IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

**Traitement du Signal**
Vol. 40, No. 5, October, 2023, pp. 2019-2027
Journal homepage: http://iieta.org/journals/ts

# A Robust Algorithm for Digital Image Copyright Protection and Tampering Detection: Employing DWT, DCT, and Blowfish Techniques

Ahmed S. Salama[1,2], Rasha Shoitan[3], Mohamed S. Abdallah[4,5*], Young Im Cho[6], Ahmad M. Nagm[2]

[1] Electrical Engineering Department, Faculty of Engineering & Technology, Future University, New Cairo 11845, Egypt
[2] Department of Computer Engineering and Electronics, Cairo Higher Institute for Engineering, Computer Science and Management, Cairo 11845, Egypt
[3] Computers and Systems Department, Electronic Research Institute, Cairo 11843, Egypt
[4] Informatics Department, Electronic Research Institute, Cairo 11843, Egypt
[5] AI Lab, DeltaX Co., Ltd., 24 Namdaemun-ro 9-gil, Jung-gu, Seoul 04522, Republic of Korea
[6] Department of Computer Engineering, Gachon University, Seongnam 13415, Republic of Korea

Corresponding Author Email: sameer@gachon.ac.kr

https://doi.org/10.18280/ts.400520

**Received:** 28 July 2023
**Revised:** 11 September 2023
**Accepted:** 19 September 2023
**Available online:** 30 October 2023

***Keywords:***
*blowfish algorithm, copyright, data integrity, DCT, digital images, DWT, encryption, watermarking*

**ABSTRACT**

With the rapid proliferation of digital images on the internet, the task of preserving image ownership and ensuring the detection of unauthorized alterations has become increasingly challenging. This study introduces a robust algorithm, leveraging Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Blowfish encryption techniques, designed to maintain copyright integrity and detect image tampering. The proposed algorithm operates on a given RGB host image, first isolating it into its constituent red, green, and blue components. For the purpose of copyright protection, the algorithm applies DWT and DCT to the green component, embedding a watermark logo within it. The blue component is subjected to Blowfish encryption, generating a ciphered blue component that aids in tampering detection. Subsequently, the least significant bits of this ciphered blue component are interchanged with those of the host image's red component, producing a novel red component. This process results in the creation of a watermarked green component, an original blue component, and a newly formed red component. These are then amalgamated to produce the final watermarked image. The proposed method is evaluated using five standard images, with simulation results demonstrating its resilience to various attacks. Importantly, the algorithm exhibits a capacity to detect any unauthorized modifications up to a granularity of 2×2 pixels.

## 1. INTRODUCTION

The burgeoning multimedia industry has resulted in the proliferation of digital media files, readily accessible via the Internet. This availability, however, has also facilitated the unauthorized acquisition of these digital contents, leading to copyright infringement and substantial losses for the original content owners. The ease of content modification and rapid transfer across the Internet further exacerbate these issues. Consequently, data piracy and copyright protection have emerged as critical challenges in preserving ownership rights [1, 2].

Digital image watermarking serves as a solution to these challenges, providing a technique for tagging digital media to establish and assert copyright ownership. This process involves the insertion of copyright information into a digital image in a manner that does not compromise the image's quality. Beyond embedding copyright information, the ability to extract this information is crucial in affirming the identity of the digital image.

One of the prevailing watermarking techniques is frequency-domain watermarking, which encompasses various forms such as Discrete Wavelet Transform (DWT) [3-6], Fast/ Discrete Fourier Transform (FFT and DFT) [7, 8], Discrete Cosine Transform (DCT) [9, 10], Principle Component Analysis (PCA) [11-13], and Singular Value Decomposition (SVD) [9, 14-17]. Typically, these methods transform host images into the frequency domain, where the watermark is discreetly embedded.

Pallaw et al. [18] proposed a robust watermarking scheme utilizing the Slantlet transform (SLT), randomized-singular value decomposition (RSVD), and Firefly algorithm optimization technique. In their approach, the original image undergoes SLT for frequency domain transformation, followed by the division of the lower-frequency SLT sub-band coefficients into 3×3 blocks. Each block is then transformed into U, S, and V matrices using the RSVD algorithm, with the encrypted watermark bits embedded into the S matrix.

Abadi and Moallem [19] introduced a robust color image watermarking algorithm that merges the DWT and DCT. The DWT is applied to the green channel of the host images, and the watermark is subsequently distributed in the DCT coefficient, selected by a particular secret key.

Furthermore, Su et al. [20] proposed an adaptive blind watermarking method based on the slant algorithm, aimed at enhancing robustness against geometric attacks. Kumar and Singh [21] developed an adaptive color image watermarking scheme using DWT, alpha blending, and entropy concepts to

balance imperceptibility and robustness. Additionally, Sharma et al. [22] presented a hybrid watermarking scheme combining singular value decomposition, discrete wavelet transformations, and the artificial bee colony for embedding a scrambled color watermark.

Salama et al. [23] suggested a triple-channel encrypted hybrid fusion technique to improve the robustness, imperceptibility, and security of medical images. Liu et al. [24] introduced image watermarking algorithms based on DWT, Hessenberg decomposition (HD), and SVD transforms. Their embedding process applied DWT to the host image to produce several sub-bands, followed by HD on LL, and SVD on the created H and the watermark logo. The singular values of the host image and the watermark were then added with a scaling factor, optimized using the Fruit fly optimization algorithm (FOA).

While most of the previously mentioned techniques primarily focus on enhancing robustness and imperceptibility, they do not address the detection of unauthorized alterations in original images. In response to this, Liu and Yuan [25] put forth a dual-tamper-detection approach that both detects tampering and facilitates self-recovery. The watermark in this method is composed of two check bits and one recovery bit. Initially, the m-bit Most Significant Bit (MSB) image is extracted from the original, from which the Parity Check Bit Labeled (PCBL) generates the first check bit. The m-bit MSB image is then partitioned into blocks, each subjected to the MD5 algorithm to produce the second check bit. The SPIHT (Set Partitioning in Hierarchical Trees) algorithm is employed on the original image to create the recovery bit. The resulting watermark is subsequently embedded into the m-bit MSB image of the original image.

Nagm and Elwan [26] propose a novel algorithm that assigns a unique code to each pixel of a medical image, thus safeguarding patient information against deliberate attacks. Sulaiman and Altaei [27] introduce an Extreme Learning Machine (ELM) classifier that is trained on extracted textual features to identify image tampering. Srivastava and Yadav [28] present a technique that leverages texture descriptors to differentiate between original and forged images. Initially, the image is converted into the YCbCr color space, followed by the application of a standard deviation (STD) filter to the Cb and Cr channels to extract vital object details. A support vector machine then classifies the images as either original or tampered.

Zhao et al. [29] introduce a tampering detection technique that employs maximum entropy criteria. The Itti model [30] is applied to the original image to generate a saliency map, which is utilized as the watermark. This watermark is then embedded into the image using the DCT-SVD method. At the receiver end, the saliency map of the watermarked image and the watermark are extracted and compared to detect any tampering.

Siddharth Bhalerao et al. [31] propose a reversible image watermarking scheme for tampering detection based on the Region of Interest (ROI). The image is partitioned into ROI and RONI (Region of Non-Interest) sections. Within the ROI, the prediction-error expansion technique is utilized to embed authentication data. This ROI is then compressed and embedded into the RONI region using the difference histogram expansion technique. It's evident that these tampering detection techniques primarily aim to ascertain whether an image has been tampered with, without considering copyright protection.

This study introduces a novel algorithm designed to both preserve ownership and detect any unauthorized tampering with images. The proposed algorithm integrates two distinct techniques: one aimed at safeguarding ownership, improving imperceptibility, and enhancing robustness, while the other focuses on detecting illicit tampering in original images. Recognizing that DWT demonstrates robustness against geometric and noise attacks, and DCT is resistant to JPEG attacks, the first technique capitalizes on the strengths of DWT and DCT. It does so by concealing the watermark within the green component of the image to bolster the method's security and resilience against various attacks. A two-level DWT is applied to the green component of the RGB image, and the resulting $LL_2$ of $HH_1$ is transformed into the DCT domain to insert the watermark within the middle coefficients of the DCT, guided by a secret key. The second technique encrypts the blue component of the image using the Blowfish algorithm [32], substituting the least significant bits of the encrypted blue component with those of the red component of the host image, thereby generating a new red component. The new red component, the watermarked green component, and the original blue component are then combined to produce the resultant watermarked image.

The primary contributions of this study are as follows:

We propose an image forgery detection and authentication scheme capable of concurrent ownership preservation and detection of unauthorized tampering and illicit alterations.

The preservation of ownership is achieved by embedding a watermark within the middle coefficients of the DCT of the $LL_2$ sub-band of the green component of the cover image. This approach offers several advantages:

- Embedding the watermark within the DCT coefficients of $LL_2$ enhances the robustness of the proposed method against various attacks.
- Concealing the watermark within the high-frequency coefficients of the green component has a negligible impact on the perceptual quality of the image.
- The use of a distinct secret key to select the coefficients, emphasizing the middle range of DCT, bolsters the security of the proposed algorithm.

Unauthorized tampering and illicit alterations are detected by using the Blowfish algorithm to create a Digital Watermark Prints Matrix (DWPs) based on integrity protection, encryption, and steganography, which can be concealed within the cover images. This method also offers several advantages:

- Tampering can be detected even if the forgery block size is as small as one pixel, as the DWP is distributed across every pixel of the watermarked images.
- The DWPs have a minimal effect on image quality.
- The created DWP exhibits dynamic properties, dependent on the structure of the cover images.
- Since the DWPs are generated from the host image, there is no need to send them to the receiver.

In the remaining sections of this research paper, the extraction and embedding methods will be explored in more detail in Section 2. Evaluation metrics, dataset information, and simulation results will be presented in Section 3. Finally, Section 4 will offer the conclusion of this research.

## 2. THE PROPOSED METHOD

This paper addresses image forgery detection and

authentication techniques based on DCT, DWT, and blowfish techniques to preserve ownership and detect unapproved tampering and unauthorized alterations simultaneously. The proposed algorithm exploits the advantages of DWT and DCT to hide the watermark inside the green component. The DWT is particularly well suited to detect the regions in the host picture where a watermark may be hidden appropriately because of its superior spatial-frequency localization capabilities. The human eye is often not sensitive to changes in HH sub-bands. Therefore, the proposed algorithm uses the spatial-frequency localization capabilities of the DWT to deceive the human eye and insert the watermark inside the HH subbands without degradation in image quality. Besides, the DCT frequencies are divided into low, mid, and high-frequency sub-bands. Mid-frequency frequencies are selected to insert the watermark, making it robust to JPEG compression.

The image ownership is preserved by embedding the watermark logo in the mid-region of the DCT values of $LL_2$ of $HH_1$ in the green band. Moreover, the unapproved alteration is detected by inserting a digital watermark prints matrix created from the blue band of the watermarked image using the blowfish algorithm and substituting it in the red band. The pros of the proposed algorithm are that hiding the copyright in the mid-DCT of the detailed DWT guarantees the robustness of the logo against different attacks. Furthermore, creating the digital watermark prints matrix from the image and distributing it to every pixel in the red band does not affect the output image size, and unapproved tampering can be detected up to 2×2 pixels. Also, these prints' reconstruction does not require sending the original images. A detailed de-scription of the proposed embedding, extraction methods and the blowfish algorithm are explained in the following subsections.

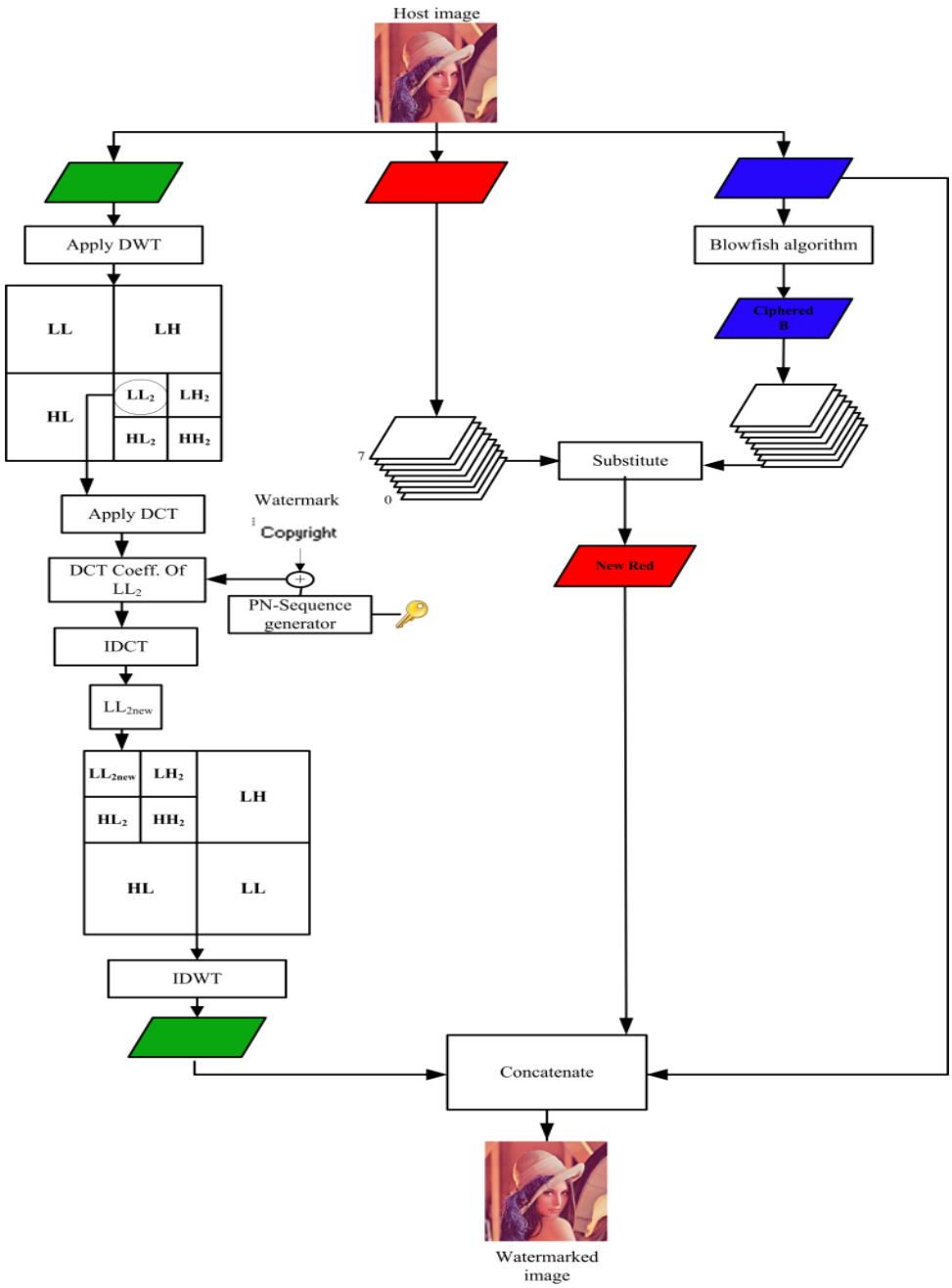



**Figure 1.** The proposed embedding method

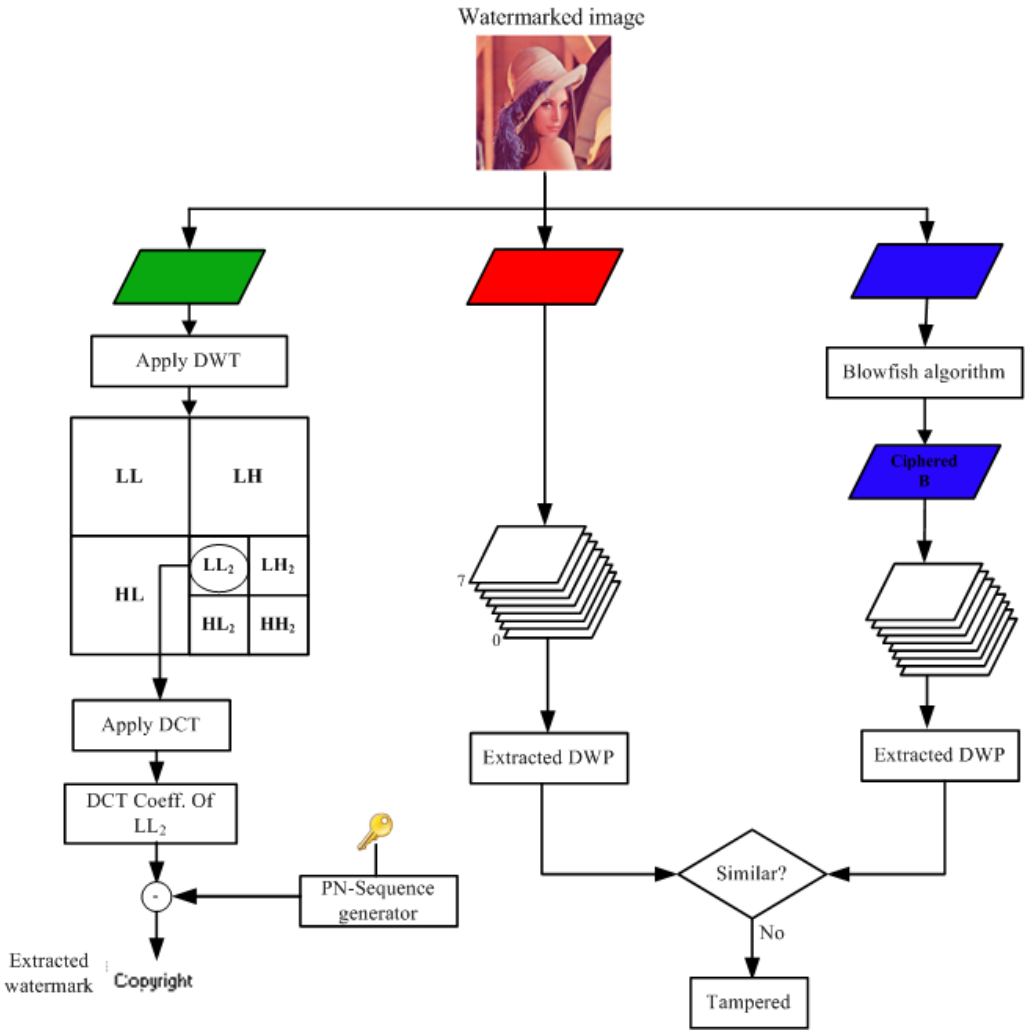



**Figure 2.** The proposed extraction method

### 2.1 The blowfish algorithm

Blowfish is an efficient encryption and decryption tool that uses a symmetric block cipher built on the Feistel function. Blowfish takes a variable-length key from 32 to 448 bits and includes 16 iterations, where each iteration is applied to a 64-bit block. The pros of blowfish over the existing technique are that it is among the fastest block cipher algorithms, is non-licensable, makes it available for all uses, can be applied to any image size and type, and proves superior for guessing attack prevention [33].

The blowfish process consists of two parts: subkeys generation and data encryption. In subkeys generation, the blowfish employs a massive number of subkeys: the P-array consists of 18 32-bit subkeys: $P_1,\ldots,P_{18}$ and four 32-bit S-boxes $S_1,\ldots..,S_4$ with 256 entries each. In data encryption: the blue component is divided into 8x8 blocks with a size equal to the blowfish key size 64. Each block X is converted to a vector with 64 bits size and fed to the blowfish algorithm as in algorithm 1. X is divided into two halves of 32 bits: $X_L$, $X_R$

**Algorithm 1:** The blowfish algorithm for encrypting the image blocks.

**Input:** Image block X
**Output:** Ciphered image block X
For i = 1 to 16:
$X_L = X_L$ XOR $P_i$
$X_R = F_n(X_L)$ XOR $X_R$
Swap $X_L$ and $X_R$
Next i
Swap $X_L$ and $X_R$ (Undo the last swap.)
$X_R = X_R$ XOR $P_{17}$
$X_L = X_L$ XOR $P_{18}$
Recombine $X_L$ and $X_R$ to get the cipher image block X.
Hint:
$F_n$ function is represented as:
Split $X_L$ into four 8 bits quarters: w, x, y, and z
$F_n(X_L) = ((S1, w + S2, x \bmod 2^{32})$ XOR S3, y) + S4, z mod $2^{32}$ .

### 2.2 The proposed embedding method

Figure 1 presents the structure of the embedding method. First, the watermark logo is hidden in the high-frequency component of the green band for copyright protection, while the digital watermark print created from the blue band is hidden in the red band for tamper detection.

The detailed steps of the embedding process are given below:

1) Decompose the host image into red, green, and blue channels.
2) Apply the DWT to the green component to obtain four subbands: $LL_1$, $HL_1$, $LH_1$, and $HH_1$.
3) Apply the DWT to $HH_1$ to get $LL_2$, $HL_2$, $LH_2$, $HH_2$.
4) Apply the DCT to the subband $LL_2$.
5) Spread the watermark with PN-sequence and a certain key in the DCT coefficient of $LL_2$.

6) Apply IDCT to the modified $LL_2$.
7) Apply IDWT to $LL_2$, $HL_2$, $LH_2$ and the modified $HH_2$ to produce the modified green component.
8) Encrypt the blue component based on the blowfish algorithm using S/N as a Key with a length 64 bit.
9) Select the least significant bits from every pixel of ciphered blue component and insert them in DWPs.
10) Select the least significant bit from every pixel of red and insert them in DWPs.
11) Substitute the DWPs of the original red and the ciphered blue component to get the modified red component.
12) Concatenate the modified red, green and original blue components to get the water-marked and authenticated image.

### 2.3 The proposed extraction method

To detect the unapproved alteration, the watermark and DWPS are extracted and compared to the original watermark and the extracted DWPs from the red band. Figure 2 shows the proposed extraction method, and the detailed steps of the extracting process are given below.

1) Decompose the watermarked image into red, green, and blue channels.
2) Encrypt the blue component with S/N has a length of 64-bit using blowfish algorithm.
3) Select the least significant bits from every pixel of ciphered blue component and create the DWPs.
4) Select the least significant bits from every pixel of red component and create the DWPs.
5) Compare the extracted DWPs from the ciphered components blue and red for tamper detection.
6) Apply the DWT to the green component to obtain four subbands: $LL_1$, $HL_1$, $LH_1$, and $HH_1$.
7) Apply the DWT to $HH_1$ to get $LL_2$, $HL_2$, $LH_2$, $HH_2$.
8) Apply the DCT to the subband $LL_2$.
9) Reconstruct the watermark from the DCT coefficient of $LL_2$.

## 3. EXPERIMENTAL RESULTS

### 3.1 Dataset

Six standard color images are chosen from different databases to be used as host images for evaluating the proposed method performance, as shown in Figures 3(a)-(f). These images are Barbara, Jetplane, Lake, Lena, Mandrill, and Pepper, of size 512×512. The watermark image is selected as a binary image of size 20×50, as shown in Figure 3(g).

The images are selected for various properties. These properties are a mix of colors, details, textures, as in Barbara, Mandrill, and Pepper, and smoothness, as in Lena.

### 3.2 Evaluation metrics

- **Peak Signal to Noise Ratio (PSNR)**

PSNR is used to evaluate the effect of the watermark embedding process on the watermarked image. Higher PSNR values reflect a low degree of watermarked image distortion. The PSNR is calculated as [34]:

$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE} \quad (1)$$

where, *MAX* represents the maximum power of the image and equals 255 which is the maximum pixel intensity. Mean square Error (MSE) represents the noise power and is calculated as the cumulative squared error between the host and the watermarked image as follows:

$$\text{MSE} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{i,j} - Y_{i,j})^2 \quad (2)$$

- **Normalized correlation coefficient NCC**

NCC is used to measure the similarity between the original and the extracted watermark image. The NCC value ranges from 0 to 1. If the NCC value is close to 1, this means that the two images are very similar; otherwise, the two images are dissimilar. NCC formula between two images of size N×M is given by:

$$\text{NCC}(X, Y) = \frac{\text{Cov}(X,Y)}{\sqrt{\text{Var}(X)}\sqrt{\text{Var}(Y)}} \quad (3)$$

where, Cov (X,Y) is the covariance between the image X and image Y. Var(X) and Var (Y) is the variance of image X and Image Y respectively. According to the Cov and Var definitions, the NCC formula can be written as:

$$\text{NCC}(X, Y) = \frac{\frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{i,j} - \bar{X})(Y_{i,j} - \bar{Y})}{\sqrt{\frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{i,j} - \bar{X})^2} \sqrt{\frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (Y_{i,j} - \bar{Y})^2}} \quad (4)$$

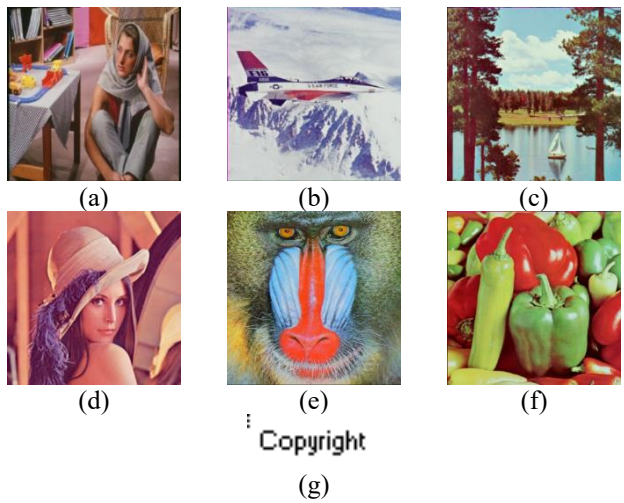



**Figure 3.** Test images (a) Barbara (b) Jetplane (c) Lake (d) Lena (e) Mandrill (f) Pepper (g) Watermark image

### 3.3 Simulation results

Different experiments are conducted to evaluate the proposed method's performance; some evaluate the proposed system's robustness, while others detect unauthorized alterations and unapproved tampering.

3.3.1 Robustness analysis

First, the proposed system is assessed corresponding to different gain factor values that were used to spread the watermark inside the DCT coefficients as mentioned in the embedding process step 5.

**Table 1.** The effect of the gain factor on the proposed system performance in terms of PSNR and NCC

| Host Image | Watermarked Image PSNR | | Watermark Image NCC | |
|---|---|---|---|---|
| | k=2 | k=25 | k=2 | k=25 |
| **Barbara** | 55.7314 | 43.565 | 0.8369 | 1 |
| **Jetplane** | 55.684 | 43.5627 | 0.8492 | 1 |
| **Lake** | 55.6918 | 43.5713 | 0.6559 | 1 |
| **Lena** | 57.2813 | 43.6333 | 0.9587 | 1 |
| **Mandrill** | 57.4999 | 43.64 | 0.7665 | 1 |
| **Pepper** | 57.4331 | 43.7298 | 0.9263 | 1 |

Table 1 tabulated the values of the PSNR and NCC for the water-marked and watermark images, respectively, at gain factors 2 and 25. It can be observed from the table at k= 2 that the quality of the watermarked image is higher than its quality at k=25.

On the contrary, the quality of the watermark logo at k=25 is better than its quality at k=2; thus, the best k value that achieves the best performance is selected empirically between 2 and 25.

Figure 4 presents the effect of the gain factor on the watermarked image and the watermark logo, respectively. It can be noticed from the figure that the gain factor effect on the watermarked image quality is a little bit small, and the watermarked image is visually the same at low and high gain factors. However, the watermark logo quality is visually better at high gain factor values. On the other hand, it can be noticed that the DWPs inserted in the red component do not affect the watermarked image and the PSNR is higher than 40 db.

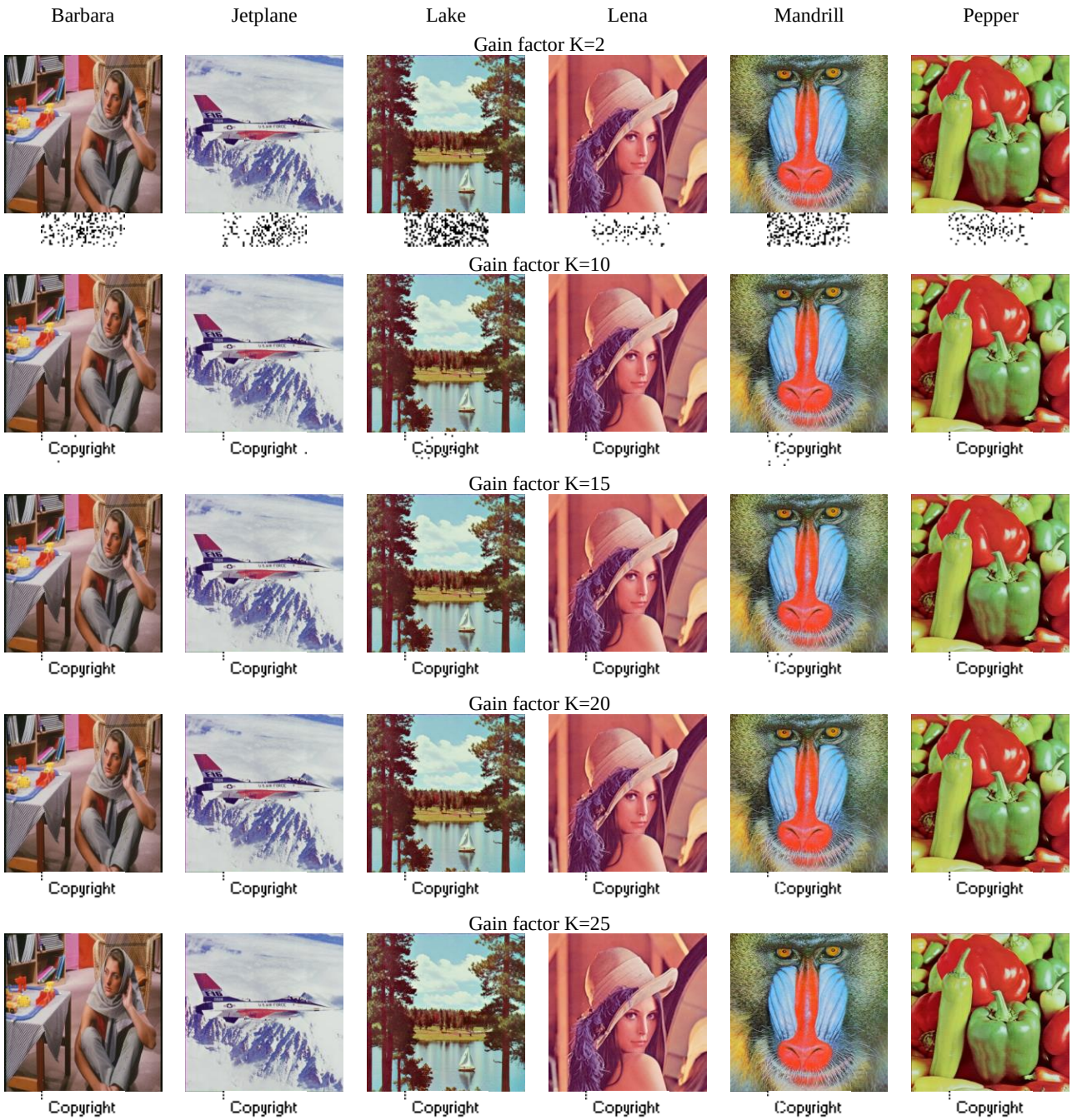



**Figure 4.** The visual effect of the gain factor on the watermarked and watermark images

For evaluating the proposed algorithm's robustness, various attacks such as salt and pepper noise, Gaussian noise, sharpening, histogram equalization, and JPEG are applied to the watermarked images. The watermark logo is extracted from the attacked watermarked image, as shown in Table 2, and the NCC values are calculated for each image. It can be observed that the extracted watermark logo is clear and sharp for salt and pepper at a variance of 0.005, histogram equalization, and sharpening. However, the extracted logo that was attacked by Gaussian noise, salt, and pepper at variance 0.02, and JPEG suffers from some distortion.

3.3.2 Tampering detection

Conversely, the proposed algorithm is evaluated against different unapproved tampering sizes, and the results are tabulated in Table 3. The watermarked image has been tampered with using various sizes such as 2×2, 4×4, and 16×16 pixels. It can be perceived from the table that the quality of the copyright logo is not affected by tampering, and the algorithm detects that the image has been exposed to tampering. These results reflect that the algorithm can detect tampering up to 2×2 pixels.

3.3.3 Comparison of the proposed method with the existing methods

The proposed method is compared with the conventional methods in terms of robustness because no conventional technique is found to preserve ownership and detect tampering simultaneously.

Table 4 compares the proposed and conventional approaches regarding PSNR for the watermarked image and NCC for the watermark logo. Although the pro-posed method is used to detect tampering and protect the copyright, and the conventional method is used only for copyright protection, it can be noticed that the proposed method outperforms the conventional method regarding the quality of the watermarked and watermark images.

**Table 2.** The effect of different attacks on the proposed algorithm performance in terms of NCC

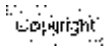
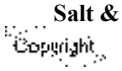
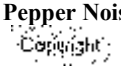
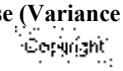
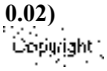
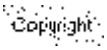
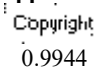
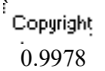
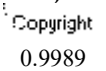
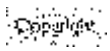
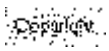
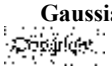
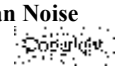
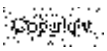
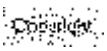
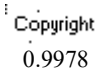
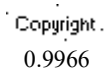
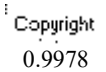
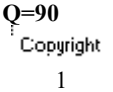
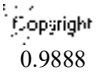
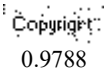
| Barbara | Jetplane | Lake | Lena | Mandrill | Pepper |
|---|---|---|---|---|---|
| **Salt & Pepper Noise (Variance = 0.02)** | | | | | |
|  |  |  |  |  |  |
| 0.9732 | 0.9743 | 0.9598 | 0.9721 | 0.9754 | 0.9709 |
| **Salt & Pepper Noise (Variance = 0.005)** | | | | | |
|  |  |  |  |  |  |
| 0.9978 | 0.9989 | 0.9944 | 0.9978 | 0.9989 | 0.9944 |
| **Gaussian Noise** | | | | | |
|  |  |  |  |  |  |
| 0.9464 | 0.9341 | 0.9352 | 0.9419 | 0.9296 | 0.9363 |
| **Histogram Equalization** | | | | | |
|  |  |  |  |  |  |
| 1 | 0.9978 | 0.9989 | 1 | 1 | 1 |
| **Sharpening** | | | | | |
|  |  |  |  |  |  |
| 1 | 1 | 1 | 1 | 1 | 1 |
| **JPEG Q=90** | | | | | |
|  |  |  |  |  |  |
| 0.9966 | 0.9978 | 0.9966 | 1 | 0.9888 | 0.9788 |

**Table 3.** The unapproved tampering detection and its effect on the proposed algorithm in terms of NCC

| | Barbara | Jetplane | Lake | Lena | Mandrill | Pepper | Tampering Detection |
|---|---|---|---|---|---|---|---|
| Tampering 2x2 |  1 |  1 |  1 |  1 |  0.984 |  1 | detected |
| Tampering 4x4 |  1 |  0.9888 |  1 |  1 |  0.977 |  1 | detected |
| Tampering 16x16 |  1 |  1 |  1 |  1 |  0.977 |  1 | detected |

**Table 4.** Comparison of the proposed system with the existing methods

| Host Image | Watermarked Image PSNR | | Watermark Image NCC | |
|---|---|---|---|---|
| | Proposed | Conventional [23] | Proposed | Conventional [23] |
| **Barbara** | 43.565 | 41.1307 | 1 | 0.989 |
| **Jetplane** | 43.5627 | 42.432 | 1 | 0.998 |
| **Lake** | 43.5713 | 41.958 | 1 | 0.899 |
| **Lena** | 43.6333 | 41.28 | 1 | 1 |
| **Mandrill** | 43.64 | 40.5823 | 1 | 0.909 |
| **Pepper** | 43.7298 | 42.475 | 1 | 0.969 |

## 4. CONCLUSION

This research proposes an image forgery and authentication technique for protecting copyright and identifying unauthorized alteration. To the author's knowledge, this is the first algorithm to protect copyright and simultaneously detect tampering. The proposed algorithm uses the DWT and DCT to hide the copyright logo in the image's green component to prove ownership. Moreover, the blowfish algorithm encrypts the blue component for creating DWPs which are swapped with the DWPs of the red component. The modified red, green, and original blue are concatenated to generate the watermarked image. The proposed algorithm is evaluated using five standard images, and PSNR and NCC are used to measure its performance. One of the key findings of this research is that the proposed algorithm can successfully detect tampering up to 2×2 pixels while preserving the quality of the copyright logo. Furthermore, the proposed algorithm is robust to different noise attacks, histogram equalization, sharpening, and JPEG. In future work, different methods for copyright protection will be implemented and utilized instead of the current one to strengthen the proposed method for attacks that differ from those mentioned in this research.

## ACKNOWLEDGMENT

This study was funded by Korea Agency for Technology and Standards in 2022, project numbers are K_G012002234001, K_G012002236201, and by the sabbatical support from Gachon University in 2023.

## REFERENCES

[1] Mahto, D.K., Singh, A.K. (2021). A survey of color image watermarking: State-of-the-art and research directions. Computers & Electrical Engineering, 93: 107255. https://doi.org/10.1016/j.compeleceng.2021.107255

[2] El Zein, O.M., El Bakrawy, L.M., Ghali, N.I. (2017). A robust 3D mesh watermarking algorithm utilizing fuzzy C-Means clustering. Future Computing and Informatics Journal, 2(2): 148-156. https://doi.org/10.1016/j.fcij.2017.10.007

[3] Zhou, X., Zhang, H., Wang, C. (2018). A robust image watermarking technique based on DWT, APDCBT, and SVD. Symmetry, 10(3): 77. https://doi.org/10.3390/sym10030077

[4] Wai, C.K., Ahmad, N.A. (2014). Robust DWT-SVD image watermarking with hybrid technique for embedding data in all frequencies. In AIP Conference Proceedings, 1605(1): 227-232. https://doi.org/10.1063/1.4887593

[5] Alenizi, F., Kurdahi, F., Eltawil, A.M., Al-Asmari, A.K. (2019). Hybrid pyramid-DWT-SVD dual data hiding technique for videos ownership protection. Multimedia Tools and Applications, 78: 14511-14547. https://doi.org/10.1007/s11042-018-6723-9

[6] Shoitan, R., Gharghory, S.M. (2021). Compressive sensing theory for improving the robustness and the security of the discrete wavelet transform-singular value decomposition watermarking scheme. Journal of Computer Science, 17(4): 414–426. https://doi.org/10.3844/jcssp.2021.414.426

[7] Cao, H., Hu, F., Sun, Y., Chen, S., Su, Q. (2022). Robust and reversible color image watermarking based on DFT in the spatial domain. Optik, 262: 169319. https://doi.org/10.1016/j.ijleo.2022.169319

[8] Kang, X., Huang, J., Shi, Y.Q., Lin, Y. (2003). A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression. IEEE Transactions on Circuits and Systems for Video Technology, 13(8): 776-786. https://doi.org/10.1109/TCSVT.2003.815957

[9] Hu, H.T., Hsu, L.Y. (2015). Exploring DWT–SVD–DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression. Computers & Electrical Engineering, 41: 52-63. https://doi.org/10.1016/j.compeleceng.2014.08.001

[10] Singh, D., Singh, S.K. (2017). DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. Multimedia Tools and Applications, 76(11): 13001-13024. https://doi.org/10.1007/s11042-016-3706-6

[11] Thakkar, F.N., Srivastava, V.K. (2017). A fast watermarking algorithm with enhanced security using compressive sensing and principle components and its performance analysis against a set of standard attacks. Multimedia Tools and Applications, 76: 15191-15219. https://doi.org/10.1007/s11042-016-3744-0

[12] Noor, R., Khan, A., Sarfaraz, A., Mehmood, Z., Cheema, A.M. (2019). Highly robust hybrid image watermarking approach using Tchebichef transform with secured PCA and CAT encryption. Soft Computing, 23: 9821-9829. https://doi.org/10.1007/s00500-019-03838-2

[13] Singh, S. (2016). New image digital watermarking using PCA-DCT and DWT. International Journal of Engineering and Management Research (IJEMR), 6(2): 472-474.

[14] Fazli, S., Moeini, M. (2016). A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. Optik, 127(2): 964-972. https://doi.org/10.1016/j.ijleo.2015.09.205

[15] Chang, C.C., Tsai, P., Lin, C.C. (2005). SVD-based digital image watermarking scheme. Pattern Recognition Letters, 26(10): 1577-1586. https://doi.org/10.1016/j.patrec.2005.01.004

[16] Jane, O., Elbaşi, E. (2014). Hybrid non-blind watermarking based on DWT and SVD. Journal of Applied Research and Technology, 12(4): 750-761. https://doi.org/10.1016/S1665-6423(14)70091-4

[17] Thanki, R., Dwivedi, V., Borisagar, K., Borra, S. (2017). A watermarking algorithm for multiple watermarks protection using SVD and compressive sensing. Informatica, 41(4): 479–493, 2017.

[18] Pallaw, V.K., Singh, K.U., Kumar, A., Singh, T., Swarup, C., Goswami, A. (2023). A robust medical image watermarking scheme based on nature-inspired optimization for telemedicine applications. Electronics, 12(2): 334. https://doi.org/10.3390/electronics12020334

[19] Abadi, R.Y., Moallem, P. (2022). Robust and optimum color image watermarking method based on a combination of DWT and DCT. Optik, 261: 169146. https://doi.org/10.1016/j.ijleo.2022.169146

[20] Su, Q., Liu, D., Sun, Y. (2022). A robust adaptive blind color image watermarking for resisting geometric attacks.

Information Sciences, 606: 194-212. https://doi.org/10.1016/j.ins.2022.05.046
[21] Kumar, S., Singh, B.K. (2021). DWT based color image watermarking using maximum entropy. Multimedia Tools and Applications, 80: 15487-15510. https://doi.org/10.1007/s11042-020-10322-9
[22] Sharma, S., Sharma, H., Sharma, J.B., Poonia, R.C. (2021). A secure and robust color image watermarking using nature-inspired intelligence. Neural Computing and Applications, 35: 4919-4937. https://doi.org/10.1007/s00521-020-05634-8
[23] Salama, A.S., Mokhtar, M.A., Tayel, M.B., Eldesouky, E., Ali, A. (2021). A triple-channel encrypted hybrid fusion technique to improve security of medical images. Computers, Materials and Continua, 68(1): 431-446. https://doi.org/10.32604/cmc.2021.016165
[24] Liu, J., Huang, J., Luo, Y., Cao, L., Yang, S., Wei, D., Zhou, R. (2019). An optimized image watermarking method based on HD and SVD in DWT domain. IEEE Access, 7: 80849-80860. https://doi.org/10.1109/ACCESS.2019.2915596.
[25] Liu, T., Yuan, X. (2021). A dual-tamper-detection method for digital image authentication and content self-recovery. Multimedia Tools and Applications, 80: 29805-29826. https://doi.org/10.1007/s11042-021-11179-2
[26] Nagm, A., Elwan, M.S. (2021). Protection of the patient data against intentional attacks using a hybrid robust watermarking code. PeerJ Computer Science, 7: e400. https://doi.org/10.7717/peerj-cs.400
[27] Sulaiman, D.S., Altaei, M.S.M. (2023). Image tampering detection using extreme learning machine. In AIP Conference Proceedings, 2457: 040002. https://doi.org/10.1063/5.0123415
[28] Srivastava, V., Yadav, S.K. (2022). Digital image tampering detection using multilevel local binary pattern texture descriptor. Journal of Applied Security Research, 17(1): 62-79. https://doi.org/10.1080/19361610.2021.1883397
[29] Zhao, B., Qin, G., Liu, P. (2015). A robust image tampering detection method based on maximum entropy criteria. Entropy, 17(12): 7948-7966. https://doi.org/10.3390/e17127854
[30] Itti, L., Koch, C., Niebur, E. (1998). A model of saliency-based visual attention for rapid scene analysis. IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(11): 1254-1259. https://doi.org/10.1109/34.730558
[31] Bhalerao, S., Ansari, I.A., Kumar, A. (2023). A reversible medical image watermarking for ROI tamper detection and recovery. Circuits, Systems, and Signal Processing, 42: 6701-6725. https://doi.org/10.1007/s00034-023-02416-0
[32] Hashim, A.T., Al-Qarrawy, S.M., Mahdi, J.A. (2009). Design and implementation of an improvement of Blowfish encryption algorithm. Iraqi Journal of Computers, Communications, Control and Systems Engineering, 9(1): 95-109.
[33] Mushtaq, M.F., Jamel, S., Disina, A.H., Pindar, Z.A., Shakir, N.S.A., Deris, M.M. (2017). A survey on the cryptographic encryption algorithms. International Journal of Advanced Computer Science and Applications, 8(11): 333-344. https://doi.org/10.14569/ijacsa.2017.081141
[34] Mrak, S.G.M.G. (2004). Reliability of objective picture quality measures. Journal of Electrical Engineering, 55(1-2): 3-10.

## NOMENCLATURE

| | |
|---|---|
| DWT | Discrete Wavelet Transform |
| DCT | Discrete Cosine Transform |
| FFT | Fast Fourier Transform |
| DFT | Discrete Fourier Transform |
| PCA | Principle Component Analysis |
| SVD | Singular Value Decomposition |
| SLT | Slantlet Transform |
| RSVD | Randomized-Singular Value Decomposition |
| HD | Hessenberg Decomposition |
| FOA | Fly Optimization Algorithm |
| PCBL | Parity Check Bit Labeled |
| SPIHT | Set Partitioning in Hierarchical Trees Algorithm |
| ELM | Extreme Learning Machine Classifier |
| STD | Standard Deviation |
| RONI | Region of NonInterest |
| DWPs | Digital Watermark Prints Matrix |
| PSNR | Peak Signal to Noise Ratio |
| MSE | Mean Square Error |
| NCC | Normalized Correlation Coefficient |