International Journal of Engineering & Technology, 7 (4) (2018) 5322-5326

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.15300
Research paper

Comparison between improved histogram shifting and LSB (bit-plan mapping) in digital watermarking techniques

Omar Ahmed Mahmood [1] *, Ahmed Sabeeh Yousif [2], Falah Y.H. Ahmed [3]

[1,2] College of Technical Administrative /Mousl, Northern Technical University ,IRAQ,+964,Iraq /University Street
[3] Department of Information Science and Computing, Faculty of Information Sciences and Engineering (FISE), Management and Science University (MSU), 40100 Shah Alam, Malaysia
**Corresponding author E-mail: omar_ahmed@ntu.edu.iq*

Abstract

Editing, reproduction and delivery of the digital multimedia are becoming particularly easier and closer with the existence of the internet and the availability of pervasive and strongly multimedia tools. Digital watermarking has emerged as a possible method to address these issues. For the proposed Histogram Shifting, modification of the histogram and shifting is applied for embedding the stage; furthermore the contribution in this method incorporated the threshold concept to improve the visual quality of the host image. The performance of the proposed watermarking schemes has been evaluated by using the watermarked images (standard images) of size 512×512 (gray scale) with a different amount of variables "random bit streams" used in the histogram sniffing. The simulations are performed in MATLAB 7 software environment and the visual quality of output image measured by PSNR metric. A comparison is made between the results of the proposed algorithm with the best method namely LSB (Bit Plane Mapping) method and demonstrates that the proposed method is superior in performance in visual quality factor.

Keywords: *Digital Watermarking Concepts; Histogram Shifting (HS); Human Visual Quality; LSB Method.*

1. Introduction

Digital revolution has become a pervasive, in which digital data almost covers our lifestyle completely. This is largely borne from advances in the technology of capturing devices that are readily available at affordable prices and with better efficiency. This entails that huge amount of digital data are constantly taken, stored and exchanged whether for luxury, education, commerce, security and many other purposes that impacts directly all sides of human life. Sharing these large amounts of digital data is becoming even more easy thanks to the advances in communication networks that allow the transfer of these data at low cost with increase reliability. Data embedding includes embedding external data into a host for management purposes. The external data presents the management data, which are embedded obscurely into the host. The embedding of data is an ad-hoc process, in which the requirements of application of data in question are considered while performing the embedding [1]. The ad-hoc nature of data embedding leads to developing sub-research areas or branches under general data embedding area. Watermarking is a general concept of embedding copyright data into a host [2]. These methods are classified, generally, into two main groups: fragile [3] and robust [4]. The visual quality of images is distorted differently by watermarking methods. In some images, such distortion affects significantly the quality of the watermarked image; and consequently the application of the watermarking methods is limited practically.
Some embedding methods allow restoring the original host lost after achieving data embedding. Such methods are referred to as reversible methods [5]. In these methods, extra restoration data are embedded along with payload for reversible restoration. Usually, the restoration of the original host is achieved after extracting the payload.
The embedding of extra information of reversible restoration reduces the maximum amount of embeddable payload in the host. This amount is referred to embedding capacity. Some data embedding methods do not allow restoring the original host losslessly after changing it to accommodate the payload. Hence, data of the original host are lost due to embedding the payload. Such methods are referred to as irreversible data embedding [5], and they are not applicable to some data, such as medical or military images, which such data lost is not allowed.

2. Type of watermarking system

2.1. Blind

A watermarking method is referred to as a blind if the watermark is extractable from the modified image without a need to compare it with the original image.

2.2. Non-blind watermarking

In a non-blind watermarking method, the original image should be compared and correlated with the modified one in order to locate and extract the payload. Practically, such kind of method is not highly applicable for watermarking [6].

2.3. Semi-blind watermarking

Original data is not used for detection but tend to give the same properties in output as non-blind. Fingerprinting and copy control are some of the applied examples semi-blind watermarking.

3. Watermarking system mode

Watermarking is achieved using two procedures: Watermark embedding and Watermark extracting both of which as are detailed as follows:

1) A randomly generated key is used to locate positions of some pixels in the spatial domain or coefficients in the frequency domain.
2) An encoder modifies features of these pixels/coefficients in order to accommodate the payload. The modification includes partial substituting the values of pixels/coefficients according to the values of the payload.

The result modified image will differ from its original. This different affects the visual quality of the modified image. In some methods, the Human Visual System (HVS) are utilized to adaptively control the visual distortion in the image after the embedding process [7]. The generated key shall be shared between the sender/receiver.

Conversely, in payload extraction, the following steps are followed:

1) A decoder locates the position of modified pixels/coefficients using the same key generated for payload embedding.
2) Each modified pixel/coefficient is scanned to extract the payload.

Note that restoring the original values of these pixels/coefficients require extra reversible extraction data, which are inserted into the host along with the payload. Otherwise, the embedding method is irreversible, and the change in the values of pixels/coefficients is permanent.

4. Watermarking system mode

From the perspective of communication theory, the hosting watermarked image is considered as a communication channel that transfers the payload, as depicted in Fig. 1. Naturally, the characteristics of such a communication channel are known in advance, contrary to traditional communication channels, the characteristics of which are assumed to be compatible with known channel models. In addition, the characteristics of such a channel are not constant, as they keep changing over the time. Consequently, it is possible to exploit the characteristics of the host image to embed adaptively the payload with an added correlation from the image to the embedding block as shown in Figure 1[8].

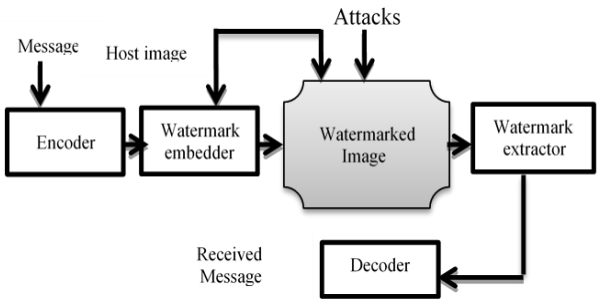

Fig. 1: The Model of Image Watermarking in Communication Theory.

5. Mathematic description of watermarking scheme

We describe the process of embedding a payload into a host mathematically. Let a host image denoted by H; which consists of pixels $P_{i,j}$ of two dimensions (i and j). Here, possible values of $P_{i,j}$ are in the range [0-255] in case of applying gray-level H. The watermarked image is denoted by $\acute{H}$, which is a sequence of $\acute{P}_{i,j}$. A randomly generated watermarking key is denoted by the symbol K.

The payload is denoted by W, where W is a sequence of bits $\{w_1,w_2,\ldots,w_i\}$ of length L, and $1 \le i \le L$. Note that $w_i \in \{0,1\}$. The payload after extraction is denoted by $\bar{W} = \{\bar{w}, \bar{w}, \ldots, \bar{w}\}$ of length L.

E is an encoder function of two inputs (H, W). E maps its two inputs into $\acute{H}$ using K as follows:

$$E(H,W)K = \acute{H} \tag{1}$$

K ensures the secrecy of the embedded payload (i.e., watermark). In extraction of the embedded watermark, a decoding function D takes an image I (as a single input) for watermark existence verification. Here, I can be a watermarked image, un-watermarked image or corrupted watermarked image, the ownership of which is to be verified by extracting the watermark using D. Such an extraction is achieved as follows:

$$D(I)K = \bar{W} \tag{2}$$

Here, the coded K is used to locate the position of watermarked pixels or coefficients in I.

In case of applying a non-blind watermarking, an additional input (the original image H) is added to D. H, here, presents the un-watermarked image of I. The watermark extraction process is defined as:

$$D(I,H)K = \bar{W} \tag{3}$$

Then, the extracted watermark $\acute{W}$ is compared with original watermark W using a comparison function C, which generates a binary output upon the following: If $\acute{W}$ and W are similar, C=1, otherwise, C=0. This process is defined as follows:

$$C_\zeta(\bar{W}, W) = \begin{cases} 1, & if C \ge \zeta \\ 0, & otherwise \end{cases} \tag{4}$$

Where ζ is a certain threshold and C is the correlation of two ($\bar{W}$, W).

6. Watermarking requirements

Watermarking is an application that is classified under the general framework of data embedding. For example, it is found in [9] that increasing the robustness of a watermarking method decreases the visual quality; however, the embedding capacity is increased. The three aforementioned requirements are detailed in the next subsections.

6.1. Visual quality

For an imperceptible watermarking method, the presence of the embedded watermark into the image must be un-detectable. Practically, a normal user does not have an access to the original image in order to make a visual quality comparison between the original and watermarked image. Hence, a scheme that is undetectable by HVS should suffice [10]. We can use criteria to evaluate the performance of a watermarking method in terms of visual quality by using Peak signal to noise ratio (PSNR).

6.2. Robustness

The second requirement of watermarking is robustness, in which an image should be able to withstand attacks that aim at removing, changing or corrupting the watermark [11]. Such robustness is subject to the application that the image is intended to be used for. Attacks may be intentional or un-intentional [12]. Conventional

image operations applied by a user may destroy the watermark data. Various operations in image compression field, such as scaling, coloring, gamma correction are examples of these operations. Nowadays, compression methods also can be classified as a kind of such altering/removing operations. Hence, a normal user, who for example, compresses a bitmap image using standard JPEG to conserve disk space, may perform un-intentional attacks. Intentional attacks require a pre-knowledge about watermarking systems and consumes more resources for attacking. Such intentional attack may involve: JPEG compression, blurring, Wiener filtering, Gaussian filtering, image rotation/re-scaling and Least Significant bit (LSB) manipulating.

6.3. Embedding capacity

Embedding capacity is the maximum amount of a payload that can be embedded into a particular image. This amount varies according to the applied watermarking method. Here, low SNR is common among watermarking channels, and it significantly reduces the embedding capacity. In images, the size of a watermark may vary between hundreds to thousands of bits [13].
The challenge is to embedding as much as possible payload while maintaining the visual quality at an acceptable level. Generally, high embedding capacity leads to more obtrusive in visual quality.
In terms of robustness, as watermark embedding capacity increases, the robustness increases too. In [14], a classification of low, medium, high and very high embedding capacity is proposed. Table-1- illustrates these classifications.

Table 1: Just an Example

Message size % of host message	Embedding capacity
0-2%	low
2-10%	Medium
10-20%	High
>20%	Very high

The embedding capacity can be calculated using as a ratio between the size of embedded payload to the size of original image, as follows:

$$Capacity = \frac{Totalnumberofbits\ (payload)}{Totalnumberofbits\ (hostingimage)} \quad (15)$$

7. Digital watermarking methods (spatial domain methods)

With the term fragile a watermarking technique which embeds a code in an image that is not readable anymore if the content is altered. Consequently, the original data are not recoverable too. And the reason why spatial domain methods became interest by the researcher? This is due to the reason of presents a high-capacity, high visual quality, low complexity, comparing to the method require transform domain. Below details of review both of these methods in this paper.

7.1. LSBS method

A bit-plane of digital image consists of a set of bits that have the same spatial position. This bit-plane is utilized in watermarking by decomposing each pixel (of a gray intensity level) into 8 different bits; where the first bit-plane consists of the Most Significant Bits (MSBs); and the 8^{th}bit-plane consists of the LSBs of pixels. A simple substitution method is then used to embed a watermark, by modulating a bit-plane according to the watermark values. Here, each bit-plane accommodates one bit from the watermark [16].
This watermarking method is considerably low computational complexity, as no mathematical operations are performed for the watermarking process. In addition, high embedding capacity can be attained at acceptable visual quality [16]. Exploiting more bit-planes for watermark embedding deteriorates the visual quality for watermarked image. The visual quality of pixels changes in different way according to the value of each pixel, where the change of bit-plane values leads to different visual quality change [17]. In the same literature, It is found that changing the bit-plane of pixels in smooth areas of an image leads to high distortion in the watermarked image when evaluated by HVS. The only disadvantage of LSB substitution is the low robustness against the attacks. Consequently, many watermarking methods have been proposed to enhance the robustness of LSB substitution-based method [20-22].

for i=1 *l(C)do*
$s_i \leftarrow c_i$
end for
generate random sequence k_i *using k*
$n \leftarrow k_i$
for i=1 *,……l(m)do*
$s_n \leftarrow c_n \leftrightarrow m_i$
$n \leftarrow n + k_i$
end for

Fig. 2: The Model of Image Watermarking in Communication Theory.

7.2. Histogram shifting method

Histogram shifting is based on that the 2^n intensity levels does occur in necessary in the histogram ofthe image, where n is the depth of pixels. Consequently, it is possible to exploit those intensity levels that do not exist to achieve watermarking. In [27], it is found such that method can achieve embedding capacity from 4 – 80 KB at PSNR=48 db in a grayscale image of size 512x512 pixels. Hence, it is therefore considered a high-performance watermarking method.
In Figure 3, an example on histogram shifting is depicted. We use this example to explain the general algorithm of histogram shifting watermarking. In this example, the following steps are followed to embed the watermark:

1) The histogram of the original image (Fig. 3 (a)) is scanned and an intensity level that does not exist in the histogram is found. Such an absent intensity level is referred to as the zero point. In this example, the zero point is the gray-level=255.
2) In the same histogram, the intensity level that occurs the most is found, and referred to peak point. In this example, the peak point is the gray-level= 154.
3) Here, the embedding capacity equal to the number of frequency of gray-level of peak point (i.e, 154), because this gray-level is used for embedding the watermark.
4) All intensity level in the range [155,254] are increased by 1, leading to shifting the histogram to the right by 1, as shown in Fig.3 (b). The shifting includes the gray-level 154 and 254. Such shifting leaves the gray-level of 154 empty in the histogram. In other word, gray-level 155 is no longer exists in the histogram as shown in the figure.
5) Then, the image is scanned again. If a pixel of gray-level 154 is found, then this pixel is used to embed one bit from the watermark as follows:

a) If watermark equal 1, then the peak point is increased by 1, i.e. the gray-level of 154 have a new value=155.
b) If watermark=0, the peak point is left without a change.

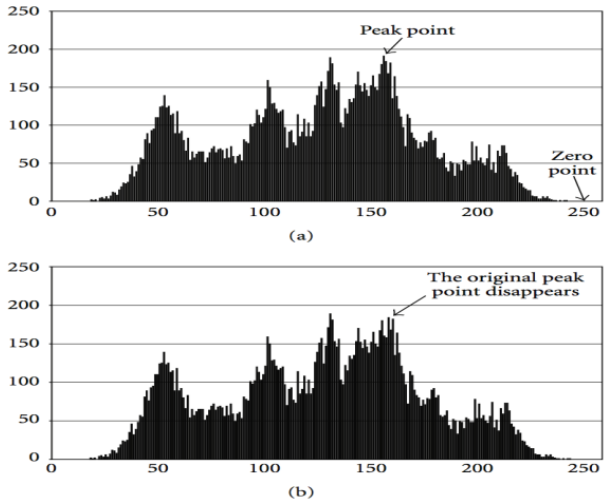

Fig. 3: Example on Histogram Shifting, where the Zero Point Is 255, and Peak Point Is 154 [19].

8. Performance and analysis of watermarking methods

In this paper, we present reviews of the experimental results for last works to the aforementioned watermarking methods. The previous experiments include histogram shifting [19] and LSB substitution [20-21] watermarking methods with used a set of standard images, followed by assessing the visual quality of watermarked images. Criteria are used for evaluation is PSNR. Further, the relation of visual quality to embedding capacity is reviews in spatial domain.

The measurement of performance of a watermarking method in term of visual quality can be achieved by a criterion referred to as Peak to signal noise ratio (PSNR). The PSNR is derived from computing mean squared error (MSE), which is the averaged pixel-by-pixel squared difference between original image P and watermarked image Ṕ as follows:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(\acute{P}_i - P_i)^2 \quad (1)$$

Where, N is total number of pixels, P_i is a pixels of i-th order in original image, and $\acute{P}_i$ is the counterpart of P_i.

Then, a signal to noise ratio (SNR) is defined as the amount of error in watermarked image in relative to the original image, as follows:

$$SNR = \frac{\frac{1}{N}\sum_{i=1}^{N}(P_i)^2}{MSE} \quad (2)$$

The value of SNR is computed in decibel (db) units as follows:

$$SNR(db) = 10log_{10}(SNR) \quad (3)$$

Finally, the PSNR is found as follows:

$$PSNR(db) = 10log_{10}\frac{P_{peak}^2}{MSE} \quad (4)$$

Here, P_{peak}^2 is the peak signal value of the image, which is 255 for 8 bits gray-scale image [23].

There is not standard value of PSNR, but generally, the larger PSNR, the better image quality. In [24], the PSNR>30 db is considered an accptable value of distortion in watermarked image. In [25], the PSNR>34 db is set as an acceptable value of it, whereas in [26], PSNR>38 db is considered as the acceptable value. In this paper, we consider the acceptable visual quality of watermarked image is that the achieve PSNR>30 db.

8.1. LSBS

Table (2) represents embedding capacity of LSBS method as constant, as each pixel accommodates one bit from payload. So, for an image of MxN pixels, the embedding capacity by LSBS in such an image is MxN bits [16-18].

Table 2: Show Relation between Visual Quality and Embedding Capacity as Constant in LSB Method [16-18]

Images	Amount of Capacity	PSNR (db)
Lena	50960	41.79
Jet	51243	40.97
Pepperss	50685	41.73
Baboon	65291	37.90

8.2. Histogram shifting (HSW)

For the proposed histogram shifting, setting the threshold to higher value results in a better embedding capacity. We set the threshold (T) to 10, 100 and 1000. The capacities at these thresholds are shown in table (3). The variance in the embedding capacity is due to the variance in statistical properties of each image.

We set a threshold value to select the intensity level for data embedding. The threshold determines the minimum number of pixels that such an intensity level should have in the histogram. We used a random bitstreamas a payload, because the amount of embeddable bits are variable according the statistic features of each image.

Table 3: Show Relation between Visual Quality and Embedding Capacity as Constant in LSB Method [16-18]

No	Images	Capacity (bits) T=0	Capacity (bits) T=10	Capacity (bits) T=100	Capacity (bits) T=1000
1	Tiffany	1	18	94	1038
2	Lake	1	1	1	1501
3	Splash	1	3	152	903
4	Pepper	3	9	76	989
5	Lena	1	69	137	1046
6	Gray21	1	12646	59	1
7	F-16	1	5	88	1078
8	Elaine	1	13	57	1329
9	Boat	1	14	197	654
10	Baboon	2	32	132	1130

In the spatial domain, we used Histogram Shifting and applied the concept of threshold to enhance the visual quality that is related directly to the amount of payload embedded. It is considered as a contribution in this work and the visual quality of the output image can be seen highly performing in terms of PSNR. Then, comparing it with Bit Plane Mapping mentioned in the literature review and it is considered the best method over the spatial domain methods [16-20], as a result it can be seen that the proposed Histogram Shifting perform high visual quality similar to the Bit Plane Mapping and also the threshold aspect works properly when applying it to the set of test images and it is valid to use this method in applications like transferring in the network channel with high capacity embedding in the host image with no degradation record.

Table 4: Show Relation between Visual Quality and Embedding Capacity as Constant in LSB Method [16-18]

Set of Images	PSNR for the Bit Plane Mapping [16-20].	PSNR for the proposed Histogram Shifting
Tiffany	34.8655	34.7633
Lake	32.3337	32.2271
Splash	42.1313	41.9221
Pepper	36.3691	36.2265
Lena	38.7898	38.7044
Gray21	51.0635	46.7221
F-16	37.5565	37.2333
Elaine	34.2419	34.2175
Boat	35.378	35.3576
Baboon	31.4001	31.3131
Tiffany	34.8655	34.7633
Lake	32.3337	32.2271
Splash	42.1313	41.9221
Pepper	36.3691	36.2265

9. Conclusion

PSNR was able to detect the visual distortion in watermarked images. It is shown that HSW achieves a variable embedding capacity and also shown that there is a trade-off between embedding capacity and visual quality. The HSW achieves a high visual quality in the standard images and also in medical images as LSBS method that done in the previous research therefore, HSW developed and performed high visual quality.

References

[1] Sabu M Thampi "Information Hiding Techniques: A Tutorial Review". Proceeding of ISTE- STTP on Network Security & Cryptography, LBSCE 2004.

[2] Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. IBM Systems Journal, 35(3.4), 313-336. https://doi.org/10.1147/sj.353.0313.

[3] Raja'S. A., Ahmed A., "A Fragile Watermarking Algorithm for Content Authentication", International Journal of Computing & Information Sciences. Vol.2, No.1, April 2004.

[4] F. Deguillaume, S. Voloshynovskiy, and T. Pun, "Secure hybrid robust watermarking resistant against tampering and copy attack", presented at Signal Processing, 2003, pp.2133-2170.

[5] Awrangjeb, M. and M. S. Kankanhalli, "Reversible watermarking using a perceptual model," Electronic Imaging, 14(1), 013014-1-8, 2005. (Pubitemid 40773601).

[6] X. Luo, D. Wang, P. Wang and F. Liu "A review on blind detection for image steganography", Signal Process., vol. 88, pp.2138, 2008. https://doi.org/10.1016/j.sigpro.2008.03.016.

[7] Juergen, S. (2005). Digital Watermarking for Digital Media. University of Cooperative Education Heidenheim, Germany.

[8] Ahmet, B. (2002). Watermarking Capacity Improvement by Low Density Parity Check Codes.Masterthesis.Bogazici University, Turkey.

[9] Gulati, K. (2003). Information Hiding Using Fractal Encoding. Master Thesis. Indian Institute of Technology Bombay, Mumbai.

[10] Shelby, P. (2000). Robust Digital Image Watermarking. Ph.D. Thesis. University of Geneve, Faculty of Science, Canada.

[11] Voyatzis, G and Pitas, I. (1999). Protecting Digital-Image Copyrights: A Framework. IEEE Trans. On Computer Graphics and Application. 19(1): 18-24.

[12] Voyatzis, G and Pitas, I. (1999). Protecting Digital-Image Copyrights: A Framework. IEEE Trans. On Computer Graphics and Application. 19(1): 18-24.

[13] Y. K. Seong, "Scene-based Video Indexing and Watermarking for Digital Broadcast Receivers ", Department of Mechatronics vol. Doctor of Philosophy Kwangju, Republic of Korea Kwangju Institute of Science and Technology 2003, p. 150.

[14] M. A. H. A. M. E.-b. Bourennane, "A Watermarking of Medical Image-New Approach Based on Multi-Layer Method," International Journal of Computer Science Issues, vol. 8, pp. 33-41, 2011.

[15] Viterbi, A. (1995). CDMA: principles of spread spectrum communication. Redwood City, CA, USA: Addison Wesley Longman Publishing Co. Inc.

[16] C. K. Chan and L. M. Chen. "Hiding data in images by simple LSB substitution", Pattern Recognit., vol. 37, pp.469 2004. https://doi.org/10.1016/j.patcog.2003.08.007.

[17] Wu, D. C. and Tsai, W. H. (2003). A steganographic method for images by pixel- value differencing. Pattern Recognition Letters. 24(9-10): 1613–1626. https://doi.org/10.1016/S0167-8655(02)00402-6.

[18] Chen, W. Y. (2003). A Comparative Study of Information Hiding Schemes Using Amplitude, Frequecy and Phase Embeddings. Ph.D. dissertation.Department of Electrical Engineering, National Cheng Kung University, Tainan, Taiwan, R.O.C.

[19] R. Caldelli, F. Filippini, and R. Becarelli, "Reversible watermarking techniques: An overview and a classification," EURASIP J. Inf. Security, vol.2010, 2010.

[20] Habes, A. (2006). Information Hiding in BMP image Implementation, Analysis and Evaluation. Information Transmissions in Computer Networks.6 (1): 1-10.

[21] Wu, M. and Liu, B. (1999). Watermarking for image authentication.Proceedings of the IEEE International Conference on Image Processing.

[22] Maniccam, S. S., and Bourbakis, N. (2004). Lossless compression and information hiding in images.Pattern Recognition. 37(3): 475–486. https://doi.org/10.1016/j.patcog.2003.08.010.

[23] Joachim, J., Eggers, J., and Bernd, G. (2000). Robustness of a blind image watermarking scheme. ICIP 2000, Special Session on WM. Sep. 10–13. Canada.

[24] Wu, N. (2004). A Study on Data Hiding for Gray-Level and Binary Images. Master Thesis. Chaoyang University of Technology, Taiwan.

[25] Cheung, W. N. (2000). Digital image watermarking in spatial and transform domains.TENCON Proceedings. 3: 374-378. https://doi.org/10.1109/TENCON.2000.892292.

[26] Hosinger, C., and Rabbani, M. (2000). Data embedding using phase dispersion. Presented at International Conference on Information Technology: Coding and Computing (ITCC2000).., vol.2.Oxford: Clarendon, pp.68–731892.

[27] Ahmed Sabeeh Y, Omar Ahmed M, and zaidomar (2018).Improved Implementation of Histogram Shifting In digital watermarking image Using Threshold.presented at Eighth International Conference on advances in computing, electronics and electrical technology Malaysia, Kuala-lumpur–CEET –18-121.