Spatial-Fields Techniques for Image Authentication

***Abbas Mones Faraj Thajeli, **Hayder Adnan Saleh, #Marwa Jamal Hadi**

*Department of Computer Techniques Engincering, Imam Alkadhim University College,
Baghdad, Iraq
orcid:0009-0008-4082-1731
** Baghdad Directorate of Education, Rusafa III, Ministry of Education,Baghdad, Iraq
Orcid:0000-0003-3672-6287
# Diyala Education Directorate, Ministry of Education, Iraq
Orcid: 0009-0003-0400-843X

DOI:10.37648/ijps.v20i01.018

[1]Received: 07/08/2025; Accepted: 19/09/2025; Published: 09/10/2025

Abstract

Digital watermarking is a technique used to hide information within digital content (such as text, images, videos, or audio files) that can be used to identify the owner of a work, verify authenticity, or protect copyright. It resembles a traditional watermark on paper, but it is embedded within the digital data to make it unnoticeable to the average user. In the proposed method, An optimal color bit is embedded in binary watermark subbands. This leads to the creation of the least significant bit (LSB), which conceals a most significant bits in the samble by using the least preferred pixels. The pixels can be randomly selected using a key. This methodology presents a streamlined and efficient solution for digital watermarking based on the least significant third and fourth bit (LSB) techniques. Compared to the traditional LSB method, the proposed algorithm is more effective for data embedding within digital images. Show that the tan enhancement in the watermarked image is improved by the autcome. To use LSB-based image watermarking, load both the host image and the watermark that needs to be protected. Next, replace the LSBs of the host image with the watermark bits. The model must endure deliberate attacks while preserving superior image quality, assessing image authenticity, and detecting any tampering. A range of consistency criteria and watermark removal assaults are utilized to assess the methods within a pilot setting.The results show that the model has high attack resistance and supports discrete watermarking..

Keywords : *Watermark; Binary Image; Spatial Domain; Authentication; Least Significant Bit (LSB); PSO; Color Images.*

1. Introduction

Image authentication has become essential in many practical applications across government institutions, private companies, and scientific research due to the ease with which digital images can be manipulated using advanced image editing software. As a result, image authentication has emerged as a significant field of study and an effective method for preserving the integrity of digital images[1]. The development of global identity management and tracking technologies, as well as image authentication, has received significant attention as an important issue to be addressed in the future. These systems aim to enhance trust by properly verifying data [2]. A watermark utilazid to embed information within digital content (image, text, audio, or video) using software such as Photoshop. The watermark must be both imperceptible and durable. The durability of a watermark is measured by its success in recovering it from the recovered content, which may contain various types of noise and compression artifacts[3]. The primary reason for needing image authentication is the increasing number of altered images. To verify the integrity of digital media content against alterations, digital watermarking technology is employed in image authentication applications to

[1] *How to cite the article:* Thajeli A.M.F., Saleh H.A., Hadi M.J. (October 2025); Spatial-Fields Techniques for Image Authentication; *International Journal of Professional Studies*; Jul-Dec 2025, Vol 20, 244-254; DOI: http://doi.org/10.37648/ijps.v20i01.018

detect tampering in modified images [4]. Recent studies have demonstrated that digital watermarking is among the more effective technologies for sample authentication. It can be categorized as soft, semi-soft, or robust ,where it is used to improve the encryption process through the embedding of watermarks [5]. When images or video files are tampered with, soft watermarks can be preserved and replaced as needed. This is possible even with slight alterations, whether inadvertent or deliberate. This accomplishment is admirable. Therefore, watermarking techniques can be used to encode/decode images, text, and video. [6, 7].The binary watermark bits are embedded in the sub-bands of the ideal colors after the PSO stage, which produces the least extreme value. LSB which utilizes the least advantaged bits of all pixels in an image to mask the much more important bits. It is possible to select pixels at random using a key. To use LSB-based image watermarking, load both the hosting image and a watermark that needs to be protected, then substitute the host image's LSB with the watermark bits. These processes result in the production of a watermarked image that must be able to survive a deliberate attack to gather high- quality, as well as be able to identify tampered areas in the image and evaluate its authenticity.

2. Related Work

Numerous studies have been conducted. In this section, we will review several important studies in this field as follows:

- In 2018 [8], the authors proposed several methods for ensuring the authenticity of images. These include currently used image authentication methods: cryptographic authentication, watermark authentication, and strong image hash authentication. In this paper, multiple methods for authentication of image and multimedia applications are summarized.
- · In 2018 [9], the authors proposed a fundamental approach to information-hiding techniques. They discussed whether information propagation should be contained or hidden. The proposed approach obscures the carrier image using the LSB algorithm. The success of the results depends on the efficiency of the information stored in them. The results demonstrate the availability of a sophisticated processing method using the LSB algorithm while maintaining the clarity of the entire image.
- In 2018 [10], a dual-image watermarking scheme was proposed to protect digital LBP-based documents. The proposed method divides the host images into three overlapping blocks. Then, using the secret watermark bits, an XOR vector is generated, and the XOR operation is performed using the system vector. By creating a shared secret key in both images, an authentication token can be embedded. The recipient can retrieve the watermark and authentication tokens from the cover image. Once the re-authentication token is generated and the authenticator is verified, Compared to its opponents, the proposed method will be more effective.
- 2019 [11]: This study presents a multi-image authentication method based on the density equation. Blocks are first extracted from multiple plain images by evaluating their spatial frequency coefficients. A statistically significant phase-encoded block is then generated using a random density mask and a logistic map sequence. Using Fresnel diffraction, a real-valued signal is obtained by transforming the complex-valued amplitude. Using the density information, the connection can be reconstructed. Only when the image is computed as a nonlinear relationship between statistically significant subblocks can it be verified. For the first time, multi-image optical authentication using the density equation technique has been implemented. Using simulations, the feasibility of the proposed approach has been demonstrated.
- In 2020 [12], this study showed that the inclusion of four-bit coding for both color channels achieved an average signal-to-noise ratio (PSNR) of 33.260 dB, with adequate detection. The researchers proposed including Authentication encoding in the first two pre-color channels and adjusting the remaining channel to address grayscale distortion.

- In 2020 [13]. In this paper, a direct method is utilazid to convert integer values of image pixels to values of integer coefficients, instead of the floating-point parameters that traditional wavelet transforms can provide.This direct relationship contributes to enhancing the quality of the processed image by reducing the necessity for rounding operations on floating-point parameters and obtaining accurate results. One method used for data authentication is the parity bit approach. Specifically, a type of fragile watermarking is implemented by applying three hidden parity bits to each block of a picture that has been separated into non-overvlapping pieces.Therefore, any modification of the pixels in the block may result in a violation of the adopted (even) parity condition, indicating the presence of tampering. The fragile watermarking process is performed by modifying the LSBs of the frequency coefficients specified according to the pre-established even parity condition. Therefore, the proposed method is effective.

- 12. In 2020 [14]. This study proposes the use of the DnCNN architecture as a denoising tool, forming the basis for evaluating the robustness of the algorithm against modern neural network attacks. To create a more practical solution, this system utilizes single-channel (grayscale) image processing, with the flexibility to expand to three-channel (color) processing, thereby enhancing the watermark's capacity. Moreover, the system can be tailored for video applications, treating each frame as a standalone image.

2.1 .Digital Watermarking

It is an effective means of protecting to providing mechanisms for verifying the data integrity of digital image files. This technology involves embedding a particular pattern in the host signal to guarantee that specific information, such as the owner's identity or authorized user data, cannot be revealed or altered.It has directly tied to the data. [15]. The process of embedding data into a multimedia department is called a label so that the object, whether an image, audio, or video, can be identified or later extracted for verification, for example. If the object is copied, it also contains the knowledge in the copy. [16].

A visible watermark contains details of an image or video. The data is usually a texture or logo that identifies the medium. When a television broadcaster's logo is affixed to a corner of a video, it is considered a visible watermark for that videoWhen applied to digital data such as music, video, or photos, invisible watermarking is not regarded as (with the potential for detecting the hidden information). Invisible watermarks make an important contribution to hinder unauthorized copying of digital media content. Digital watermarks are transmitted within a digital signal as a hidden message using 2 parties. Another utilazed of invisible watermarks is to add descriptive details to digital images [17, 18]. Mohanty identified three components in any watermarking algorithm:

Watermark retention.Encryption algorithm for insertion.Decryption module. Each owner has a unique watermark. To differentiate between buyers of multiple copies of the same format content, the owner may use various watermarks. The symbol 1, the S sign, generates 1' using a humorous encoder.The watermarking process consists of four main stages: embedding, extraction, distribution, and decision-making. In the embedding stage, To get it ready for embedding, the image that will be watermarked undergoes preprocessing. Usually, this procedure entails changing the picture to the intended modification. In the distribution stage, the protected, watermarked image is distributed via digital channels (on websites or broadcast channels). During the extraction phase, attempts are made to retrieve the disseminated image's embedded watermark or signature.. At the decision-making stage, any discrepancies or modifications that may have occurred to the image during distribution are examined, and a comparison between the extracted and original watermarks is made. A common method for doing this is to calculate the Hamming distance.

$$HD = (W \bmod . W) / \|W\|$$

Wehre Wmod is the modified vector
W is the original vector
||W|| is the norm (magniude) of vector W
The similarity between Wmod and W is calculated by comparing the HD value to a threshold T. [19,20].

2.1.1. Reviw of (LSB) techniuqe

There are 2 majore department, the Spatial ,and the Frequency domain, in which watermarks are embedded in the unaltered data. In the second domain, each piece of information is compressed by representing it with a set of parameters, and techniques divide the signal into parts, factoring in account the linkage of pixels in gap and the hypothetical understanding of another domine information. The discrete wavelet transform (DWT) ,and the discrete cosine transform (DCT) are considered two popular methods for discrete cosine transform (DWT) [19]. DWT is a hierarchical image decomposition technique that is particularly important for handling non-motionless signals. This transformation is particularly important for processing non-stationary signals, as it is based on waves with a finite duration and variable frequency. The transform is based on finite duration and variable frequency wavelets. The wavelet provides spatial and frequency information at a fixed resolution in the time domain, using a consistent window shape. The high-frequency signal exhibits widespread distribution, and DCT fluctuates as well. In the low-frequency part, there is an impressive rate gap that can be extracted from the signal [22]. In spatial domains, watermarks are embedded into the original data by directly modifying pixel values. Various techniques exist for embedding watermarks in the spatial domain, such as local binary pattern (LBP) and least significant bit (LSB) [23, 24].

The basic idea behind LSB technology is a simple principle: embedding information into the cover image. The pixels within the cover image are altered via bits of the confidential message. despit the degit is embedded in the earliest 8 bytes of the network, it only requires 1 to 4 bits to be altered, depending on the nature of the embedded letters [25]. On rate, merely fifty percent of the bits in an image are required to embed a hidden message in a cover image. Due to the low quality of watermarked images based on less than 4 LSB bits, modifications to a pixel's LSB result in subtle alter in the color intensity of the image. These alter are imperceptible to the human visual system. However, these modifications can be detected by a passive attacker who performs a very simple process to extract the changed bits [26]. illustration, Figure 1 exhibits a 1-bit LSB. In Figure 1, the pixel merit of the cover image is 141 $(10001101)_2$, and the secret data is 0. For a 1-bit LSB, the transform pixel merit of the cover image is 140 $(10001100)_2$. The LSB technique allows one bit to be stored per pixel. If the cover image is 256 × 256 pixels in size, It can hold 8,192 bytes, or 65,536 bits, of embedded data in total [25].

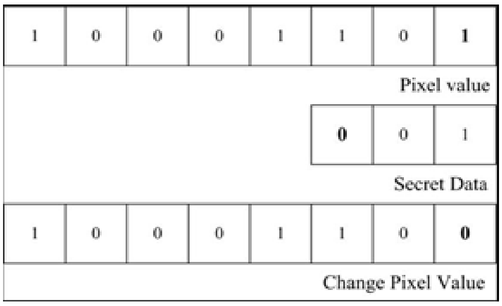

Figure (1): An example of 1 bit LSB [23]

3. Materials & Methods

In the proposed method, verify image authentication. Through a kit of urgent stages that integrate and labor in harmony, a new watermarking algorithm has been proposed. Based on the LSB technique, the proposed watermark image is a reversed value, and it is embedded using a different order than traditional LSB. This is to meet specific security requirements. It is not expected that the hidden watermark image will be rearranged in a different order and inserted as shown in Figure 2, which demonstrate the general framework of the animated procedure. Firstly, select the watermark image and cover, also select which is a grayscale image, and then their values were inverted and converted to binary form. Secondly, the watermark is embedded in the cover using the proposed algorithm. Hence, we obtain the image containing the watermark. Finally, the recipient will retrieve the watermark again. Using an extraction algorithm.

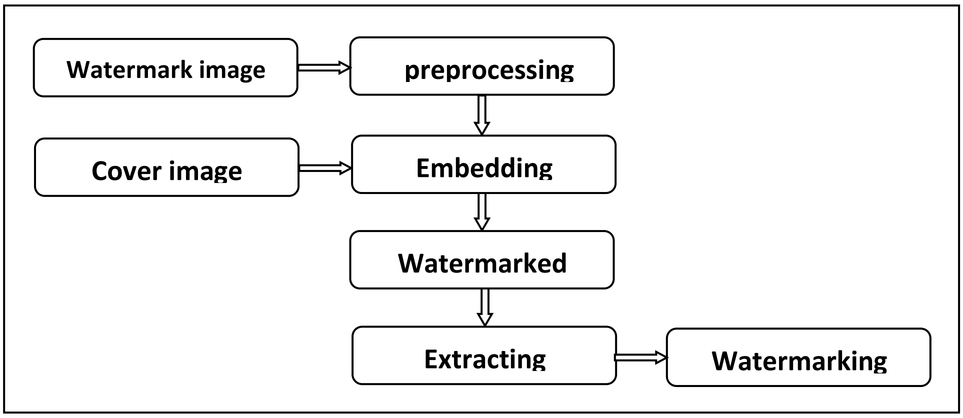

Figure (2): proposed method

3.1 Embedding phase

In this segmant, proposed an embedding techniqe to hide the sample, which was based on the LSB technique. This can be summarized by stating that the bits move from right to left. The numerical value represented by the bit increases. The first bit from the right represents the number 1 for us, while the last represents the number 128. Therefore, as we move to the right, the numerical value represented by the bit decreases. The bit has little effect on the data; for instance, reversing the first bit's value for one pixel (or all) won't make a big difference. If the intensity of the red color in that pixel was 127, the value will become 126 after changing the bit. The first is from 1 to 0, and the human eye won't notice the change, so it's called the least influential bit. The more we move to the right, the less important the bit becomes.The proposed algorithm is applied in two main stages. Firstly, pick the watermark image, which is a grayscale image, then convey it to the binary form values, and then invert it for more security. In the second stage, we will read each pixel in the cover image, extract its binary color, and then change the value of the least significant bit; specifically, we suggest altering the second least (2nd LSB) of each color to match one of the bits from the watermark image. The second pixel from the left, for example, will contain the first 3 bits of the watercolor image, where each color contains one of the bits of the image. The mechanism of the algorithm is shown in the figure (3), and Algorithm (1) illustrates the process of the embedding algorithm.

Algorithm 1: Embedding Algorithm

```
Inputs:
The Cover Image & Watermark Image.
Output:
Watermarked Image
Begin
Step1: Read Cover image image $O_p$ & Watermark gray scale image $W_p$
Step2: Resize the Op to [1024 1024] and Wp to specific size.
Step3: Convert the $W_p$ to binary values.
Step4: Inverse the $W_P$.
Step5: Read all pixels in the cover image and extract the color pairs in it.
Step5: limitation the harmonize of the image data isertion point.
Step6: Embedding the length of the $W_P$ in the 2nd LSB.
Step7: in these step Get the watermarked image
Step8: Save the Image.
Step9: End .
```

3.2 Extracting phase

In this section, the watermark bits are converted into symbols that are displayed as text as a watermark. We will describe the steps of the extraction algorithm. After receiving the watermarked image, the extraction process begins with the second (LSB) of per of the 16 pixels, starting from the specified coordinate, and continues until we have processed all 16 pixels to extract the span of the watermark image. Next, the digits of copies included by the sender is determined. Based on this information, which of the available copies can be selected to display, and the watermark embedded in the second LSF at the specified locations, if any, can be obtained. The algorithm then checks if the X-coordinate is even, subtracting 1 from it X; if the X-coordinate is odd and adding 1 to X. The watermark bit is then obtained, which is then inverted. Finally, Algorithm 2 illustrates the process of the Extracting Algorithm.

Algorithm 2: The Extracting Algorithm

```
Input:
Watermarked I.
Output:
Watermark I.
Begin
```

Step1: Reading the embedded watermark from the image.
Step2: Get the watermark data from the 2rd LSB .
Step3:
Step4: Inverse the W_p image
Step6: Convert to grayscale image.
Step10: Save the Image.
Step10: End .

4. Results & Discussion

In this segmant, research findings exihbit the prpductivity and triumph of the digital watermarking embedding technique, especially at the receiving end, where the watermark images are embedded within a host image. In the practical aspect of the handeled strategy, per color image is 256×256 bits in size. file arrangement with diverse texture, the binary watermark with the size of 128×128 (24-BMP), to begin with the research necessity to deliberate a host image, which is broadly in RGB form; Figure (3) shows the binary image, which makes it a watermark, while Figure (4) shows the innovative image and the original image's histogram. post that, the algorithm got the watermarked images. To distort, we removed the watermark from the original image to compare the results with the innovative images. The second time, the same secret data, 1024 bytes in size, was embedded within the images, and watermarked images were obtained without noticeable distortions. Next, for comparison, we removed the watermark from the original image. shown in figure (5).

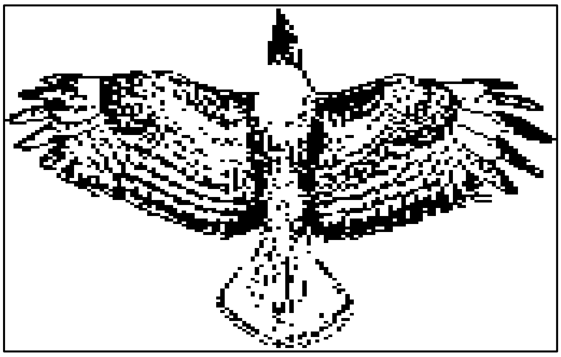

Figure (3):The watermark binary image

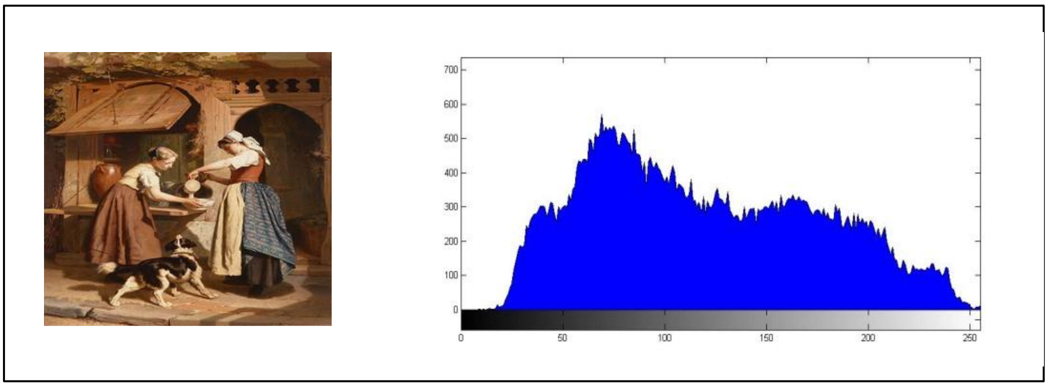

Figure (4): Histogram of original image

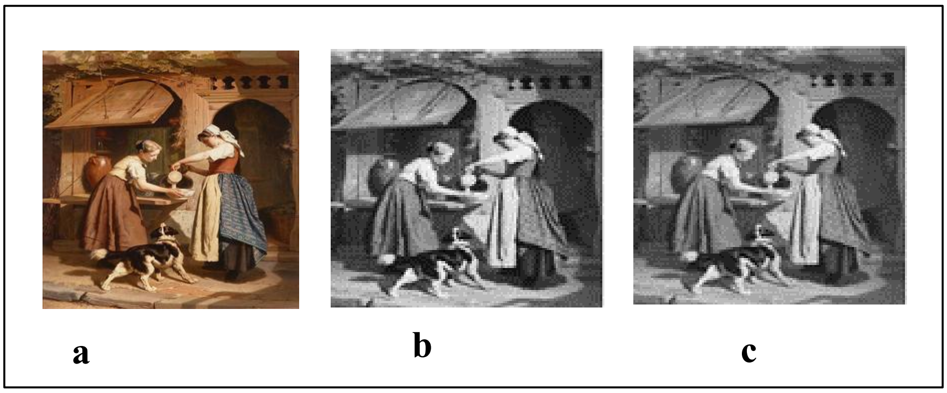

Figure (5): display findings appled LSB algorithm(a) innovatuve image (b) gray scle image, (c) Watermarked Image

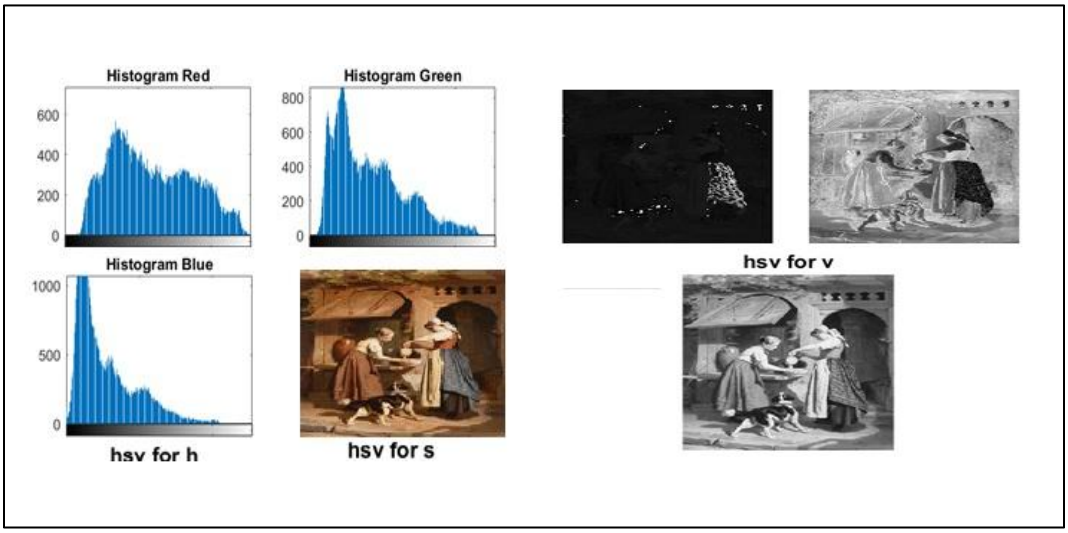

Figure (6): Histogram after LSB stage

Note that there is no variation midway the innovatuve and watermarked images. This indicates that no distortion occurred in the watermarked images. We obtained a satisfactory outcomes and calculated the peak signal-to-noise ratio (PSNR). The PSNR value was utilized to assess the watermarked photos' quality. The term PSNR, It is commonly utilized as an indicator for image distortion recovery quality.[4], is used. It is without difficulty delineated defined by the mean square error (MSE) of two mXn images, I and K, where one image is approximately the noise of the other. The MSE is delineated according to Equation (2), while the PSNR is calculated using Equation (1).

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

where MSE is the mean square error and MAX is equal to 255 in grayscale images, 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 K is the watermarked image and I is the original image.

depend on Equations (1) and (2), the resercher estimate the signal-to-noise ratio (PSNR) of our recommended algorithm to evaluate the standard of watermarked images generated by the proposed algorithm. The findage shown in Table (1) reveal the calculated SNR results. Based on Equations (1) and (2), the rechersh calculate the mean square error (MSE) and signal-to-noise ratio (PSNR) of our suggested approach for determining watermarked image quality. Table (1) present the calculated results. The method uses the LSB technique to encrypt the message image inside the cover imagery with watermarking, and then it is decrypted using the same technique to restore the original form of the cover image and message image. For image security, we employ the spatial domain approach (LSB), which is a straightforward, easy, and more efficient method. The bulk streamlined path of image watermarking may be found using this technique by first determining the significant bit head from 1 to 8 and then revealing the associated PSNR and MSE.

Table 1 Watermarking MSE & PSNR Performance data

Image no.	Orginal omage		Watermarked image	
	MSE	PSNR	MSE	PSNR
1	0.0012	099.254	0.2056	067.0760
2	0.0004	098.215	0.0095	080.4077
3	0.0000	104.124	0.0095	080.4077
4	0.0008	102.136	0.0076	081.4062
5	0.0068	087.364	0.0095	080.4417
6	0.0025	091.478	0.0034	084.8493
7	0.0205	065.145	0.0000	099.0000
8	0.0046	086.012	0.0034	084.8493

Figure (7) shows the performance analysis of MSE and PSNR from Table (4.19).

When the number of times the algorithm is trained increases, the MSE value will decrease to approach zero, thus obtaining better results in general. The opposite is true for PSNR, which indicates that the algorithm achieves satisfactory results in achieving the research objectives

.

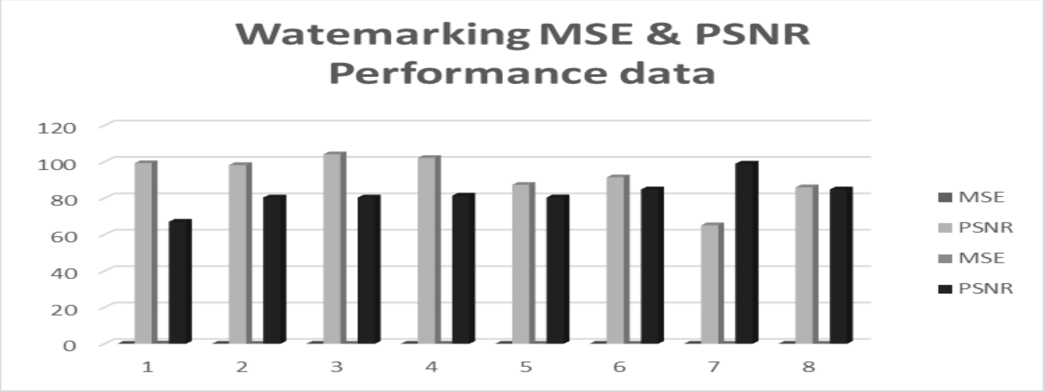

Figure (7): Display an Analysis of Performance of MSE and PSNR from the Table (1).

5. Conclusions

To protect images and preserve copyright from infringement, watermarking technology has been used. Due to its broad scope, it is the subject of extensive research by commercial companies seeking to dominate it. This field combines other cryptographic techniques with watermarking. Based on the requirements of image owners and their desired outcomes, To enhance the security level, a fitting algorithm can be opted to generate the watermark. The proposed method effectively hides information by using a watermark image. In this methodThe watermark image gets embedded into the host image through the use of the LSB modulus process. The LSB algorithm has proven effective in finding low-level regions utilazid to hide the watermark..

References

Abdullatif, M., Jalab, H., Obaidat, M., & others. (2013). Properties of digital image watermarking. *Proceedings of the IEEE 9th International Colloquium on Signal Processing and its Applications*. IEEE.

Al-Otum, H. M. (2014). Semi-fragile watermarking for grayscale image authentication and tamper detection based on an adjusted expanded-bit multiscale quantization-based technique. *Journal of Visual Communication and Image Representation, 25*(5), 1064–1081.

Awad, J. H., & Majeed, B. D. (2021). Image watermarking based on IWT and parity bit checking. *Iraqi Journal of Science*, 2726–2739.

Bamatraf, A., Ibrahim, R., & Salleh, M. N. B. M. (2010). Digital watermarking algorithm using LSB. *2010 International Conference on Computer Applications and Industrial Electronics*, IEEE.

Chen, C. (2018). Study on information hiding technology based on digital image. *IOP Conference Series: Materials Science and Engineering, 394*(3). IOP Publishing.

Chuang, J.-C., & Hu, Y.-C. (2011). An adaptive image authentication scheme for vector quantization compressed image. *Journal of Visual Communication and Image Representation, 22*(5), 440–449.

Cox, I. J., & Miller, M. (2002). The first 50 years of electronic watermarking. *EURASIP Journal of Applied Signal Processing, 2002*(2), 126–132.

El-Shazly, E. H. M. (2012). *Digital image watermarking in transform domains* [Unpublished manuscript].

Fridrich, J. (n.d.). *Robust digital watermarking based on key-dependent basis function* [Unpublished manuscript].

Hong, W., Li, X., Chen, S., & Lin, Y. (2020). A color image authentication scheme with grayscale invariance. *IEEE Access*.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Kashyap, N., & Sinha, G. R. (2012). Image watermarking using 3-level discrete wavelet transform (DWT). *International Journal of Modern Education and Computer Science, 4*(3), 50–56.

Khatua, S., & Rana, D. (n.d.). *DWT based image watermarking for information security* [Unpublished manuscript].

Li, M., Xiao, D., & Zhang, Y. (2016). Attack and improvement of the fidelity preserved fragile watermarking of digital images. *Arabian Journal for Science and Engineering, 41*(3), 941–950. https://doi.org/10.1007/s13369-015-1880-x

Marakumbi, P., & Khanapuri, J. V. (2018). Particle swarm optimization. *International Research Journal of Engineering and Technology (IRJET), 5*(12), 2395–0056.

Mohanty, S. P. (1999). *Digital watermarking: A tutorial review*. Retrieved from http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999Mohanty.pdf

Mousavi, S. M., Naghsh, A., & Abu-Bakar, S. A. R. (2014). Watermarking techniques used in medical images: A survey. *Journal of Digital Imaging, 27*(6), 714–729. https://doi.org/10.1007/s10278-014-9710-3

Muyco, S. D., & Hernandez, A. A. (2019). Least significant bit hash algorithm for digital image watermarking authentication. *Proceedings of the 2019 5th International Conference on Computing and Artificial Intelligence*.

Nikam, B. D., & Gaikwade, S. B. (n.d.). *Review on digital watermarking techniques* [Unpublished manuscript].

Pal, P., Jana, B., & Bhaumik, J. (2019). Watermarking scheme using local binary pattern for image authentication and tamper detection through dual image. *Security and Privacy, 2*(2), e59.

Sarkar, R., Hemavathy, R., & Shobha, G. (2012). *An invisible watermarking technique for image verification* [Unpublished manuscript].

Singh, B. K., & Dua, T. (2015). Image authentication using digital watermarking. *International Journal of Computational Engineering Research (IJCER), 5*(4), 2250–3005

Sui, L., Zhang, Q., Wang, Y., Zhang, M., & He, W. (2019). An optical multiple-image authentication based on transport of intensity equation. *Optics and Lasers in Engineering, 116*, 116–124. https://doi.org/10.1016/j.optlaseng.2018.12.015

Tao, H., Chongmin, H., Li, X., & others. (2014). Robust image watermarking theories and techniques: A review. *Journal of Applied Research and Technology, 12*(1), 122–138.

Yazdi, H. S. (2025). CSRWA: Covert and severe attacks resistant watermarking algorithm. *International Journal, 82*(1), 1027–1047.

Zhao, X., Bateman, P., & Ho, A. T. S. (2011). Image authentication using active watermarking and passive forensics techniques. In *Multimedia analysis, processing and communications* (pp. 139–183). Springer, Berlin, Heidelberg.

About Authors

Abbas Mones Faraj Department of Computer science, Software Engineering,Abbas Mones Faraj was born in baghdad, Iraq, in 1975. He received the B.S. degree in Computer science from the Mustansiriyah University , in 2000, and the M.S. degree in Software Engineering from Ferdowsi University of Mashhad, Iran.in 2017. He is currently working toward the Ph.D. degree in Computer Engineering at Islamic Azad University, Isfahan, Iran. His Scopus Author ID is 5869630780.

Hayder Adnan Saleh received a Bachelor's degree in Computer Science from Ibn Al-Haytham College of the Pure Sciences / University of Baghdad in the year.2007, holds a master's degree from the Department of Computer Science at the College of Education, Al-Mustansiriya University in 2021. I am currently working as an in the Third Rusafa Directorate of Education, the Iraqi Ministry of Education and Scopus ID: 57219255311

Marwa Jama Hadi obtained his Bachelor's degree in Computer Science from the College of Education in 2008, and his Master's degree from the Department of Computer Science at the College of Education at Al-Mustansiriya University in 2023. I currently work in the Diyala Education Directorate of the Iraqi Ministry of Education and ORCID: 0009-0003-0400-843X.