Engineering and Technology Journal e-ISSN: 2456-3358
Volume 08 Issue 05 May-2023, Page No.-2176-2182
DOI: 10.47191/etj/v8i5.03, I.F. – 7.136

Securing Digital Information through Image Watermarking with LSB Algorithm: A Comprehensive Overview and Implementation using MATLAB

Anmar Aidi Shareef[1], Mohammed Ghadhban Ahmed[2]
[1,2]Electronics and Control Engineering Department, Technical Engineering College-Kirkuk, Northern Technical University

ABSTRACT: Over the years, researchers have been intrigued by the concept of information hiding, which involves concealing secrets and protecting information. Digital watermarking and steganography tools have been developed to achieve this objective, particularly in the realm of digital rights management. Digital watermark technology functions by embedding copyright information into the carrier, with the aim of safeguarding it. The digital watermark serves as a linkage between the hidden data and carrier data. In most instances, the carrier data is distorted during the concealment process, and cannot be restored to its original state. This study provides a comprehensive overview of image watermarking and the various security concerns surrounding it. The Image Watermarking technique using the Least Significant Bit (LSB) algorithm has been adopted in this work for embedding images/messages/logos into images. The study has been executed using MATLAB.

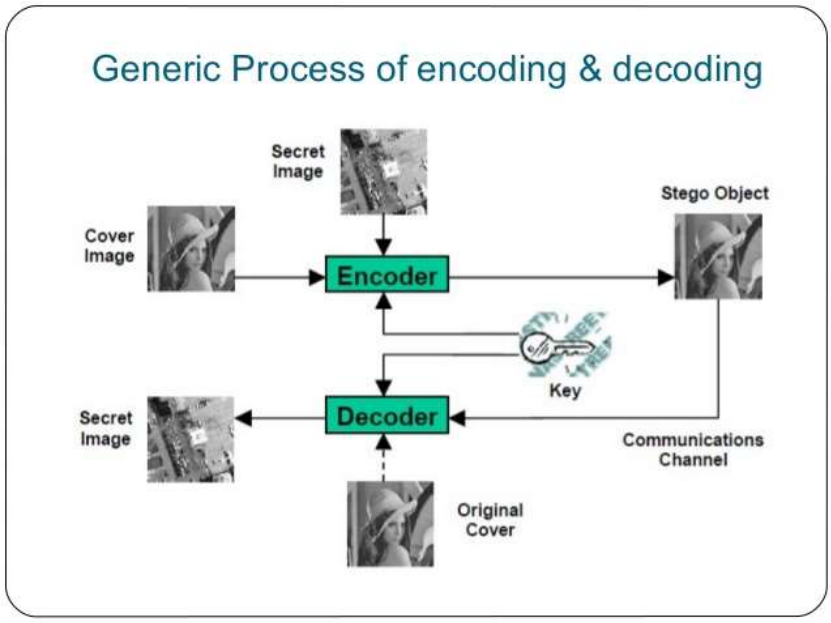
KEYWORDS: Watermarking, Digital Image

INTRODUCTION

In the digital era, digital image authentication is a significant concern because images can be easily tampered with. Ensuring the authenticity of digital images has been a pressing concern for researchers for the past few decades [1]. To address this concern, various watermarking techniques have been developed depending on the desired application. However, creating a watermarking system that is both robust and secure is a challenging task [1]. This paper provides an in-depth discussion of standard watermarking system frameworks and the standard requirements used to design watermarking techniques for different applications.

With the widespread use of the internet for communication globally, data transmission has become faster and more convenient. However, it has also increased the risk of data hacking [2]. Hackers can slightly modify confidential data and publish it online without the owner's permission. The term 'watermark' originated from the German term "Westermarck" towards the end of the eighteenth century. It was named 'watermark' because the marks resemble the effect of water on paper [3]. Digital watermarking technology is used for data security, copyright protection, and authentication. Watermarking can be applied to images, video, audio, and signals, and it consists of two sections: watermark embedding and watermark extraction [3].

In today's world, most individuals prefer to use the internet as their primary medium to transfer data worldwide due to technological advancements [2]. Data transmission has become simple, fast, and accurate, but data security remains a significant issue. Private or confidential data can be hacked in various ways, and it is crucial to consider data security. Data security involves protecting data from unauthorized users or hackers and ensuring high security to prevent data alteration [2]. In recent years, data security has gained more attention due to the massive increase in data transfer rates over the internet.



The technique of Least Significant Bit (LSB) is widely used for digital image watermarking in the spatial domain [4]. LSB replaces the least significant bits of selected pixels with the information to be hidden [4]. This method has various versions that enhance the algorithm in different ways. A secure digital image watermarking system comprises of two primary components, namely the watermark embedding and watermark extraction parts [5]. The watermark embedding process starts with pre-processing the cover image and calculating its entropy to determine the image's embedding capacity [5]. The watermark image is then encoded using an optical image encoding technique and embedded into the high entropy values of the host image, using a secret key [5]. The system further employs amplitude and phase shaping information of a laser beam to generate the watermarked image [5].

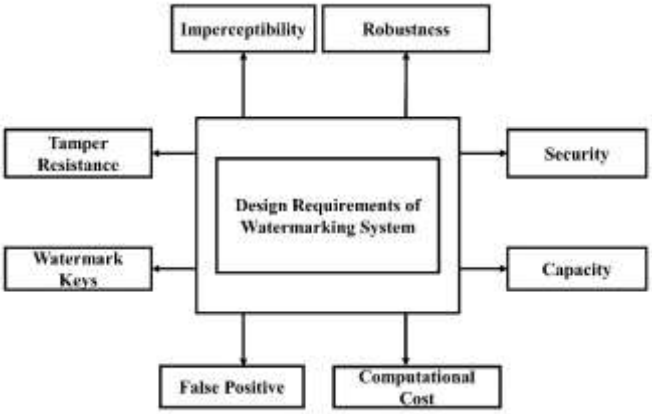
Image Watermarking Backgrounds and Frameworks

The proliferation of global computer networks, the internet, and multimedia systems has led to the easy distribution of digital content through various communication channels. To protect digital information against illegal possession, duplication, manipulation, usage, and distribution through physical transmission media during communications, information processing, and data storage, digital image watermarking has emerged as a crucial research area. Digital watermarking techniques have been developed by integrating paper configuration, quality, and quantity considerations that started with paper watermarks in 1282. [6]

Digital watermarking is widely used for enhancing security, providing confidentiality, integrity, and availability, with various innovations being incorporated since 1995. In this technique, a symbol of owner authenticity (watermark) is embedded into the host signal, and the watermark data can later be extracted. The watermark data may be visible or invisible, containing a single bit, a set of binary data, or a number of samples in the host signal. [7]

To achieve an optimal balance between imperceptibility, robustness, and capacity of a digital image watermarking technology, information entropy plays an essential role in the digital image watermarking scheme. To imitate the human visual perception system, information entropy is used through a Just Noticeable Difference (JND) model. Information entropy can be defined in terms of masking effect and can be utilized to determine the positions at which the data are inserted, minimizing perceptual distortion and providing better robustness and good imperceptibility. [8]

Digital image watermarking techniques are employed to add a watermark to multimedia data to ensure authenticity and protect a copyright holder from the unauthorized manipulation of their data. Thus, it is necessary to define the requirements or characteristics of a watermarking system, which are listed in the following subsections. These requirements evaluate the performance of watermarking systems based on applications. [9]

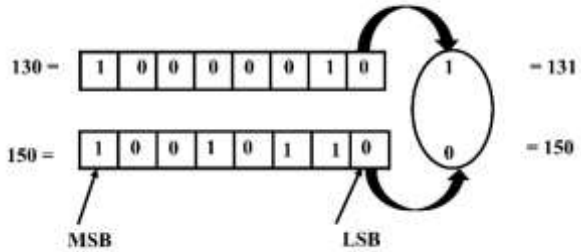


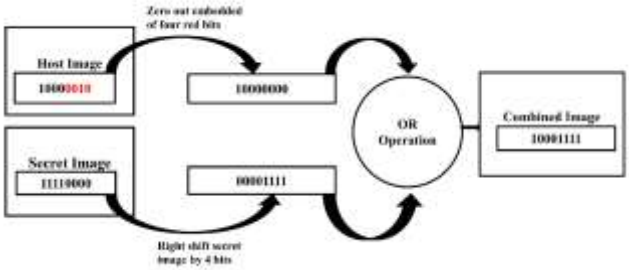
Digital Watermarking: Implementation Techniques

A digital watermark is a unique code that is inserted into an image, providing it with an added layer of authenticity and ownership. This technique has been extensively discussed and analyzed in various academic papers, which outline the optimal qualities of an effective digital watermark [10]. The key features of a digital watermark include its imperceptibility to avoid interference with the original image, statistical invisibility to prevent detection or deletion, ease of extraction to reduce computational requirements, and accuracy of detection to minimize false positives and false negatives. Additionally, the watermark should be capable of producing multiple variations, robust to various types of image manipulations such as filtering and compression, and should allow the identification of the image's true owner [10]. A watermarking scheme is illustrated in Figure 1, which involves generating a watermark W as a pseudo-random sequence to ensure statistical invisibility, extracting signal information from the original image I and embedding it into the watermark, and producing the watermarked image I' that is identical to I. For watermark detection, a suspected image J is analyzed for its signal information, a suspected watermark V is extracted based on prior knowledge of the original image I and watermark W, and a similarity measure S is performed on V and W. Finally, S is compared to a threshold, and if S exceeds the threshold, the watermark W is detected; otherwise, no watermark is detected [10].

Least Significant BIT

Spatial domain watermarking using the least significant bit (LSB) modification algorithm is a common technique [11]. This method involves altering the LSB of randomly chosen pixels to hide the most significant bit (MSB) of another, generating a random signal using a specific key. The watermark is inserted into the least significant bits of the host image and can be extracted in the same way [11]. Although this algorithm is easy to implement and simple, it may be affected by undesirable noise, cropping, lossy compression, and other factors and can be attacked by hackers setting all the LSB bits to "1" and easily modifying the embedded watermark [11]. However, this technique provides high perceptual transparency and has a negligible impact on the host image [11]. Researchers have studied modifications to the LSB technique related to the spatial domain, using bit-planes of digital discrete signals (e.g., audio or images) [11][12]. These bit-planes represent the signal as a set of bits with the same bit position in each binary number [11]. Most techniques use only one bit-plane for embedding, typically the least significant bit or eighth bit-plane, but some have used three or even four bit-planes for embedding with acceptable image quality [11]. The four least significant bits of the cover image can be replaced with the chosen bit of the secret image by using an OR operation in a specific manner [12]. This method involves converting the host image into a stream of binary bits, outputting zero in the embedded bit, shifting the secret image to the right by four bits, and then performing an OR operation on these two images to obtain the combined image [12]. Figure 1 depicts this operation [11][12]





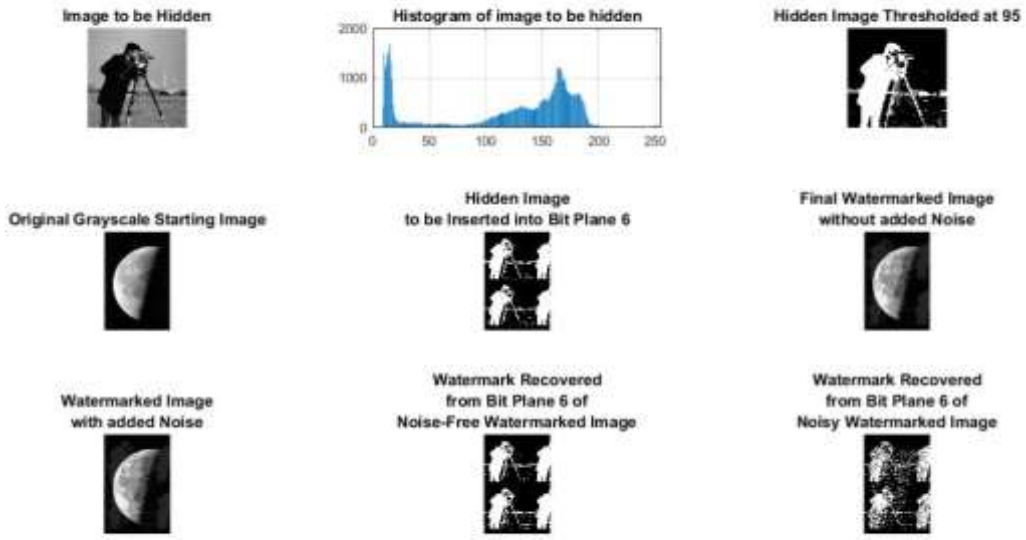
The Significance of the LSB in this paper

The embedding of watermarks into the least significant bits of a cover object is a widely used method in watermarking. However, this conventional LSB substitution technique has several drawbacks [13]. An advanced method to overcome these limitations involves using a pseudorandom number generator to select pixels for watermark embedding based on a given key [13]. This technique enhances the security of the watermark, making it difficult for hackers or unintended users to view the watermark [13]. Nonetheless, this method is still vulnerable to LSB substitution with a constant value. If the algorithm is discovered, an intermediate party can easily modify the embedded watermark [14]. Therefore, an improvement over the basic LSB substitution approach is to use a pseudo-random number generator to determine the pixels for watermark embedding based on a given "seed" or key [13,15]. This technique increases the security of the watermark by making it more difficult for intermediate parties to view it [16]. However, the algorithm remains vulnerable to LSB substitution with a constant value [13]

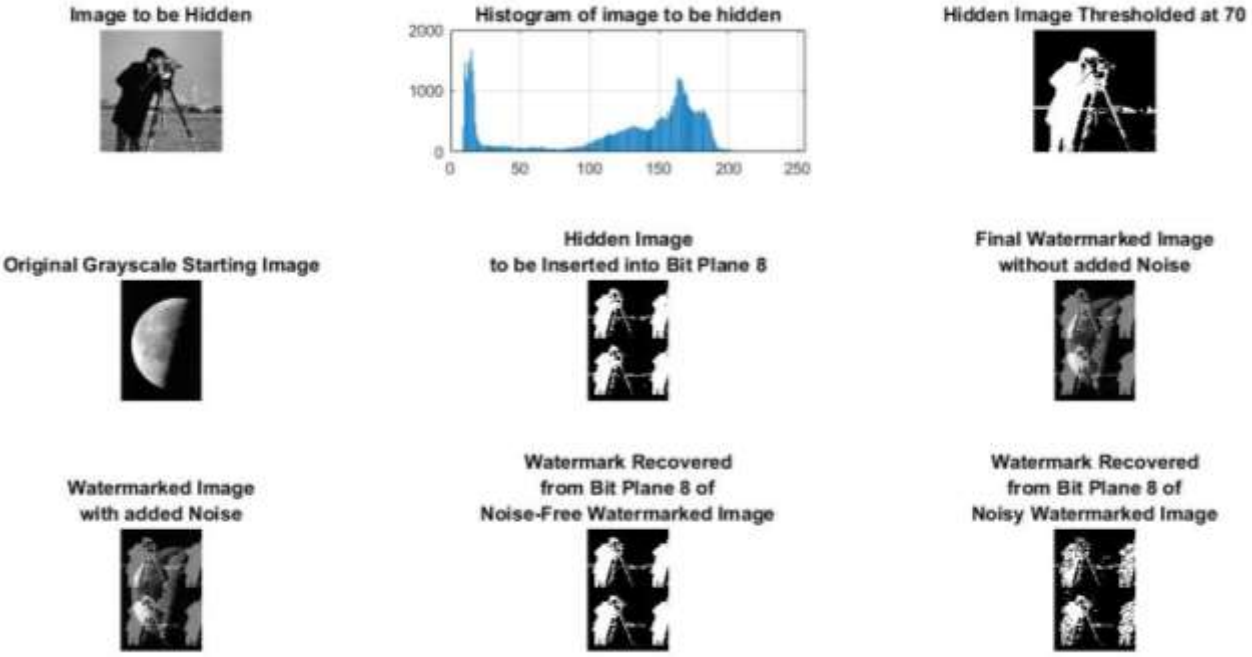
RESULTS

A watermark is a sequence of pseudo-random numbers that can be accurately detected by using linear block codes since most watermarking schemes do not utilize error correction. To enhance current methods, the purpose of my research is to develop a new watermarking technique that employs error-correction techniques. The effectiveness of the proposed watermark will be tested to ensure it meets specific criteria, with image processing and other computations performed using MATLAB. The main objective of this study is to determine whether the error-correcting watermark approach offers any advantages over traditional watermarking methods. The new watermarking scheme under development aims to address the current limitations by using error-correction techniques to improve watermark detection accuracy. By comparing the results obtained from testing the proposed technique with traditional watermarking methods, this study aims to identify any advantages of the error-correcting approach. Additionally, this research aims to investigate the trade-off between the detection accuracy and computational complexity of the error-correcting watermarking scheme.

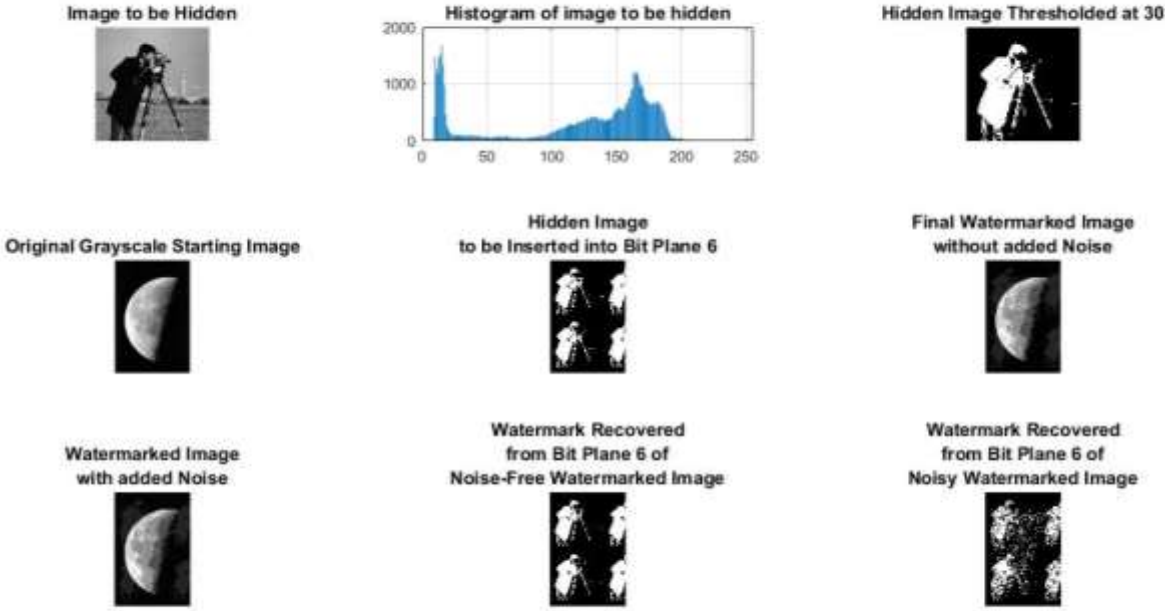
When the threshold at 95



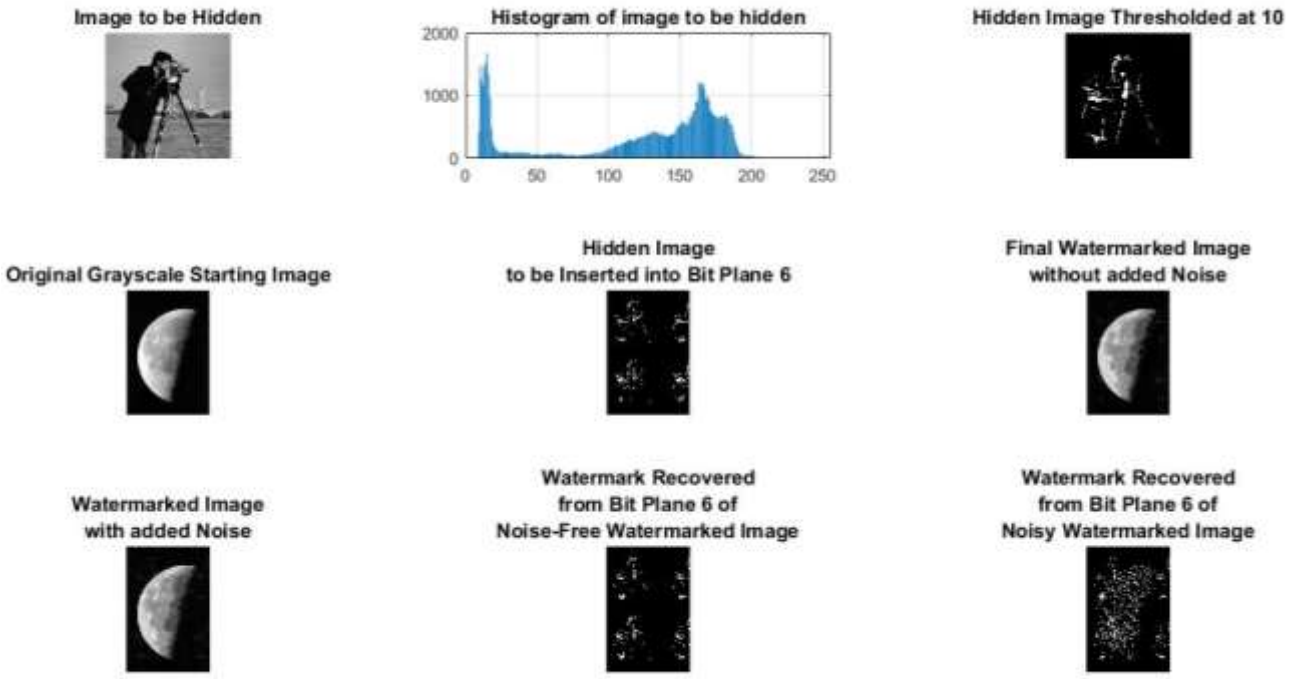
When the threshold at 70



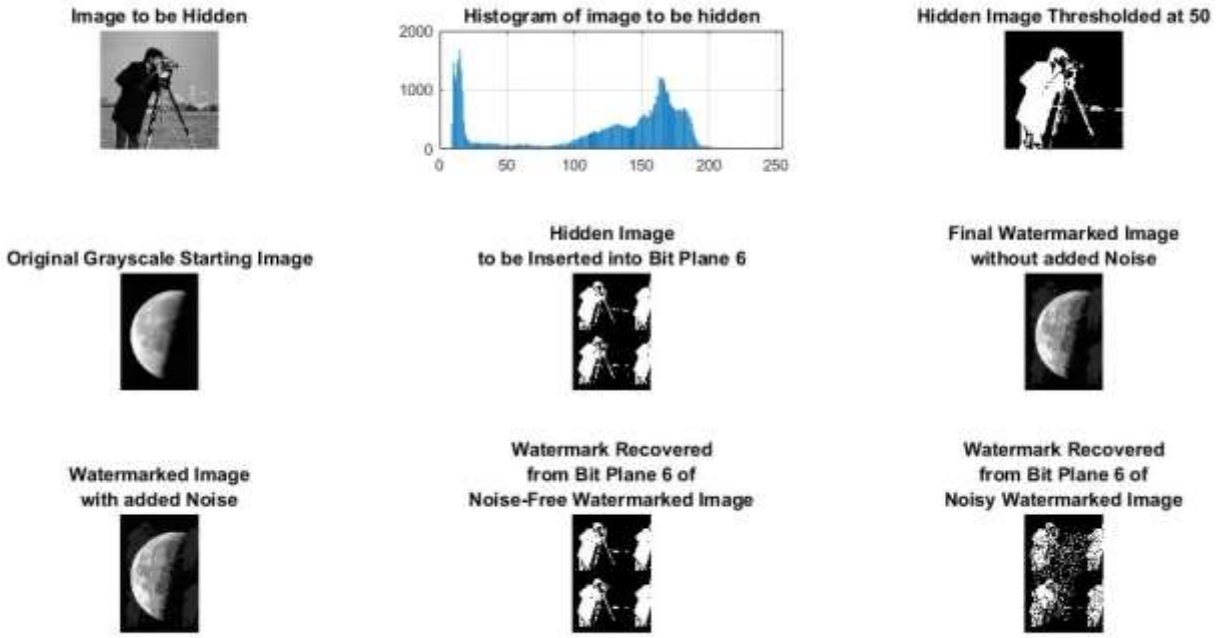
When the threshold at 50



When the threshold at 30



When the threshold is 10



CONCLUSION

The objective of this paper is to introduce a novel embedding technique that randomly conceals images/messages within the LSB of the selected pixel's component(s) by utilizing a polynomial. Compared to using a random generator, a hacker would have to predict all coefficients of the polynomial correctly to decode the embedded message. This approach can enhance the security of the watermark, as the probability

of predicting all coefficients accurately is much lower. MATLAB was used as the tool for implementing this algorithm. The primary goal of this program is to substitute the LSB of the base image with the MSB of the watermark. In the future, this technique may also be applied to other types of data and tested on various images to evaluate its effectiveness. Furthermore, this embedding scheme could be extended to include additional layers of security to prevent unauthorized access to the watermark. The proposed approach could help to improve the overall security and reliability of watermarking techniques.

REFERENCES

1. Cox, I. J., Miller, M. L., & Bloom, J. A. (2002). Digital watermarking. Morgan Kaufmann.
2. Alharbi, A., & Sohail, M. S. (2019). Watermarking: An important technique for digital image authentication. Journal of Electrical Systems and Information Technology, 6(2), 175-184.
3. Bhattacharya, S., & Debnath, R. (2018). A review on watermarking techniques. Journal of Computer Science and Engineering, 4(2), 48-58
4. Singh, N., & Kaur, G. (2021). Digital Watermarking Techniques for Secure Data Transmission: A Comprehensive Review. Journal of Ambient Intelligence and Humanized Computing, 12(9), 10251-10274. https://doi.org/10.1007/s12652-021-03552-w
5. Sharma, S., & Saini, R. (2017). Digital image watermarking: A technical review. Journal of King Saud University-Computer and Information Sciences, 29(4), 454-467. https://doi.org/10.1016/j.jksuci.2016.04.002
6. B. Huang, G. Xiang, and W. Zhou, "Digital watermarking technology and its application in image protection," in International Conference on Mechatronics and Automation, 2016.
7. F. Hartung and M. Kutter, "Multimedia watermarking techniques," Proceedings of the IEEE, vol. 87, no. 7, pp. 1079-1107, 1999.
8. X. Kang, "Just-noticeable difference based video watermarking using motion vector," Journal of Zhejiang University-SCIENCE C (Computers & Electronics), vol. 15, no. 10, pp. 875-882, 2014.
9. M. H. Shirali-Shahreza and M. Shirali-Shahreza, "A survey of digital image watermarking techniques," in International Conference on Computer and Automation Engineering, 2010.
10. Kaur, M., & Kaur, P. (2017). Digital watermarking: A review. International Journal of Computer Applications, 170(10), 6-11.
11. R. Chandramouli and N. Memon, "Digital Watermarking," Proceedings of the IEEE, vol. 87, no. 7, pp. 1167-1180, 1999.
12. L. Wang and X. Wang, "A novel watermarking algorithm based on digital image
13. Lian, X., Zhang, D., & Yang, X. (2006). A robust image watermarking scheme in wavelet domain based on chaos. Signal Processing: An International Journal, 86(12), 3653-3663
14. Khalaf, K. S., Sharif, M. A., & Wahhab, M. S. (2022). Digital Communication Based on Image Security using Grasshopper Optimization and Chaotic Map. International Journal of Engineering, 35(10), 1981-1988.
15. Sharif, M. A., & Tan, X. (2018, March). IPMC flow sensor exploiting self-generated vortices. In *Electroactive Polymer Actuators and Devices (EAPAD) XX* (Vol. 10594, pp. 269-277). SPIE.
16. Sharif, M. A. A. (2022, April). Electro-thermally controllable twisted coiled actuators (TCA) using nylon line. In *Electroactive Polymer Actuators and Devices (EAPAD) XXIV* (Vol. 12042, pp. 376-381). SPIE.