a survey of watermarking technique distinguishing the proprietor of an image, recognizing the recipient of an image, or giving verification and approval of the content in an image. Next, to that, there is another sort of techniques utilized as a part of information hiding, for example, steganography and cryptography. There are contrasts between these three methods, and they have their own advantage and disadvantage.

A. Digital Watermarking

Digital image watermarking is defined as the process to hide the information into host image, which is to be protected and extracted for copy right protection and its verification [1, 2, 3]. The media might be altered with the end goal that the inserted code is intangible or about indistinct to the client, yet might be distinguished through a computerized recognition process. Most usually, digital watermarking is connected to media signal, for example, pictures, audio signals, and video signals [4, 5, 6, 7, 8, 9]. In any case, it might likewise be connected to different sorts of media articles, including reports (e.g., through the line, word or character shifting), programming, multi-dimensional illustrations models, and surface textures of items.

Word Origin and History for watermark started in 1708, “distinctive mark on paper,” from water (n.1) + mark (n.1). Cf. German wassermarke. Not produced by water, but probably so called because it looks like a wet spot. The verb is recorded from 1866. The Italians were the first to use watermarks in the manufacture of paper in the 1270’s.Then watermark was used in banknote production by the Bank of England in 1697. It is a decent security feature in light of the fact that the watermark can’t be photocopied or checked successfully.

B. Invisible Watermark

Invisible watermark is a mark that have been embedded into a host image that not visible by human perspective. This mark can only be decoded by certain software to determine the owner. There are three types of invisible watermark that are robust, fragile and semi fragile. Many of existing watermarking schemes focused on the robust means to mark an image invisibly without really addressing the ends of an invisible watermarking scheme 10, 11, 12.

Robust watermarking are hard to expel from the object in which they are inserted, notwithstanding different assaults. The fragile watermarking algorithms are concerned with complete integrity verification. The slightest modification of the host image will alter or destroy the fragile watermark.

The semi-fragile watermarking algorithms are worried about uprightness of content confirmation. The semi-fragile watermarking can segregate regular image preparing and little content safeguarding noise.

C. Grayscale Image

The definition of grayscale is a spectrum of shades of gray with no possibility of color. The maximum dim of shade that doesn’t have any presence of the reflected light is black. In contrast, the maximum brightest of shade that has fully reflection or transmission of light is white. The transmission of light by three main colors that is Red, Green and Blue (RGB) or reflection of light by three main pigments that is Cyan, Magenta and Yellow (CMY) illustrate the body of the intermediate shade of gray. A decimal number from 0 to 255, or 0000 0000 to 1111 1111 representing (RGB) each component of brightness levels transmission of light. 8-bit grayscale imaging method have 8 bit in binary representation for example R=G=B = 0000 0000 represent white and R=G=B = 1111 1111. In (CMY) grayscale image, a percentage number from 0 to 100, representing (CMY) each pixel levels reflection of light. C =M=Y = 100 representing black and C=M=Y = 0 representing white.

D. Related Work on Image Watermarking

To propose a new technique for immediately authenticating that the content of a watermarked image (stamped) will not be changed once it was embedded [13]. It consists of an invisible watermarking process, which stamps a watermark pattern onto a source image and produces a verification key. The extraction process of watermark that decode an embedded watermark from the stamped image is based on the verification key [14, 15, 16]. It permits both, automatic verification and visual inspection which compares the watermark applied previously with an extracted watermark. The figure below shows the block diagram of the process.

After proposed watermarking have been tested on high quality grayscale images, synthetic images and color images with uniform color, the result is as expected. The watermark can be embedded into a test image without a little visible artifact and retain faithful color and details. Figure and table below shows the result of this research.

III. METHODOLOGY

A. *Embedding Process*

The principle of embedding is fairly simple and effective [17]. First, the pixel position will be determined using spiral scan technique as shown in the figure below. Embedding method of spiral scan technique:

The bits of 2-D array are scanned using spiral scanning technique and the bits are saved in a 1-D array.

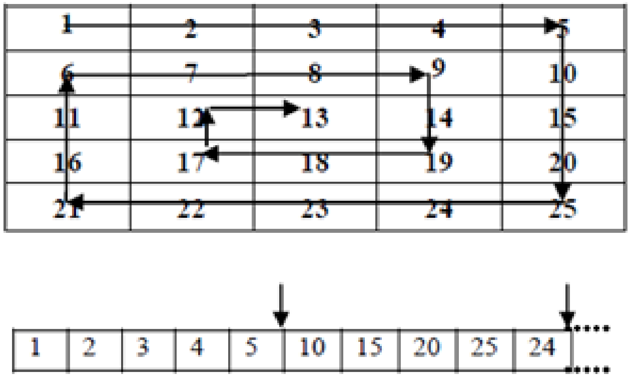


Fig. 1. Spiral scan technique

The generated 1-D array is scanned and the bits are saved in a 2-D array to generate embedded array.

1	2	3	4	5
10	15	20	25	24
23	22	21	16	11
6	7	8	9	14
19	18	17	12	13

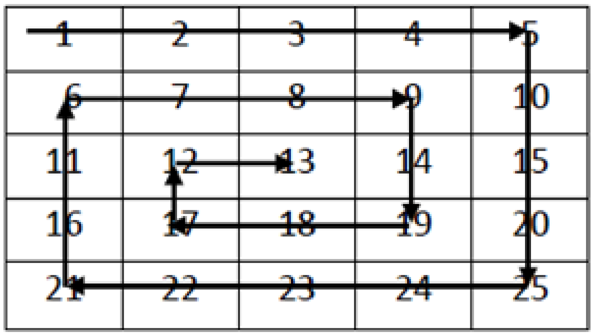


Fig. 2. Spiral scan technique

After the pixel position has determined, it will be embedded to watermark within the cover images using starting from 1st bit plane (LSB) to 8th bit plane (MSB). After embedding process is done, then the value of PSNR is calculated for every watermarked image. Watermark size will be change to shows the relationship between imperceptibility and capacity of the watermarked image.

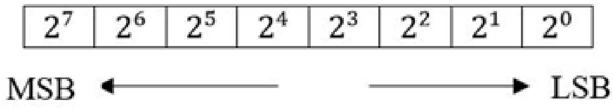


Fig. 3. Number of bits

$$\text{Peak Signal-to-Noise, PSNR} = 10 \log \frac{c^2 Max}{MSE} \quad (1)$$

Where,

$$\text{MSE} = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})^2 \quad (2)$$

PSNR is measured in decibel (dB). When the value of PSNR lowest then 30 dB quality of the result will be low, and embedding will be distortion. Therefore, to obtain the highest quality, the value of PSNR must be more than 40dB.

B. *Robustness Evaluation*

There is other measurement that can be utilized to calculate the correlation among the host and decoded watermark data.

$$\text{NCC}(W, W') = \frac{\sum_{i=1}^{M} \sum_{j=1}^{M} W(i,j) W'(i,j)}{\sqrt{\sum_{i=1}^{M} \sum_{j=1}^{M} W^2(i,j)} \sqrt{\sum_{i=1}^{M} \sum_{j=1}^{M} W'^2(i,j)}}$$

(3)

In this algorithm, W and W′ construct the host and the decoded watermarks considering i, j is the basis in the binary watermark image. The correlation among W and W′ is large in case that NCC (W, W′) is near to 1.

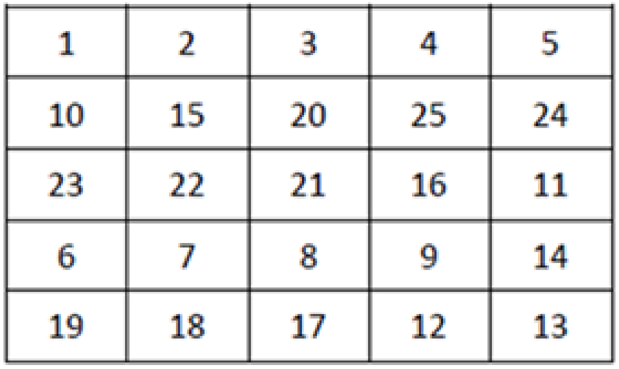
In contrast, it will show very small correlation among W and W′. By using these algorithms, particular image processing or enhancement procedures are executed to determine the robustness of this technique.

C. *Extraction Process*

First of all, in the extracting process is detect row and column to extract bit from 1st bit plane and watermark bit will be collected spirally then reconstructed the image. Comparison among extracted bit pattern and the initial one to nearly recognize the owner of the cover image can be an alternative if the high level assault been launch on the main watermark and completely corrupt it.

The element stored from encoded 2-D array also will be decoded by linear scanning and the elements will be stored in a spiral way as shown in Figure 4 and Figure 5 below:

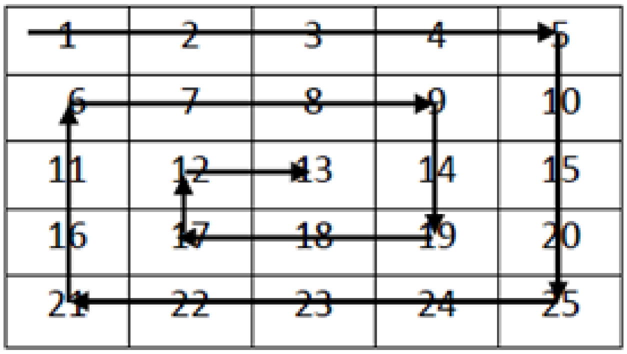
From encoded 2-D array:



1	2	3	4	5
10	15	20	25	24
23	22	21	16	11
6	7	8	9	14
19	18	17	12	13

Fig. 4. Embedded technique

The decoded array is generated by linear scanning of the elements from the above array and the elements are stored in a spiral way in a separate array, as shown below.



1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

Fig. 5. Extracting technique

IV. SIMULATION AND EXPERIMENTAL RESULT

A set of TVET image and picture image are utilized. The images are in grayscale TIFF format with a size of 512 × 512 pixels. Each of the images is represented by eight bit-depth. The cover images are available at USC-SIPI website where it provides datasets for the use of research. The figure shows the cover images used in this project.

Fig. 6. Cover image presented by a) Ariel, b) Elaine

Before the embedding process, there are processes taken place in the cover image. The first step is to select a location position of the cover image then change image into double. The cover image has to change into bit slicing. The main reasons for bit plane slicing are to slice the image into different bit planes. It will compose into lower and higher order bits. In this project, the cover image has been sliced into the 8-bit plane. Figure 7 below is the output of the coding above presenting the 8-bit decomposition of the cover image.

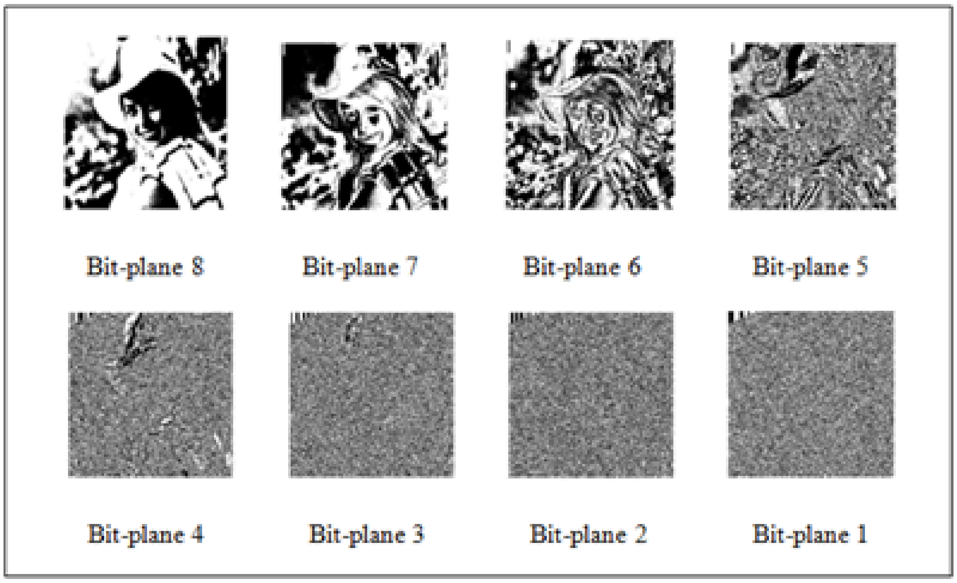


Fig. 7. 8-bit planes decomposition using a binary bit

TABLE 1
THE IMPACT OF 8-BIT PLANE INTO THE WHOLE IMAGE USING BINARY DECOMPOSITION BIT-PLANE

Bit plane no.	1	2	3	4	5	6	7	8
Impact value on image luminance	2	4	8	16	32	64	128	256

In the watermark preparation, the first step is to resize the cover into 10%, 20%, 30%, 40%, 50% with a size of the cover image then slice into the 8-bit plane. The next step is before embedding process takes place, all watermark image bits have to be assembled into sequential binary stream (bit stream).

In embedding process using spiral scan technique, the bit of binary watermark is used to overwrite the LSB of the cover image pixel in a clockwise pattern. Start from column minimum to maximum then start from row minimum to maximum. After that, the embedding process will continue from column maximum to minimum then row maximum to minimum. This process will continue until all bit from watermark is embedded. By using MATLAB tools, the proposed technique is implemented and two testing image that is Elaine, Stream, and bridge. This image is in grayscale format and sizes of 512 × 512. The value of PSNR and NCC is calculated after changing the watermark size. For the extracting process, we compared spiral with sequential extraction to prove that this embedding technique is not easily extracted. The table below show the result for each image:

TABLE 2
DIFFERENT VALUE OF PSNR AND NCC BETWEEN THE SPIRAL SCAN AND SEQUENTIAL TECHNIQUE IN STREAMANDBRIDGE.TIFF

Size of watermark	Embed percent	PSNR (dB)	NCC	
			Spiral	Sequent
209952	10%	52.0924	1	0.7241
419528	20%	45.6889	1	0.4803
627200	30%	40.4480	1	0.3242
839808	40%	35.5668	1	0.2410
1048352	50%	31.5866	1	0.1943

TABLE 3
DIFFERENT VALUE OF PSNR AND NCC BETWEEN THE SPIRAL SCAN AND SEQUENTIAL TECHNIQUE IN ELAINE.TIFF

Size of watermark	Embed percent	PSNR (dB)	NCC	
			Spiral	Sequent
209952	10%	52.1010	1	0.8520
419528	20%	45.6015	1	0.5645
627200	30%	40.4927	1	0.4070
839808	40%	35.7180	1	0.3061
1048352	50%	31.7685	1	0.2486

The result will show different value PSNR after embedding and value for NCC for spiral and sequential extraction of watermark in two watermarked image and which method is much better to use. From the above tables, it is proved that the proposed technique is able to embed watermark of size 50% of cover image with the value of PSNR is greater than the acceptable value (30dB). The results also prove that the proposed technique is robust because the most value of NCC is below 0.7 when extract with a sequential technique.

In Figure 8 and Figure 9 below is result of the extraction of watermark for each technique of every watermarked image. All figures below show only the 10% size of the watermark from the cover image.

a) Original watermark

b) Spiral extraction watermark

c) Sequential extraction watermark

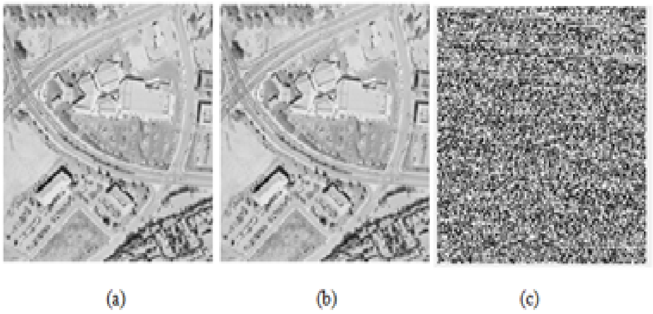


Fig. 8. Ariel.tiff watermark extraction of both techniques

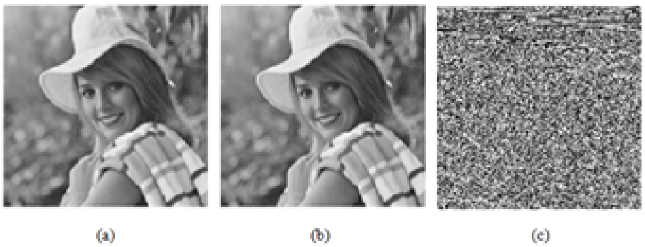


Fig. 9. Elaine.tiff watermark extraction of both technique

V. DISCUSSION AND IMPLICATION

Based on the result in this chapter, we can conclude that size watermark affect the value of PSNR and quality watermarked image. When PSNR value is larger than 30 dB, the quality of the image is the best quality. The spiral embedding technique make the watermark more robust because it orders the pixels of the image in a spiral pattern to avoid the embedding from being as effortlessly extracted. Differently from sequence embedding and extracting, since the pixels of the image are organized in the same manner as the original image, the observer will be able to extract without any extra effort. When we try to extract the watermark that has been embedded using the spiral technique in sequence order, the value of NCC extracted watermark is below 0.7. The Spiral Embedding and extracting designed for grayscale images to resist a visual attack. Its embedding pattern should reduce the effectiveness of statistical attacks that prefer a random distribution of embedded pixels in the cover image. The goal of the Spiral Embedding is to have a simple algorithm to embed content into an image using LSB embedding that will resist a visual attack.

In this project, analysis for the proposed technique has been successfully implemented and results are delivered. The value of PSNR and NCC of the method are compared for implementation on the major algorithms of steganography deployed in TVET or any digital imaging. The important of the watermark as a clarification of copyright, in order to avoid harm used and as a trademark purpose for well known.

VI. CONCLUSION

As conclusion, these projects focus on embedding an invisible watermark using LSB and spiral scan technique in grayscale image. It can help and give a new idea to protect the copyright of TVET and any digital information and provide the safe use of digital information. Previous research shows that PSNR is the most usually watermarked image quality metric that been used to determine the levels of strength and weakness of watermarking algorithms. Other than that, NCC is the most common metric used to verify the strength of the algorithm used after attacks were applied. This project mainly depends on the result of these two parameters to make sure this project successfully is done.

A. *Recommendations*

In Grayscale image watermarking using LSB and spiral scan embedding, there is a lot of improvement that can be done to make the research more advance and useful. In the future, this project can make several improvements in order to add another feature such as:

a) Use ISB embedding technique instead of LSB to improve the robustness of analysis execution to allow greater watermark can be loaded in the image and more difficult to extract.

b) More research is needed on the possible spiral scan embedding technique that may offer better performance.

REFERENCES

[1] M. Haribabu, C. H. Bindu, and K. V. Swamy, "A secure & invisible image watermarking scheme based on wavelet transform in HSI color space," *Procedia Computer Science*, vol. 93, pp. 462–468, 2016. doi: https://doi.org/10.1016/j.procs.2016.07.234

[2] C.-T. Hsu and J.-L. Wu, "Multiresolution watermarking for digital images," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 45, no. 8, pp. 1097–1101, 1998. doi: https://doi.org/10.1109/82.718818

[3] J. J. O'Ruanaidh, W. Dowling, and F. Boland, "Watermarking digital images for copyright protection," *IEE Proceedings-Vision, Image and Signal Processing*, vol. 143, no. 4, pp. 250–256, 1996. doi: https://doi.org/10.1049/ip-vis:19960711

[4] J. Huang, Y. Q. Shi, and Y. Shi, "Embedding im-

age watermarks in dc components," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 10, no. 6, pp. 974–979, 2000. doi: https://doi.org/10.1109/76.867936

[5] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "The effect of matching watermark and compression transforms in compressed color images," In *Proceedings of International Conference on Image Processing, ICIP 98,* Chicago, IL, 1998. doi: https://doi.org/10.1109/icip.1998.723519

[6] R. B. Wolfgang and E. J. Delp, "Overview of image security techniques with applications in multimedia systems." In *Proceedings of Multimedia Networks: Security, Displays, Terminals, and Gateways,* Dallas, TX: International Society for Optics and Photonics, 1998. doi: https://doi.org/10.1117/12.300900

[7] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1108–1126, 1999. doi: https://doi.org/10.1109/5.771067

[8] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1593–1601, 2001. doi: https://doi.org/10.1109/83.951543

[9] F. Dragomir, O. E. Dragomir, M. E. Ivan, S. S. Iliescu, and I. Stănescu, "Optimal embedded system for two-axis tracking PV panels," *Journal of Applied and Physical Sciences*, vol. 3, no. 1, pp. 1–6, 2017. doi: https://doi.org/10.20474/japs-3.1.1

[10] W. Zeng and B. Liu, "On resolving rightful ownerships of digital images by invisible watermarks," vol. 1. *Proceedings of International Conference on Image Processing,* Santa Barbara, CA: IEEE, 1997, pp. 552–555.

[11] W. Zeng, and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images," *IEEE Transactions on Image Processing*, vol. 8, no. 11, pp. 1534–1548, 1999. doi: https://doi.org/10.1109/83.799882

[12] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal processing*, vol. 66, no. 3, pp. 385–403, 1998. doi: https://doi.org/10.1016/s0165-1684(98)00017-6

[13] M. M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," vol. 2. In *Proceedings of International Conference on Image Processing,* Santa Barbara, CA: IEEE, 1997, pp. 680–683.

[14] S. P. Mohanty, P. Guturu, E. Kougianos, and N. Pati, "A novel invisible color image watermarking scheme using image adaptive watermark creation and robust insertion-extraction." In *Eighth IEEE International Symposium on Multimedia, ISM'06,* San Diego, CA: IEEE, 2006. doi: https://doi.org/10.1109/ism.2006.7 pp. 153–160.

[15] D. Vaishnavi and T. Subashini, "Robust and invisible image watermarking in RGB color space using SVD," *Procedia Computer Science*, vol. 46, pp. 1770–1777, 2015. doi: https://doi.org/10.1016/j.procs.2015.02.130

[16] M. A. Sayah, N. A. Kabir, and M. S. Jaafar, "Phantom study: Non uniformity quantity of technetium-99m in different segments of myocardial spect image," *International Journal of Applied and Physical Sciences*, vol. 3, no. 2, pp. 37–41, 2017. doi: https://doi.org/10.20469/ijaps.3.50002-2

[17] D. Chopra, P. Gupta, G. Sanjay, and A. Gupta, "LSB based digital image watermarking for gray scale image," *IOSR journal of Computer Engineering*, vol. 6, no. 1, pp. 36–41, 2012. doi: https://doi.org/10.9790/0661-0613641