Ianna Journal of Interdisciplinary Studies
ISSN:2735-9883 \ E-ISSN:2735-9891

VOL -06 NO 2, 2024

WATERMARKING AND ITS TECHNIQUES: A REVIEW

Harpreet Kaur[1]Roop Shikha[2,]

[1]Assistant Professor, Department of Electronics & Communication Engineering, Swami Vivekanand Institute of Engineering & Technology, Banur, Punjab-140601

[2]Assistant Professor, Department of Electronics & Communication Engineering, Swami Vivekanand Institute of Engineering & Technology, Banur, Punjab-140601

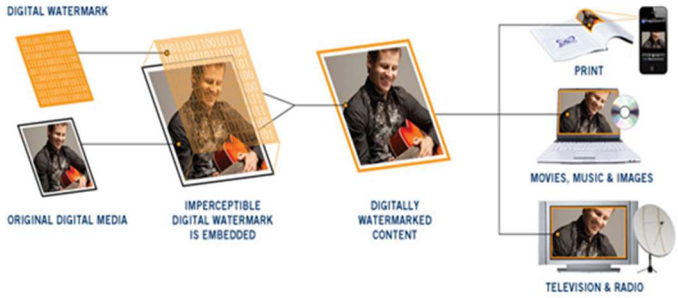
Abstract:

The necessity for copyright enforcement technology that can prevent copyright ownership and theft of multimedia items has become critical due to the rapid evolution of networked multimedia systems. Numerous data-hiding technologies, such as Steganography and cryptography, have been developed. One technique for concealing information in a digital image is steganography. Many of the existing digital watermarking methods are based on the relationship between steganography and cryptography. Recent developments in digital copyright protection techniques have generated a lot of interest. We'll talk about the watermarking process and its numerous methods in this essay.

Keywords: Watermarking; LSB; DFT; DCT; DWT; Performance Evaluation Metrices

INTRODUCTION

The public's access to digital material including audio, photos, and videos has regularly grown as a result of the Internet's rapid expansion. Analogue media is not preferred over digital media. Because of the ease with which digital content may now be created, copied, transmitted, and distributed, there is an urgent need for copyright enforcement systems that can safeguard the ownership of multimedia objects. For this, a variety of information-hiding methods, including cryptography, steganography, and watermarking, are being deployed [1]. Steganography involves hiding their mere existence, while cryptography protects the substance of messages by encrypting the message. Modern steganographic communication channels are simple to utilise thanks to advancements in computer and network technologies. Digital media is protected by copyright, data authentication, and security thanks to digital watermarking techniques [2]. It is a method connected to the long-ago covered writing method of information concealment [3]. Digital watermarking is the process of incorporating a secret piece of information, such as a watermark, into digital multimedia files like images, sounds, and videos. To identify the true owner or identity of the digital media, the encoded information is extracted. The following uses for watermarking exist: Copy Control, Broadcast Monitoring, Authentication, Proof of Ownership (copyright and IP protection), Data Hiding, and Copy Control. Fig. 1 illustrates a digital watermarking example.



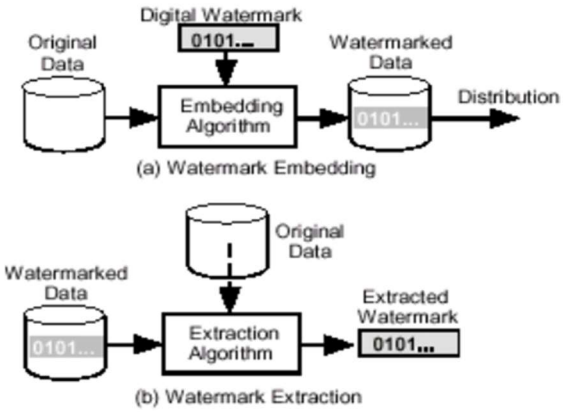
Digital watermarking

We provide a brief overview of the history of digital watermarking in Section 2, followed by a discussion of the fundamentals of digital picture watermarking, including its prerequisites and uses. The processes utilised for digital watermarking are presented in Section 3. The performance evaluation metrics are discussed in Section 4.

DIGITAL WATERMARKING

The process of putting a watermark into a multimedia object is known as watermarking. This watermark may be presented as text, a picture, an audio file, a video file, or graphics. Digital watermarking can also be considered a signature that discloses the identify of the owner [4].The transparent Logos that are frequently found placed at the corner of films or photos in an effort to prevent copyright infringement are one example of digital watermarking [5], [6]. Secret information is concealed by digital watermarking, which can be some text, an author's serial number, a company emblem, or graphics. Even if the watermarked material is processed, duplicated, or redistributed, this embedded information may still be recoverable [7]. Due to flaws in the Human Vision System (HVS), digital watermarking is possible; as a result, it becomes invisible and prevents degradation [8]. Visible and invisible watermarking are the two different types of watermarking. Applications of watermarking include ownership rights, broadcast monitoring, and DVD copy control. The fundamental steps of watermarking are shown in Fig. 2. The process of watermarking consists of four steps:

Watermark embedding: In this step we have an original image and a watermark. A watermark is embedded into original image and the image obtained is known as watermarked image.



Watermarking process

- Distribution: This step can be also known as transmission step. During this step the watermarked image may be subjected to attacks either deliberately or due to transmission error or noise.
- Watermark extraction: When the watermarked image is obtained the watermark is extracted from the image by using various extraction algorithms.
- Watermark detection: Once the watermark is extracted, it is compared with original watermark and co-relation coefficient (CR) is calculated. If the CR is above threshold, then the ownership is preserved.

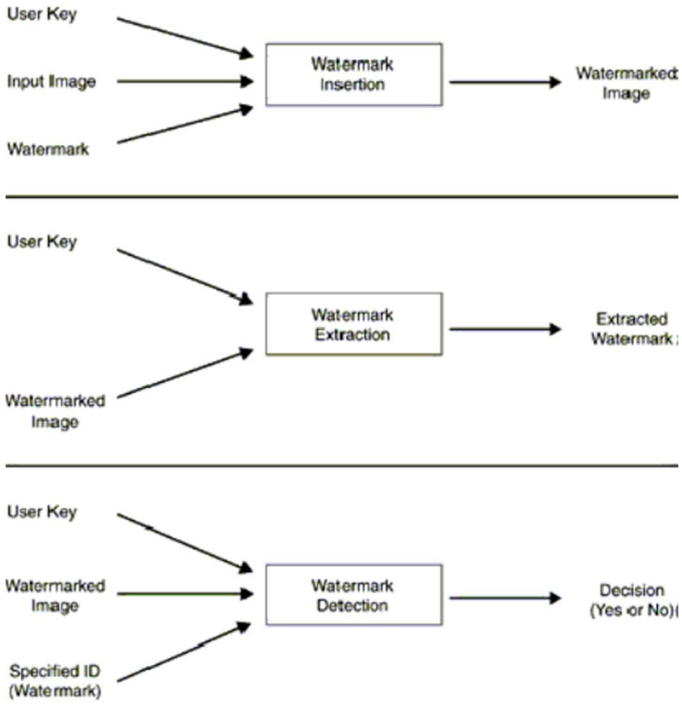
The requirements of watermarking are:

- Reliability: There are two levels of reliability: robustness and false negatives [9]. Robustness is the ability to detect after signal processing, geometrical and non geometrical attacks.
- Tamper Resistance: It is should be hostile to attacks [10].
- Hiding capacity: Size of information that can be hidden in cover image. If the hiding capacity is large then it allows smaller cover image with message of fixed capacity to be embedded [11].
- Transparency: Describes similarity between original and extracted watermark [12].
- Security: A watermark should be accessible only by authorized parties. A watermark should be secure enough that hackers cannot remove the watermark.

WATERMARKING TECHNIQUES

Watermarking technique can be applied in two domains:

Spatial domain and Transform domain.



Phases of watermarking

Spatial domain

In spatial domain methods, the watermark is directly embedded by altering the pixels, which results in an alteration of the intensity values [13]. This method combines straightforward pixel operations with the host image without applying any changes to it. By comparing the pixels' values to what is predicted, the watermark can be found. This technique's shortcomings include limited embedded information, a lower level of noise and compression resistance, and a weaker level of geometric attack resistance. These methods have recently been abandoned. Least Significant Bit (LSB) Modification, Patchwork, Texture Block Coding, Correlation-based, SSM modulation-based, etc. are a few popular spatial domain algorithms. The LSB algorithm is the most often used one.

Least Significant bit(LSB)

LSB, which swaps out the pixels' least significant bits (which were chosen to conceal the information). In this illustration, information will only be embedded using the least significant bit of each pixel [14]. There have been several enhanced variations of this approach put forth. In an upgraded version, pixels are determined using keys and pseudo random numbers. A two-step technique was proposed by Schyndel[15]. The simpler method involves embedding the msequence on the LSB of the picture data, while the more complicated method involves LSB addition. Celik [16] proposed a method that adds new operational points to capacity distortion curves and recovers the watermark by compressing the distorted curves.

Patchwork algorithm

This method was created in the MIT Media Lab [17]. It is a statistical pseudorandom model. This technique incorporates information into pixel brightness levels using the statistical properties of pixels. According to Hartung and Kutter [18], patchwork is a technique in which randomly chosen pairs of pixels are utilised to hide one bit by raising and lowering it by one. The expected value of the sum of the differences between the pixel pairs is given by 2N if the image satisfies certain statistical criteria.

Texture Block Coding

Used primarily for photos with texture parts. This technique conceals data within a picture's continuous random texture patterns. Due to the identical distortion in both picture areas, this approach is remarkably resilient to distortion of any kind and yet allows for watermark recovery using autocorrelation [18].

Transform domain

By altering transform coefficients to support additional features, the transform domain approach makes use of the characteristics of other domains. There are two types of transform domain methods: frequency domain and wavelet domain.

Frequency domain

The coefficients of a modified image are watermarked in the frequency domain, and the watermarked image is then inverted to produce the image in the spatial domain.[19] JPEG-based [20], spread spectrum [21], [22], and content-based techniques [23] are the approaches employed in the frequency domain.The Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and other techniques are used to transform frequency images.

Discrete Fourier Transform (DFT)

A stationary signal—one whose qualities don't change—can be broken down into its constituent parts using the Fourier transform. When processing signals made up of a mix of sine and cosine signals (sinusoids), it is a potent tool [24]. Phase and magnitude are the two halves of a Fourier coefficient [25]. The fact that DFT is rotation, translation, and scale invariant aids it in recovering from geometrical distortions, which is one of its key advantages. Pereira[26] states that DFT techniques can be categorised into two groups: those based on invariance and those that embed a template into the image that is sought out during the detection of the watermark and provides details about the alteration the image has undergone. Using log-polar and log-log maps, Pereira [27] presented template-based recovery of Fourier-Based Watermarks in 1999.

Discrete Cosine Transform (DCT)

DCT represents data in terms of frequency space rather than amplitude space, similar to a Fourier Transform. The perceptibility of changes is estimated using Watson's DCT-based visual model [28], [29], [30] in terms of an image block DCT. An early frequency domain technique for

watermarking digital images is based on the robustness and transparency of spread-spectrum communications. When DCT coefficients have high intensity values, the watermark signal is strong; when they have low values, it is attenuated. Watermark is quite resilient and transparent when introduced into perceptually important components. The entire image is affected by the addition of a watermark to one DCT coefficient. Many algorithms are presented based on these transformation functions. A method to modulate DCT coefficients using a one-dimensional bipolar binary sequence was proposed by Boland [31]. In his DCT approach, proposed by Barni [32], pseudo random numbers are incorporated into the DCT coefficients. This algorithm is resistant to Gaussian noise, JPEG compression, low pass and median filtering, histogram equalisation, stretching, and resizing. In 1996, Bors [33] proposed an algorithm that was an expanded version of Barni's technique by inserting watermark in mid frequency coefficients. Barni also claimed that watermark insertion in high frequency are subject to attacks whilst in low frequencies are sensitive to adjustments. Another approach by Zhu [34] recommended that a picture be segmented into non-overlapping blocks with watermarks contained in their DCT coefficients. The algorithm's results showed that the DC component is better suited to embed watermarks on DCT domain than the AC component. In order to increase resistance against jpeg compression, Lin [35] proposed DCT watermarking by putting watermark in low frequency component. The image quality can be decreased by simply changing the low frequency component, so in this technique, the DCT coefficient is changed using the concept of the mathematical residual. With the help of this method, the embedded watermark can continue to function despite being assaulted by image processing procedures, especially when using the high compression ratio JPEG format.

Wavelet domain

Wavelets are mathematical operations that separate data into distinct frequency components. Each frequency component is subsequently analysed with resolution that is matched to its scale. Jean Morlet developed the concept of the wavelet transform, which gave seismic analysis a new mathematical tool [36]. According to Morley's definition in [37], a wavelet is a family of functions made up of the translations and dilations of a single function known as the "mother wavelet" (t).

$$\psi(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right) \qquad (1)$$

Where a is scaling factor which measures the degree of compression and b is translation factor which measures the time location.

Discrete WaveleteTransformtion

Wavelet transformations constitute the basis of the wavelet domain. Both time and frequency information are included in the wavelet domain. Because of their benefits, such as simultaneous

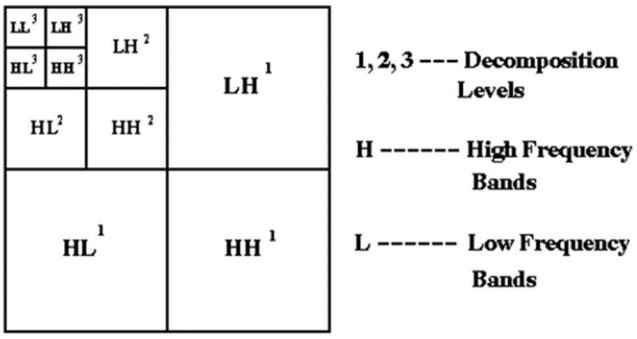
localisation in time and frequency and quick computation, wavelets are frequently employed in many different industries. The four components of the DWT co-efficient are LL, LH, HL, and HH. LH, HL, and HH are high frequency band components, while LL is a component with a low frequency band. Since changes in the high frequency band are not visible to HVS, which are sensitive to low frequency band changes, the watermark is placed there [38].

The steps of algorithm are following:

In this the original image is decomposed in various sub bands.

DWT transformation, these sub bands can be decomposed to one, two or three level.

The watermark is embedded in the sub band that is most suitable.



3-Level DWT

- After embedding watermark inverse transformation is performed and watermarked image is obtained.

DWT can be broken down into numerous layers. Figure 4 depicts a 3-Level DWT. Due of its various benefits, it is the transformation that is employed the most frequently. Numerous algorithms are built on DWT transformations. Blind picture watermarking using a chaotic key was proposed by Zhuancheng [38], where the watermark is embedded in the LL subband and dynamic coefficient quantization is used to achieve invisibility and robustness, resulting in the embedding of significant information. This transformation has undergone a lot of labour. High frequency subbands were also used for watermark embedding because they offered greater robustness than low frequency subbands. Watermarks should be initially embedded in low frequency subbands, and the remaining data should be contained in high frequency subbands, according to Daren [40]. A unique integer wavelet transform-based lossless data concealing approach for digital photos has been presented by Guorong Xuan et al., [41]. DFT, SVD, and DCT are just a few of the transformations that have been combined with DWT.

PERFORMANCE EVALUATION METRIC

MSE (mean square error)

The distinction between values suggested by an estimate and the actual quality that is being certified is what is meant by the definition of it. MSE is shown as:

$$\text{MS E} = \frac{1}{\text{XY}\left[\sum_{i=1}^{X}\sum_{j=1}^{Y}(c(i,j) - e(i,j))\right]}$$

The image's height and width are represented by the values X and Y. The embed image's pixel value is e (imp), while the cover image's value is c (i, j).

PSNR (peak signal to noise ratio)

The ratio of maximum power to corrupting noise determines how well an image is represented. It stands for either image degradation or image repair [42].A decibel scale is used to describe it. The quality of the image is higher the higher the PSNR value. PSNR is displayed as:

$$PSNR = 10\log_{10}\left(\frac{L * L}{\text{MSE}}\right)$$

Techniques	Advantages	Disadvantages
LSB	• Easy To understand and Implement. • Less distortion in image quality. • High transparency.	• Limited information embedded. • Less resistant to noise and compression. • Less Robustness.
Patchwork	• Uses statistical characterstics.	• Limited information embedded.
Texture Block Coding	• High robustness	• Limited information embedded.
Discrete Fourier Transform(DFT)	• Powerful tool for analyzing Stationary signals. • It is rotation, scaling and translation invariant which helps it in recovering from geometrical distortions.	• Complex computations. • Difficult to understand. • High Cost.
Discrete Cosine Transform(DCT)	• Mid frequency coefficients does not get affected by watermark insertion, hence watermark cannot be removed by any attack.	• Embedding in high frequency are vunerable to attacks whereas in low frequencies it is sensitive to alterations. • Blockwise DCT destroys invariance.
Discrete Wavelet Transform(DWT)	• Simultaneous localization in both time and frequency domains. • Able to separate fine details. • Fast computation	• High Computation cost. • Complex implementation.

Comparsion of different techniques with there advantages and disadvantages.

SNR(Signal to Noise ratio)

SNR (Signal to Noise ratio) gauges the imaging's sensitivity. Measuring the signal strength in relation to the noise is helpful. It is calculated using the following formula:

$$S\,NR_{db} = 10\log_{10}\left(\frac{P_{signal}}{P_{noise}}\right)$$

BER (bit error ratio)

The ratio of the number of bits received in mistake to the total number of bits received is known as bit error rate, or BER.

$$BER = \frac{P}{(H * W)}$$

CONCLUSION

In this essay, we've covered a number of digital watermarking-related topics, including an overview, the fundamentals, the requirements, the methods, and the applications and restrictions. The benefits and drawbacks of watermarking techniques are discussed in order to aid new researchers in related fields. We sought to include fundamental information about watermarking in this paper to aid new researchers.

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Digital image steganography: Survey and analysis of current methods, Signal Processing 90 (3)(2010) 727–752.

[2] P. Singh, R. Chadha, A survey of digital watermarking techniques, applications and attacks.

[3] G. Voyatzis, I. Pitas, The use of watermarks in the protection of digital multimedia products, Proceedings of the IEEE 87 (7) (1999) 1197–1207.

[4] V. M. Potdar, S. Han, E. Chang, A survey of digital image watermarking techniques, in: Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on, IEEE, 2005, pp. 709–716.

[5] E. Hussein, M. A. Belal, Digital watermarking techniques, applications and attacks applied to digital media: A survey, International Journal of Engineering 1 (7).

[6] C. I. Podilchuk, E. J. Delp, Digital watermarking: algorithms and applications, Signal Processing Magazine, IEEE 18 (4) (2001) 33–46.

[7] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, J. K. Su, Attacks on digital watermarks: classification, estimation based attacks, and benchmarks,Communications Magazine, IEEE 39 (8) (2001) 118–126.

[8] A. Kaur, J. Kaur, Survey on digital image watermarking: Techniques and attacks.

[9] F. A. Petitcolas, Watermarking schemes evaluation, Signal Processing Magazine, IEEE 17 (5) (2000) 58–64.

[10] I. J. Cox, M. L. Miller, J. A. Bloom, Watermarking applications and their properties, in: Information Technology: Coding and Computing, 2000. Proceedings. International Conference on, IEEE, 2000, pp. 6–10.

[11] E. T. Lin, E. J. Delp, A review of data hiding in digital images, in: PICS, 1999, pp. 274–278.

[12] M. D. Swanson, M. Kobayashi, A. H. Tewfik, Multimedia data embedding and watermarking technologies, Proceedings of the IEEE 86 (6) (1998) 1064–1087.

[13] L. Liu, A survey on digital watermarking technologies, Tech. rep., Technical Report, Stony Brook University, New York, USA (2005).

[14] D. Chopra, P. Gupta, A. Gupta, Lsb based digital image watermarking for gray scale image, IOSR Journal of Computer Engineering (IOSRJCE) ISSN 2278–0661.

[15] R. G. van Schyndel, A. Z. Tirkel, C. F. Osborne, A digital watermark, in: Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference, Vol. 2, IEEE, 1994, pp. 86–90.

[16] M. U. Celik, G. Sharma, A. M. Tekalp, E. Saber, Lossless generalized-lsb data embedding, Image Processing, IEEE Transactions on 14 (2) (2005) 253–266.

[17] N. Nikolaidis, I. Pitas, Robust image watermarking in the spatial domain, Signal processing 66 (3) (1998) 385–403.

[18] F. Hartung, M. Kutter, Multimedia watermarking techniques, Proceedings of the IEEE 87 (7) (1999) 1079–1107.

[19] F. Y. Shih, S. Y. Wu, Combinational image watermarking in the spatial and frequency domains, Pattern Recognition 36 (4) (2003) 969–975.

[20] J. Zhao, E. Koch, Embedding robust labels into images for copyright protection, in: KnowRight, Citeseer, 1995, pp. 242–251.

[21] J. CoxI, J. Kilian, F. Leighton, et al., Secure spread spectrum watermarking for multimedia, IEEE transactions on image processing 6 (12) (1997) 1673–1687.

[22] J. J. Ruanaidh, T. Pun, Rotation, scale and translation invariant spread spectrum digital image watermarking, Signal processing 66 (3) (1998) 303–317.

[23] P. Bas, J.-M. Chassery, B. Macq, Image watermarking: an evolution to content based approaches, Pattern recognition 35 (3) (2002) 545–561.

[24] R. N. Bracewell, R. Bracewell, The Fourier transform and its applications, Vol. 31999, McGraw-Hill New York, 1986.

[25] T. K. Tsui, X.-P. Zhang, D. Androutsos, Color image watermarking using multidimensional fourier transforms, Information Forensics and Security, IEEE Transactions on 3 (1) (2008) 16–28.

[26] S. Pereira, T. Pun, Fast robust template matching for a_ne resistant image watermarks, in: Information Hiding, Springer, 2000, pp. 199–210.

[27] S. Pereira, J. J. Ruanaidh, F. Deguillaume, G. Csurka, T. Pun, Template based recovery of fourier-based watermarks using log-polar and log-log maps, in: Multimedia Computing and Systems, 1999. IEEE International Conference on, Vol. 1, IEEE, 1999, pp. 870–874.

[28] A. B. Watson, Digital images and human vision, MIT press, 1993.

[29] M. Eyadat, S. Vasikarla, Performance evaluation of an incorporated dct block-based watermarking algorithm with human visual system model, Pattern recognition letters 26 (10) (2005) 1405–1411.

[30] W. Osberger, N. Bergmann, A. Maeder, An automatic image quality assessment technique incorporating higher level perceptual factors, in: Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on, IEEE, 1998, pp. 414–418.

[31] J. O´ .Ruanaidh, W. Dowling, F. Boland, Watermarking digital images for copyright protection, IEE Proceedings-Vision, Image and Signal Processing 143 (4) (1996) 250–256.

[32] M. Barni, F. Bartolini, V. Cappellini, A. Piva, A dct-domain system for robust image watermarking, Signal processing 66 (3) (1998) 357–372.

[33] A. G. Bors, I. Pitas, Image watermarking using dct domain constraints, in: Image Processing, 1996. Proceedings. International Conference on, 5 Vol. 3, IEEE, 1996, pp. 231–234.

[34] G. Zhu, N. Sang, Watermarking algorithm research and implementation based on dct block, World Academy of Science, Engineering and Technology 45 (2008) 38–42.

[35] S. D. Lin, S.-C. Shie, J. Guo, Improving the robustness of dct-based image watermarking against jpeg compression, Computer Standards & Interfaces 32 (1) (2010) 54–60.

[36] S. Mallat, A wavelet tour of signal processing, Access Online via Elsevier, 1999.

[37] P. Wojtaszczyk, A mathematical introduction to wavelets, Vol. 37, Cambridge University Press, 1997.

[38] S. Swami, Digital image watermarking using 3 level discrete wavelet transform.

[38] Z. Zhuancheng, Z. Dianfu, Y. Xiaoping, A robust image blind watermarking algorithm based on adaptive quantization step in dwt [j], Journal of Image and Graphics 11 (6) (2006) 840–847.

[39] R. SOHEILI MOHAMMAD, A robust digital image watermarking scheme based on dwt, JOURNAL OF ADVANCES IN COMPUTER RESEARCH.

[40] Daren, Huang and Jiufen, Liu and Jiwu, Huang and Hongmei, Liu, A DWT-based image watermarking algorithm, Proceedings of the IEEE International Conference on Multimedia and Expo, 2001, pp. 429-432

[41] G. Xua, Y. Q. Shi, C. Yang, Y. Zheng, D. Zou, P. Chai, Lossless data hiding using integer wavelet transform and threshold embedding technique, in: Multimedia and Expo, 2005. ICME 2005. IEEE International Conference on, IEEE, 2005, pp. 1520–1523.

[42] P. Kaushik, Y. Sharma, Comparison of di_erent image enhancement techniques based upon psnr&mse, International Journal of Applied Engineering Research 7 (11) 2012.