IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMPLEMENTATION OF DIGITAL IMAGE WATERMARKING FOR JPEG IMAGES

[1]DHASHANEE J, [2]DR. SUDHA M S, [3]CHANDRIKA O P, [4]DEEKSHA P,[5]ADARSH A

[1345]STUDENT, [2]ASSO.PROFESSOR

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

CAMBRIDGE INSTITUTE OF TECHNOLOGY, KRPURAM, BENGALURU-36.

Abstract:Digital watermarking is the method of hiding digital data in any form of multimedia data such as image, audio, video, etc. Digital watermarks are used for verifying the integrity and authenticity of multimedia data and also used to prevent fraud and forgery. This paper introduces a straightforward and reliable watermarking algorithm employing the third and fourth least significant bits (LSB) technique. Compared to traditional LSB methods, the proposed algorithm demonstrates enhanced robustness in concealing data within images. Specifically, the algorithm embeds two bits within the third and fourth LSB positions. Experimental findings indicate superior quality of the resulting watermarked image.

***Index Terms*-Digital watermarking, Grayscale images, secret data, LSB, PSNR.**

I. INTRODUCTION

Digital watermarking is a technique used to embed covert markers in various types of digital signals, such as audio, video, or images. These markers are typically used to identify ownership or authenticate the integrity of the signal. Unlike metadata, digital watermarks do not change the size of the carrier signal and can be either robust or fragile depending on the intended use case. One application of digital watermarking is source tracking, where watermarks are embedded at each point of distribution to trace the origin of illegally copied content, such as movies. Digital watermarking is a method used to embed imperceptible markers within digital content, such as images, videos, audio files, or documents. These markers are typically added to assert ownership, authenticate the integrity of the content, or track its distribution. Unlike traditional watermarks applied to physical media, digital watermarks are hidden within the content itself and are usually not detectable to the human eye or ear. Digital watermarking techniques vary in robustness and fragility, depending on the intended use case, with some designed to withstand modifications to the content while others are easily destroyed by such alterations. Overall, digital watermarking serves as a passive protection tool, allowing for the identification and tracking of digital content without degrading its quality or controlling access to it.

In an era dominated by digital content, the need to protect intellectual property and ensure data integrity has become increasingly critical. Digital watermarking emerges as a potent solution, offering a covert means of embedding identifying information within various forms of digital media. This introduction delves into the fundamentals of digital watermarking, exploring its principles, applications, challenges, and future prospects.

Digital watermarking can be likened to a hidden signature within digital content, serving as a form of copyright protection and authentication. Unlike traditional watermarks visible on physical documents, digital watermarks are imperceptible to the human senses, seamlessly integrated into the digital signal itself. This covert nature allows for discreet ownership identification and content tracking without compromising the user experience.

At its core, digital watermarking involves the embedding of additional data, termed the watermark, into the original digital signal, often referred to as the carrier signal. The process typically entails modifying the carrier signal in a manner that is imperceptible to users but can be detected and extracted through specialized algorithms. The watermark may contain information such as copyright details, authorship attribution, or transactional data, depending on the application requirements.

The versatility of digital watermarking extends across various domains, including media and entertainment, document authentication, forensic analysis, and copyright enforcement. In the media industry, digital watermarks play a pivotal role in combating piracy by enabling content creators to trace unauthorized copies back to their source. Moreover, digital watermarks find utility in document verification, ensuring the authenticity and integrity of digital contracts, certificates, and official records.

II. RELATED RESEARCH

In this sectionTahera Akhtar Laskar and K. Hemachandran etal.[1] proposed two watermarking algorithms for embedding and extraction process and use two images as cover image and watermark image of same format as input image. They have considered two image formats JPEG (JointPhotographic Experts Group) and PNG (Portable Network Graphics) of different resolutions for analyzing the performanceof the proposed algorithm.

K. Deepika, Sudha M. S., Sandhya Rani M.H etal. [2] proposed adigital watermarking scheme based on integer wavelet transform and histogram techniques. Lifting scheme-based integer wavelet transform is used to provide ease of transformation of compressed data and to increase the data embedding capacity. Also, histogram technique which is one of the reversible data hidings is used to embed the secret data into original image and retrieve the original data back after extraction.

Dr. Khaldoon M. Al-Dwairi, Meran M. Al-Hadidi et al. [3] proposed anImplementation for a Digital Watermarking Algorithm on Different Image Format Types.

Lamia Alam, Pranab Kumar Dhar, Mirza A. F. M. Rashidul Hasan, Mohammed Golam Sarwar Bhuyan, and Golam Moktader Daiyanet al. [4] proposed an improved JPEG compression algorithm by modifying the luminance quantization table for color image. Quantization step plays an important role in JPEG compression process.

Anuja Dixit, Rahul Dixit et al. [5] proposed aet al.Review on Digital Image Watermarking Techniques

Abdullah Bamatraf et al. [6] proposed digitalwatermarking algorithm using combination of least significantbit and inverse bit to improve quality of watermarked image. In this, before embedding the watermark the algorithm usesLSB by inversing the binary values of the watermark textand shifting the watermark according to the odd or evennumber of pixel coordinates.

M. S. Sudha, T. C. Thanuja et al. [7] proposed thehardware implementationof the image watermarking algorithmoffers numerous distinct advantages over the software implementation in terms of low power consumption, less area usage and reliability.

Mehmet Utku Celik, Gaurav Sharma, Eli Saber, Ahmet Murat Tekalp et al.[8] proposed amethod that thwarts the VQ attack while sustaining the superior localization properties of block wise independent watermarking methods.

III. METHODOLOGY

The Least Significant Bit (LSB) technique is a straightforward method commonly employed to embed information within a cover image. This technique involves altering the least significant bits of pixel values in the cover image to encode a secret message. Typically, the first 8 bytes of the grid are reserved for embedding the number of bits needed to represent the secret message, with subsequent bits altered according to the message..

One notable advantage of the LSB technique is its simplicity, requiring minimal computational overhead for both embedding and extraction processes. On average, only half of the bits in the image need to be modified to conceal a secret message effectively.However, a trade-off exists between the level of concealment and the resulting image quality. Since LSB alterations affect only the least significant bits of pixel values, the changes in color intensity are minimal, rendering them imperceptible to the human visual system. Consequently, the quality of the watermarked image may degrade slightly, particularly when using higher bit depths.

Despite its effectiveness in hiding information from human observers, the LSB technique is vulnerable to passive attacks. An attacker can easily extract the embedded message by analyzing the altered LSBs, as the extraction process involves simple bitwise operations

.

For example,

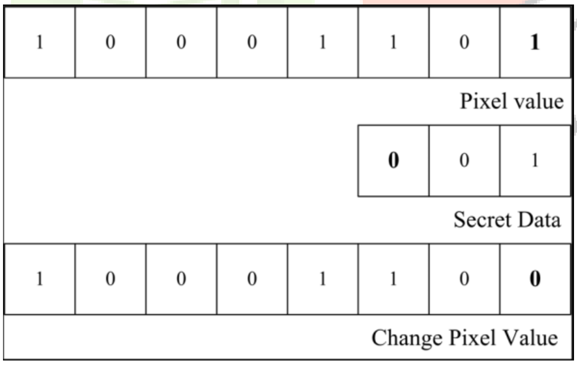
Figure 1 shows the 1-bit LSB, In Figure 1, the pixel valueof the cover image is 141(10001101)2 and the secret datais 0. It applies to LSB-1 that the changed pixel value ofthe cover is 140(10001100)2.

For instance, in the case of 1-bit LSB embedding, a change from a pixel value of 141 to 140 represents the encoding of a single bit of secret data. Given the binary nature of the LSB encoding, each pixel can store one bit of information, allowing for a total capacity of 65,536 bits in a 256 x 256-pixel image.

In conclusion, while the LSB technique offers simplicity and effectiveness in concealing information within images, its

Susceptibility to passive attacks and potential degradation of image quality necessitates careful consideration of its use in

Practical applications requiring robust security and high-quality visuals.



1	0	0	0	1	1	0	**1**
							Pixel value
					0	0	1
							Secret Data
1	0	0	0	1	1	0	**0**
							Change Pixel Value

Figure 1. An example of 1-bit LSB

Proposed Method: LSB-Based Watermarking Algorithm. In our proposed watermarking algorithm, we depart from the conventional approach of utilizing the first LSB and instead focus on the third and fourth LSB for embedding data. This unconventional choice is motivated by security considerations, as it adds an additional layer of obscurity to the embedded data. Byleveraging less commonly targeted LSBs, our algorithm enhances the resilience against detection and extraction by unauthorized parties.

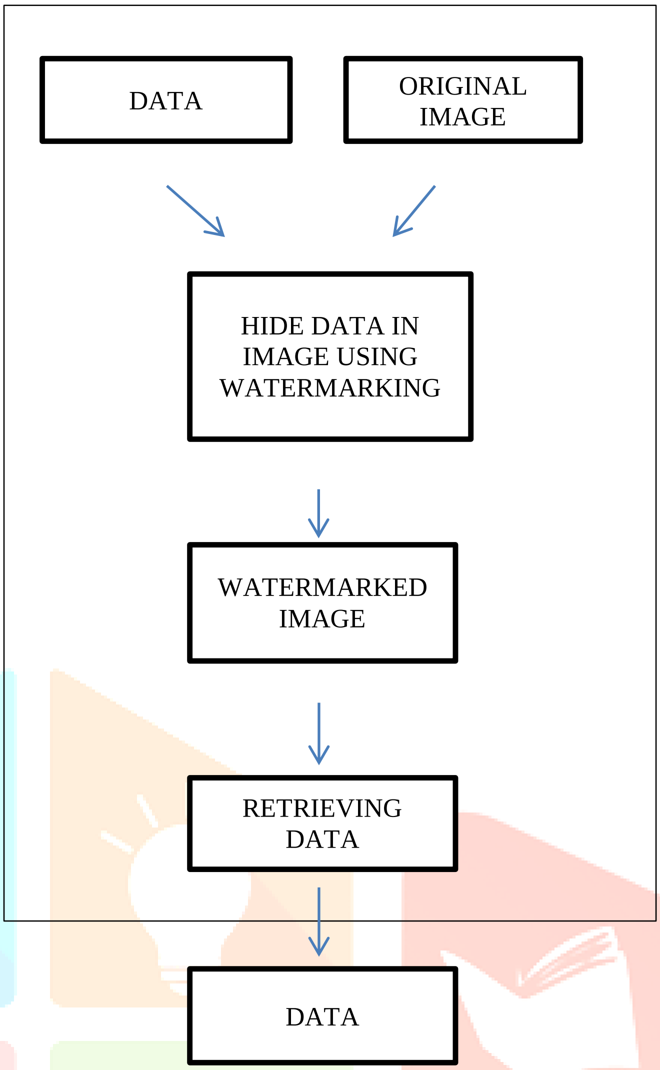


Figure 2. The framework of the proposed method.

Algorithm Framework:
The framework of our proposed method is depicted in Figure 2. Initially, we select a grayscale image as the carrier and convert the data to binary format. Subsequently, the data is concealed within the image using our novel algorithm.

Embedding Algorithm:
The embedding algorithm is implemented in MATLAB. This process involves encoding the binary data into the third and fourth LSBs of the image pixels, ensuring minimal impact on the visual quality while maximizing the security of the embedded information.

Watermarked Image Generation:
Upon embedding the data, the resulting watermarked image is obtained, ready for transmission or distribution.

Extraction Algorithm:
The extraction algorithm facilitates the retrieval of the hidden data from the watermarked image. This process reverses the embedding steps, extracting the encoded information from the third and fourth LSBs.

Conclusion:
In conclusion, our proposed LSB-based watermarking algorithm offers a novel approach to data embedding, prioritizing security through the utilization of less predictable LSBs. By deviating from conventional methods, we aim to enhance the robustness of data hiding techniques against adversarial attacks while maintaining a balance between security and perceptual quality. Through experimental validation and further

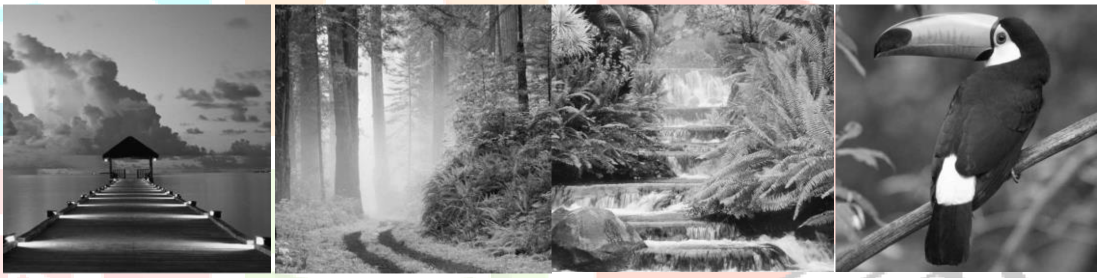
refinement, we anticipate our proposed method to contribute to the advancement of watermarking algorithms for secure data transmission and protection.

IV. RESULTS AND DISCUSSION

The experiment involved utilizing four 512x512 grayscale images as cover images for digital watermarking. The process was conducted in two phases, embedding secret data into these images. Initially, 128 bytes of data were embedded into specific pixels, modifying the third and fourth least significant bits (LSBs) of these pixels. This process was carefully executed to ensure that the resulting watermarked images did not exhibit any noticeable distortion when compared to the original images. The differences between the original and watermarked images were then analyzed by subtracting the watermarked image from the original, aiming to observe any discrepancies.

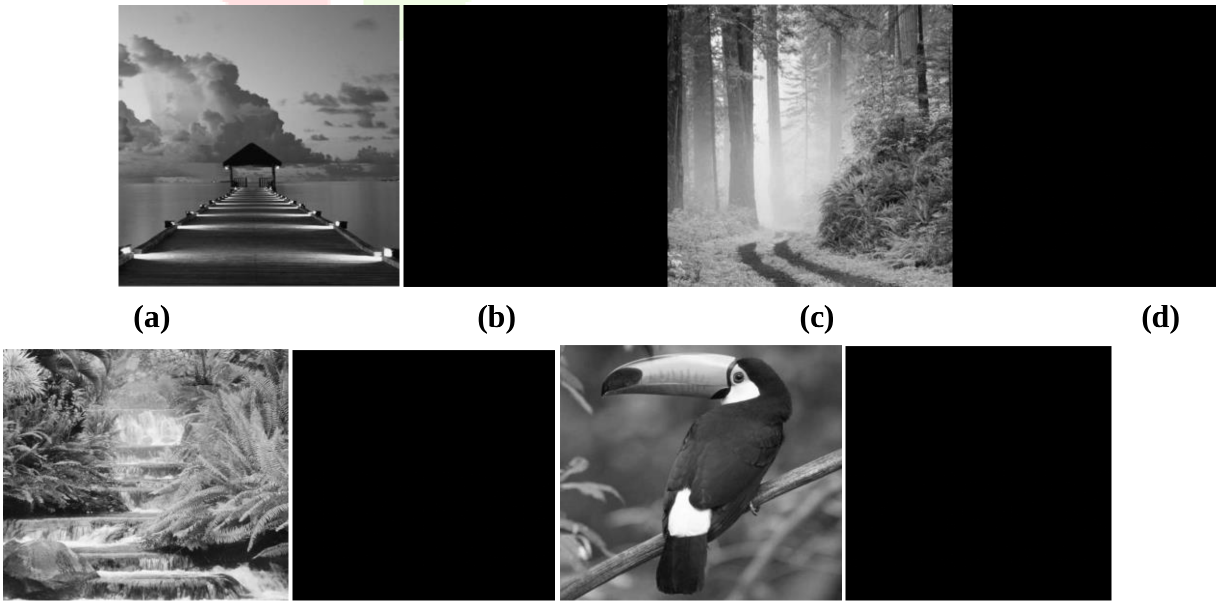
In the subsequent phase, the same procedure was applied but with an increased amount of secret data, embedding 1023 bytes into the images. Despite the larger data size, the watermarked images remained undistorted to the naked eye, and the same method of subtracting the watermarked image from the original was employed to examine the differences.

The analysis of the differences between the original and watermarked images, as illustrated in Figure 6, revealed that these differences are minimal, manifesting as nearly black images. This outcome is attributed to the modifications made to the third and fourth LSBs, with the values of these bits being 4 and 8, respectively. Consequently, the maximum pixel value difference observed between the original and watermarked images is 12. Given that a pixel value of 12 in grayscale imagery is visually akin to black, the alterations made through watermarking are effectively imperceptible, thus demonstrating the efficacy of this method in embedding secret data without compromising the visual integrity of the images.



(a) (b) (c) (d)

Figure 3: The four cover images: (a) Dock (b) Forest (c) Waterfall (d) Toco Toucan



(a) (b) (c) (d)

(e) (f)(g) (h)

Figure 4: The four watermarked images and the difference: (a)

Watermarked Dock (b) Difference of Dock (c) Watermarked Forest (d)Difference of Forest (e) Watermarked Waterfall (f) Difference of Waterfall (g) Watermarked Toco Toucan (h) Difference of Toco Toucan.

The peak signal-to-noise ratio (PSNR) is a widely recognized metric for assessing the quality of reconstruction in image compression tasks. It offers a measure of the fidelity or accuracy with which a compressed or manipulated image, such as a watermarked image, replicates the original image. PSNR is particularly valuable in contexts where an image undergoes alterations, yet it's crucial to maintain its visual integrity as close to the original as possible. The computation of PSNR is intrinsically linked to the mean squared error (MSE) between the original image (denoted as I) and its altered version (denoted as K), across all pixel values. MSE quantifies the average squared difference between corresponding pixels of the two images, providing a basis to evaluate the extent of noise or error introduced during the processing.

The formula to calculate MSE is as follows:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \end{aligned} \quad (1)$$

where MAX is equal to 255 in grayscale images, and MSE is the mean square error, which is defined as:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad (2)$$

Where I is the original image and K is the watermarked image.

The PSNR value is expressed in decibels (dB) and serves as an indicator of the reconstructed image's quality. Higher PSNR values suggest lesser distortion and better quality, indicating that the watermarked or compressed image closely resembles the original. In the context of watermarking, achieving high PSNR values implies that the watermark is embedded in such a way that it introduces minimal visible distortion, effectively making the alterations imperceptible to the human eye while ensuring the integrity and security of the embedded data.

Table 1: PSNR of the watermarked images

Image	**PSNR for 128 bytes embedded**	**PSNR for 1023 bytes embedded**
Dock	61.8427	52.7970
Forest	61.110	**52.5255**
Waterfall	61.731	52.6988
Toco Toucan	61.7138	52.5255

Based on equations (1) and (2), the Peak Signal-to-Noise Ratio (PSNR) was calculated for the proposed algorithm to assess the quality of the watermarked images. Table 1 presents the results of the PSNR calculations.

Typical values for the PSNR range between 30dB and 40dB. If the PSNR of the watermarked image exceeds 30dB, it becomes difficult for the human eye to discern differences from the cover image.

The PSNR values for the watermarked images, as shown in Table 1, indicate excellent invisibility of the watermark, with the original and watermarked images being indistinguishable to the human visual system. Specifically, the PSNR for the four images exceeds 52 when embedding 1023 bytes of secret data, while embedding fewer secret data results in higher PSNR values, as evidenced by PSNR values exceeding 61 when embedding 128 bytes.

These results underscore the effectiveness of the proposed algorithm in achieving high-quality watermarking with imperceptible changes to the original images.

V. CONCLUSIONS

The watermarking research is progressing very fast and numerous researchers from various fields are focusing to develop some workable scheme. Different companies also working to get commercial products. We hope some commercial and effective schemes will be available in future.

VI. REFERENCE

[1] Laskar, Tahera & Hemachandran, K.. (2017). A Study of Digital Image Watermarking for JPEG and PNG Images using Discrete Wavelet Transform. Indian Journal of Science and Technology. 10. 1-13. 10.17485/ijst/2017/v10i20/112176

[2] Deepika, K & Rani, Sandhya &MS, Sudha. (2021). FPGA Implementation of Digital Watermarking Using Integer Wavelet Transform and AES Techniques.

[3] Aldwairi, Khaldoon & a Hadidi, Meran. (2017). Implementation for a Digital Watermarking Algorithm on Different Image Format Types. International Journal of Advanced Research in Computer Science and Software Engineering. 7. 195. 10.23956/ijarcsse. v7i11.503.

[4] Alam, Lamia, et al. "An improved JPEG image compression algorithm by modifying luminance quantization table." International Journal of Computer Science and Network Security (IJCSNS) 17.1 (2017): 200.

[5] Dixit, Anuja, and Rahul Dixit. "A review on digital image watermarking techniques." International Journal of Image, Graphics & Signal Processing 9.4 (2017): 56-66.

[6] Bamatraf, Abdullah, Rosziati Ibrahim, and Mohd Najib B. Mohd Salleh. "Digital watermarking algorithm using LSB." 2010 International Conference on Computer Applications and Industrial Electronics. IEEE, 2010.

[7]MS, Sudha & T C, Thanuja. (2018). FPGA Implementation of DTCWT and PCA Based Watermarking Technique. International Journal of Reconfigurable and Embedded Systems (IJRES). 7. 82. 10.11591/ijres. v7. i2. pp82-90.

[8] Celik, Mehmet & Sharma, Gaurav & Saber, Eli & Tekalp, A. (2002). Hierarchical watermarking for secure image authentication with localization. IEEE Transactions on Image Processing. 11. 585-595. 10.1109/TIP.2002.1014990.

[9] MS, Sudha. (2018). DIGITAL IMAGE AUTHENTICATION (DIA)-A SURVEY. 10.13140/RG.2.2.13104.66564. MS, Sudha. (2018). DIGITAL IMAGE AUTHENTICATION (DIA)-A SURVEY. 10.13140/RG.2.2.13104.66564.

[10] Sudha, M &MS, Sudha. (2018). Randomly Tampered Image Detection and Self-Recovery for a Text Document Using Shamir Secret Sharing.

[11] MS, Sudha & T C, Thanuja. (2018). FPGA Implementation of DTCWT and PCA Based Watermarking Technique. International Journal of Reconfigurable and Embedded Systems (IJRES). 7. 82. 10.11591/ijres. v7. i2. pp82-90.

[12]Bamatraf, Abdullah & Ibrahim, Rosziati & Salleh, Mohd. (2011). Digital watermarking algorithm using LSB. 155 - 159. 10.1109/ICCAIE.2010.5735066.