ISSN: 0067-2904

# Image Authentication Proofing Scheme Based on RLG by Employing the Characteristics of DCT

**Fahmi Ghozzi[1]*, Khalid Kadhim Jabbar[2], Ahmad Fakhfakh[3]**

[1] *Department of Electronic, National School of Electronics and Telecommunications of Sfax, University of Sfax, Tunisia.*

[2] *Department of Computer Science, College of Education, Mustansiriyah University, Baghdad, Iraq.*

[3] *Laboratory of Signals, Systems, Artificial intelligence and Networks (SM@RTS), Digital Research Center of Sfax(CRNS), Sfax, Tunisia.*

Received: 9/4/2024 Accepted: 14/9/2024 Published: 30/9/2025

**Abstract**

The impetus behind the emergence of information security was the need to send sensitive data over the often insecure Internet networks. Information and communication technology fields have used authentication to verify alleged users identities and prevent intruders from achieving their goals. However, with the increasing use of digital images in multimedia applications, particularly those requiring high levels of security, there has been a growing interest in ways to ensure their safety. A secret key was generated randomly to add to the proposed encryption system, increasing its complexity to preserve privacy and reduce the influence of intruders. Our method uses a reversible logical approach for security and privacy based on discrete cosine transforms (DCT) to propose a semi-fragile watermark approach to detect and locate any changes. The results show a high degree of accuracy in verifying and establishing the color image's reliability, all while maintaining image quality during the embedding and retrieval phases. Results showed that the proposed method is very good at finding and locating any manipulation by the intruder on the colored image while maintaining the image quality after the embedding process.

Keywords: Authentication, DCT, Information Security, Reliability, Watermark.

# نظام تدقيق مصادقة الصورة أستنادا الى RLG من خلال توظيف خصائص DCT

**فهمي كوزي[1]*, خالد كاظم جبار[2], أحمد الفخفاخ[3]**

[1] قسم الإلكترونيك ، المدرسة الوطنية للإلكترونيك والاتصالات بصفاقس ،جامعة صفاقس، صفاقس،تونس

[2] قسم علوم الحاسوب، كلية التربية، الجامعة المستنصرية، بغداد، العراق

[3] مخبر SM@RTS, مركز البحث في الرقميات بصفاقس ، صفاقس، تونس

**الخلاصة**

كان الدافع وراء ظهور أمن المعلومات هو الحاجة إلى إرسال بيانات حساسة عبر شبكات الإنترنت التي غالب ما تكون غير امنة. تم استعمال المصادقة في مجالات تقنية المعلومات والاتصالات للتحقق من هوية المستخدم المزعومة ومنع المتطفلين من تحقيق اهدافهم، ولكن نظرًا لاستعمال الصور الرقمية بشكل متزايد في تطبيقات الوسائط المتعددة ، خاصة تلك التي تحتاج إلى مستوى عالٍ من الأمان ، فقد كان هناك اهتمام

* khalik.jabbar@uomustansiriyah.edu.iq

متزايد بطرق التأكد من أنها حقيقية. يتم إضافة مفتاح سري يتم توليدة بصورة عشوائيَّة  الى نظام التشفير المقترح من اجل زيادة التعقيد للحفاظ على الخصوصية وللحد من تأثير المتطفلين، يتم استعمال النهج المنطقي القابل للعكس للأمان والخصوصية استنادًا إلى تحويلات جيب التمام المنفصلة (DCT) لاقتراح نهج العلامة المائية شبه الهش لاكتشاف التغييرات وتحديد موقعها ان وجدت. تظهر النتائج التي تم الحصول عليها من امكانية التحقق وإثبات موثوقية الصورة الملونة بدرجة عالية من الدقة مع الحفاظ على جودة الصورة أثناء مرحلتي التضمين والاسترجاع. لقد أظهرت النتائج أن الطريقة المقترحة جيدة جدًا في العثور على أي تلاعب يقوم به المتطفل على الصورة الملونة وتحديد مكانها مع الحفاظ على جودة الصورة بعد عملية التضمين.

## 1. Introduction

The requirement to send sensitive data across unsecured internet networks has given rise to the field of information security. Information technology and communications fields use authentication to verify a user's claimed identity and prevent impersonation. Multimedia applications increasingly use digital images, necessitating a high level of security. This has led to a rise in interest in ways to verify their authenticity. Digital images are typically transmitted over insecure media, such as the Internet and other computer networks. As a result, it is important to prevent tampering with medical photographs [1–4], because this could affect the outcomes of treatments that rely on the photos. Most people refer to the process of checking images using the terms active authentication and passive authentication. Digital watermarking and digital signatures are examples of active authentication, which involves putting a symbol inside a piece of media to prove that it belongs to its owner.

Passive authentication can detect tampering. There are two broad categories: those that rely on forgery and those that don't. A watermark demonstrates the owner's rights to the content by embedding a seal, signature, or sign within multimedia (such as photos, films, or physical objects) [5–8]. Money is one of the watermark's most important aspects because it is unaffected by attempts to delete, steal, or copy the watermark itself, unlike many approaches that attempt to hide or encrypt content. One definition of a watermark is a stamp, trademark, or symbol implanted in multimedia, such as images, audio recordings, movies, or physical things, to demonstrate the owner's rights to the product or content [9–11]. The watermark is a signal inserted into the material in a way that does not impair accuracy or ensure control and is unaffected by attempts to erase, snatch, or duplicate [12]. A watermark, which is akin to an official signature, serves as a distinctive mark on photographs and designs, enabling customers to monitor your business.

## 2. Related Work

In [13], the researchers developed a reversible quantum image watermarking method using the most significant qubit (MSQb) and the least significant qubit (LSQb). The peak signal-to-noise ratio (PSNR) of a carrier image with a watermark that was added using this method is about 4% higher than the PSNR of a carrier image with a watermark that was added using the traditional LSQb method. On the other hand, a new technique was used in order to find the best location in the host image to hide the digital image [14] by integrating two algorithms: the improved honeycomb algorithm, which is used to encrypt the digital watermark, and the blue monkey heuristic algorithm, which watermark. Moreover, in order to verify the security and robustness of the proposed method against various common image processing attacks such as Gaussian noise, rotation, salt and pepper noise, sharpening, median filter, where the filter is averaged, compression, and cropping, some performance metrics such as peak signal to noise ratio (PSNR) and mean square error (MSE) are also calculated. Likewise, normal correlation (NC) is used. In order to verify the similarity between the original and extracted digital watermark. The results showed that the proposed system is efficient and provides a high degree of security and robustness against most attacks compared to previous methods. The author in [15] suggested a watermarking system (WS) for telehealth applications. This method employed the lifting wavelet transform (LWT) and DCT techniques to insert a signature watermark picture and patient report with a length of 80 characters. This study used LWT to break down the host picture into sub-bands, followed by DCT to further alter the important sub-bands. Then, the author employed an alternative method to extract the watermarked data from the DCT-transformed sub-bands, which included both encrypted patient data and a signature watermark. In [16], the researchers suggested utilizing a cryptographic web service to identify manipulated medical photos. On the other hand, this non-blind watermarking approach incorporates the Extended Producer Responsibility (EPR) into the radiological pictures for identification and security. The method relies on DCT and compressive sensing (CS) to encrypt watermark data and transform a host picture, respectively. Using a two-stage watermarking strategy, the authors of [17] aimed to implant both the fingerprints and faces of their patients.

Initially, the authors encrypted the fingerprint by extracting minutiae details from the original facial image and encoding them into a key. To achieve the second level of watermarked image (WI), the original fingerprint was encrypted again and the watermarked picture was inserted into it. Finally, the watermark was inserted using the DCT sub-bands and the encrypted watermark image. The article [18] shows that different transform operations, such as the DCT, the discrete wavelet transform (DWT), and the singular value decomposition (SVD), can add watermarking to a host picture; however, one cannot expect a single transformation to fulfill all design criteria at once. To fix this problem, they created a hybrid blind digital image watermarking method based on the DCT, DWT, and SVD. In [19], the authors merged three well-known transforms into a single system. The experiments revealed that the method outperforms other previously published methods, achieving PSNR values of 44.0567 dB and structural similarity index measure (SSIM) values of 0.9800. It has a very high Normalized Cross Correlation (NCC) value of 1.000 and a very low back end ratio (BER) value of 0.000, both of which are excellent ratings for robustness.

## 3. Research Methodology

### 3.1 Discrete Cosine Transformation

A given image's DCT is a function of only two dimensions. A small number of DCT coefficients, known as a DCT property, concentrate visually meaningful information in a typical image. The DCT is a common and extremely general domain-watermarking algorithm. The picture breaks up into different frequency bands, revealing the low (FL) in the top left corner, followed by the middle (FM) and high (FH) on the lower and right borders (see Fig. 1). The FM middle frequency band is ideal for watermarking media. In a low-frequency FL ensemble, human vision is capable of reading the watermark. It's also likely that the FH high-frequency watermark band will cause local distortion, especially at the edges. This technique is resistant to common forms of attack like compression, noise, sharpening, and filtering. The spatial watermarking method is more complicated than this one [20].

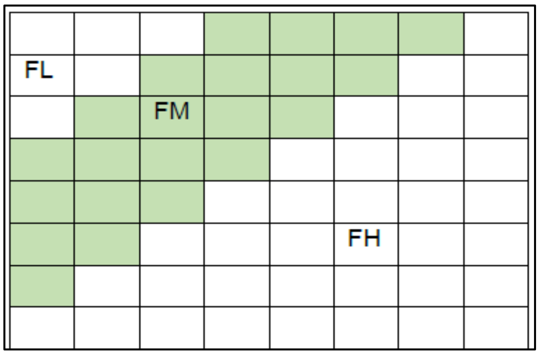


**Figure 1:** DCT frequency 8×8 block [20]

3.2 Revisable logic gates (RLG)

RLG is a digital logic gate that always gives the same result, no matter what the inputs are. Reversible mappings (RLGs) remain reversible because the numbers that enter and exit from them are the same. Applications that require minimal power and weight include optical estimation, discrete-time signal processing, nanotechnology, and bio-information. The security is a major concern for all of these uses [21].

The proposed approach employed reversible logic gates such as the SCL gate, Fredkin gate, Toffoli gate, Feynman gate, and XOR gate to construct the secret key generation system.

## 4. Statement of the problem

In our current era, the importance of using the web cannot be ignored. On the other hand, preserving privacy has become a major challenge due to technological development and individual capabilities in dealing with it.

In order to preserve the privacy and intellectual property of Internet users, it became necessary to find innovative methods that could handle complexity while ensuring security and confidentiality. The proposed system addresses a significant portion of these challenges by constructing a security system that minimizes time consumption and upholds the image's quality. To achieve the principle of reliability, proving the reliability of the image by detecting manipulation and locating the intended manipulation, no matter how simple, is another challenge. The proposed system employs a new scientific methodology to combine randomness in key generation using logical gates and the DCT function. This approach provides flexibility in handling the low-frequency region, thereby enhancing the system's efficiency.

## 5. The Proposed Method

The proposed method consists of a set of basic stages, namely:

1. Embedding stage.
2. Extraction stage.
3. Tamper detection stage.
4. Key Generational stage.

The above stages work sequentially, and each stage depends on the success of the previous stage. Furthermore, the steps of embedding and extracting heavily rely on the key generation step, which is a critical part of making the proposed method more private and complicated. Fig. 1 shows the main steps of the embedding stage. The 128×128 binary watermark bits will be embedded in the 256×256 color image and set within the low frequency range in a set of parameters that are randomly chosen after the DCT stage. These parameters depend on the DCT, key generation stage, and revisable logic gate sub-systems, as shown in Fig. 2.

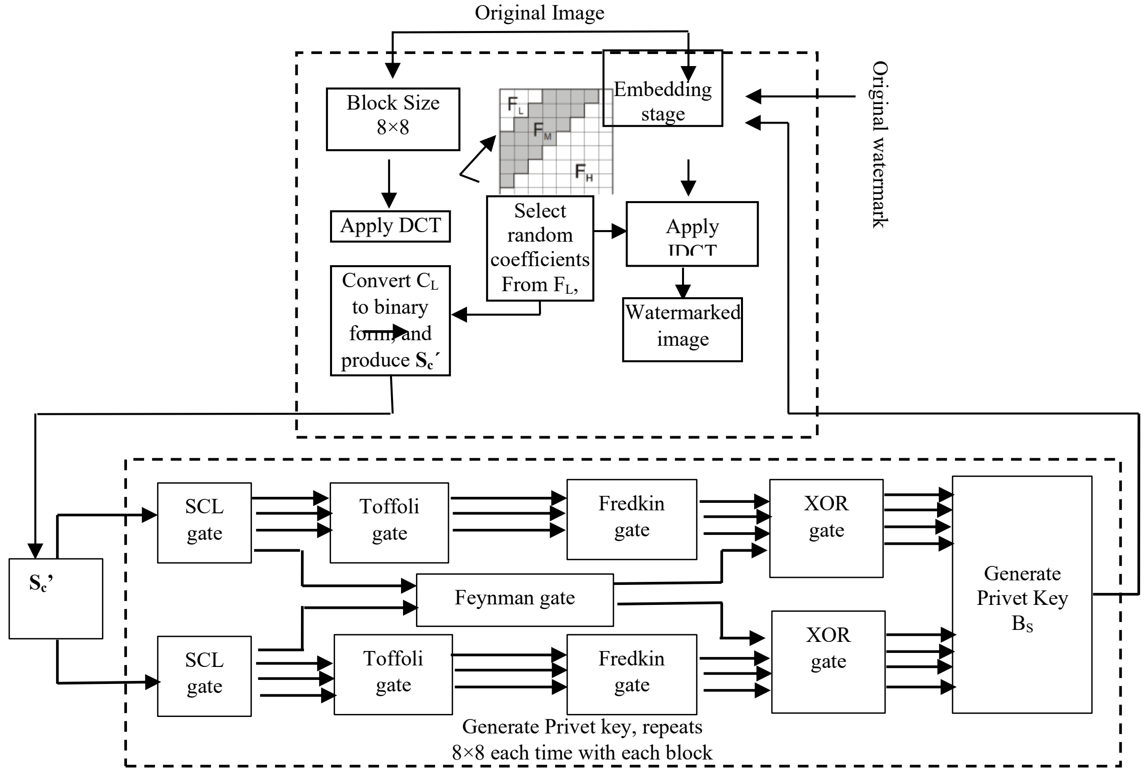


**Figure 2:**Main diagram of proposed scheme.

The embedding stage begins with the process of dividing the 256 × 256 color image into a group of 8 × 8 blocks. This process creates a group of blocks, and DCT was used to extract the transactions within those blocks. Later, the system will randomly select a set of transactions, specifically from the low-frequency area.

After converting the data into binary format, the system will pass those binary values to a complex system, which consists of a set of revisable logic gates developed by [21]. This system will then obtain a binary string known as the secret key, on which it will rely later in the embedding stage. Once the revisable logic gate sub-system receives the second string, it repeats this process eight times for each block. This ensures the creation of binary bits that align with the number of bits in the binary sign and the parameters of the low-frequency region, as illustrated in algorithm 1.

Algorithm 1: Embedding Stage.
 Input: Original image as $O_i$, Original watermark as $O_w$
 Output: Watermarked image as $W_i$
  Begin
1. Read $O_i$, $O_w$; // where $O_i$ (256×256), and $O_w$(128×128).
2. Divide $O_i$ into non-overlapping blocks with a size of 8×8 to produce the corresponding block of DCT coefficients as $C_b$;
3. Perform DCT to the whole $C_b$ to produce transformed blocks: $C_b$';
4. Select random coefficients from $C_b$' (form low frequency domain) and produce the selected coefficients: $S_c$
5. Convert $S_c$ to the binary form and produce $S_c$′;

```
6.  Generate the binary sequence (private key) as: $B_S$, Based on the developed revisable logic gate scheme, (repeat the same operation 8×8 each time with each main block from the low-frequency domain and produce matrix of binary sequence with  size of 128×128, which is identical to the size of the original watermark ($B_S$= $O_W$).
7.  While  i<> length of $B_S$
Begin
   If $B_{S\,(i,\,j)}$ = 1 then
       Perform the embedding process between  $O_{W\,(I,\,j)}$ with the corresponding blocks of low-frequency domain; // to the most left-hand side
  Next i;
   Else
Next i;
   End (IF);
         End (While);
8.  Perform the inverse discrete cosine transform (IDCT);
9.  The watermark reconstructed.
10. END (begin); END.
```

Afterwards, the selected transactions convert into binary format. After sending the selected transactions to the revisable logic gates sub-system to obtain the secret key, which is a string of binary numbers, Fig. 3 illustrates the process of obtaining the binary logo from the host.

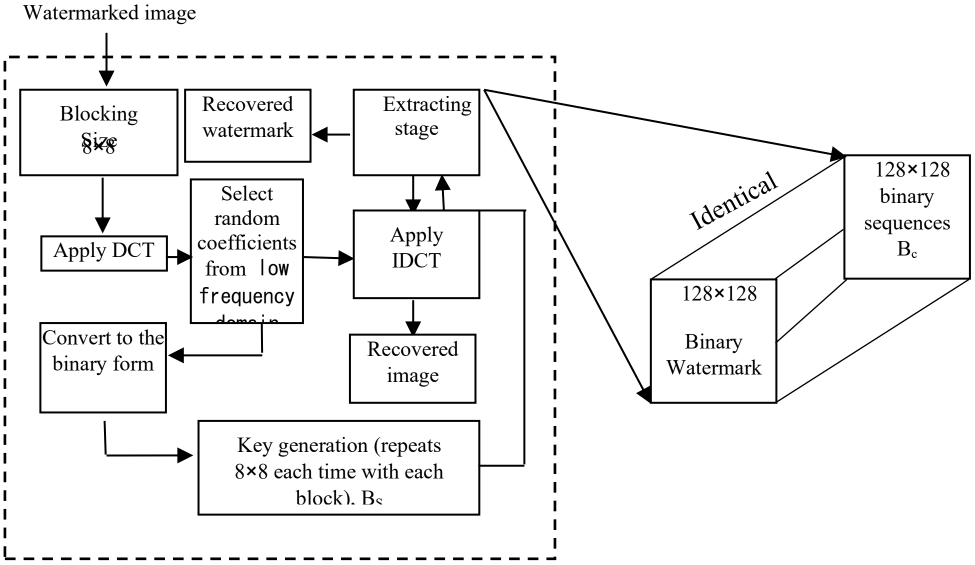

Watermarked image
Blocking Size 8×8
Recovered watermark
Extracting stage
Apply DCT
Select random coefficients from low frequency domain
Apply IDCT
Convert to the binary form
Recovered image
Key generation (repeats 8×8 each time with each block). Bs
Identical
128×128 binary sequences Bc
128×128 Binary Watermark

**Figure 3:**Main diagram of extraction stage

After the end of the extraction stage, our result will get both the binary logo and color image, and this is a natural output for this stage, which is important to us because we will rely on it later in the stage of detecting manipulation or forgery in the original content of the color image, if any, as shown in the following algorithm 2:

```
Algorithm 2: Extraction Stage
  Input: $W_i$
  Output: Recovered watermark as $R_w$
    Begin
1. Read $W_i$;
```

2. Divide $W_i$ into non-overlapping blocks with a size of 8×8 to produce the corresponding block of DCT coefficients as: $C_b$;
3. Perform DCT to the whole $C_b$ to produce transformed blocks: $C_b'$
4. Select random coefficients from $C_b'$ (form low-frequency domain) and produce the selected coefficients: $S_c$
5. Generate the binary sequence as a private key: $B_S$, based on the developed revisable logic gate scheme, (repeat the same operation 8×8 each time with each main block from the low-frequency domain) and produce a matrix of binary sequence with a size of 128×128, which is identical to the size of the original watermark ($B_S= O_W$).

```
6. While i<> length of $B_S$
Begin
If $B_{S\,(i,j)} = 1$ then
    $R_{W\,(i,j)} = 1$;
      Next i;
  Else
      Next i;
 End (IF);
End (While);
```

7. Perform IDCT;
8. The watermark is extracted as $R_w$, and the image is also recovered as $O_i'$.
9. END.

Given the high likelihood of image manipulation by those seeking to deceive, a new method was developed to determine whether the image has changed, thereby verifying its authenticity. Fig. 4 represents a general scheme for the extraction stage.

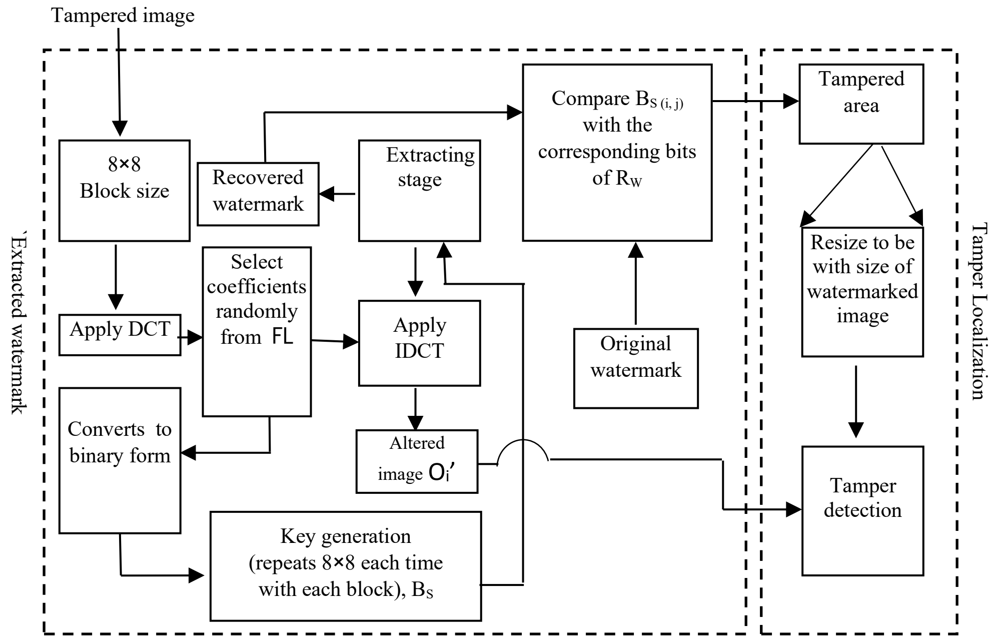


**Figure 4**:A main diagram of the tamper localization stage

To find the wrong bits, which are no longer the same as they were before the embedding stage, the original binary flag is needed and the recovered binary flag after the embedding process. Later, the sum of those incorrect bits represents the actual manipulation sites, if any, on the color image. Following this step, spots of a different color will appear in the colored image, indicating the changes made to the original content. The algorithm below outlines the primary steps required to complete the discovery stage and identify any intended modifications to the color image:

Algorithm 3: Tampering Area(s) localization Stage.

```
  Input: watermarked image\ tampered image as: $T_i$
  Output: Recovered watermark as: $R_w$, Tampered image as: $T_i'$
    Begin
1.  Read the watermarked image\ tampered image as: $T_i$;
2.  Perform the Blocking size 8×8 to produce the corresponding block: $T_{ib}$;
3.  Perform DCT to the whole $T_{ib}$ of the original image to -produce transformed blocks: $T_{ib}$';
4.  Select random coefficients from $T_{ib}$' and produce the selected coefficients: $T_s$;
5.  Convert $T_s$ to the binary form and produce $T_s'$;
6.  Generate the binary sequence as a private key from $T_s'$ based on the developed revisable logic gate scheme, (repeat the same operation 8×8 each time with each main block from the low-frequency domain) and produce a matrix of binary sequence with a size of 128×128, which is identical to the size of the original watermark ($T_{ms}' = O_W$);
7.  If the $T_{ms}'_{(i, j)} = O_{W(i, j)}$ Then $T_{R(i, j)}=1$, where $T_{R(i, j)}$: the recovered watermark form the tampered image;
      Else
         $T_{R(i, j)}$=o;
    End (IF);
8.  Perform IDCT;
9.  The watermark $T_{R(i, j)}$ extracted;
10. Compare each bit of $T_{R(i, j)}$ with the corresponding bit of $O_w$ to produce the different area (tampered area) as: $A_t$;
11. Resize $A_t$ to be with the size of $O_i'$;
12. Stamp the tampered area according to the corresponding location between $O_i'$ and $A_t$;
13. Produce $T_i'$;
14. End; End.
```

## 6. Results

Various color images are used in the embedding stage, using 256×256 Bitmap (BMP) color images as hosts. These images can carry extra information during the embedding stage without compromising the quality of the final image. On the other hand, embedding can handle various types of color images with the same efficiency; the type we adopted allows us to handle high contrast in nature without visible distortions in the host image, and the samples used to extract the results are shown in Table 1, along with a detailed description of each image, as shown below:

**Table 1:** Original images' properties

| **Original image 256×256** | | | | | | |
|---|---|---|---|---|---|---|
| **Name** | Baboon | Bazaar | Circus man | Maroc | peppers | Soldiers |
| **Texture (BMP)** | High texture | Digital | Low texture | Painted | High texture | Low texture |

The embedding stage used a binary watermark with a 128×128 size. The addition of binary watermark bits to the color image parameters at the far left of each parameter will not alter the basic color of that color area, ensuring the embedding process meets both subjective and objective standards, leading to good and satisfactory results. Fig. 5 shows the original watermark:

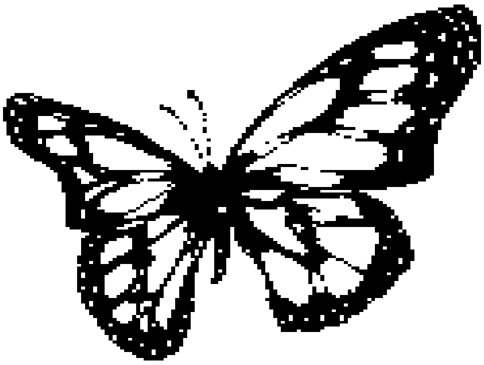
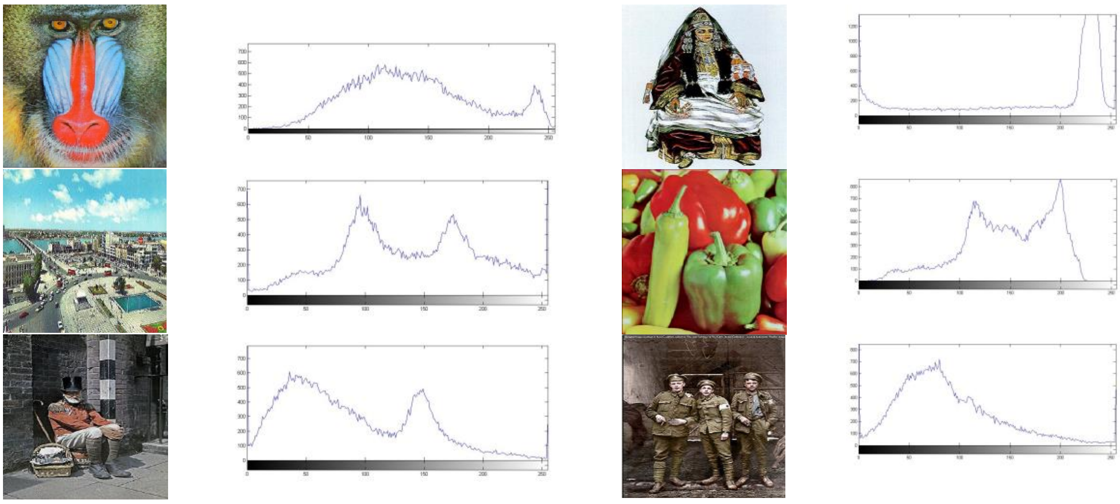


**Figure 5:**Original watermark

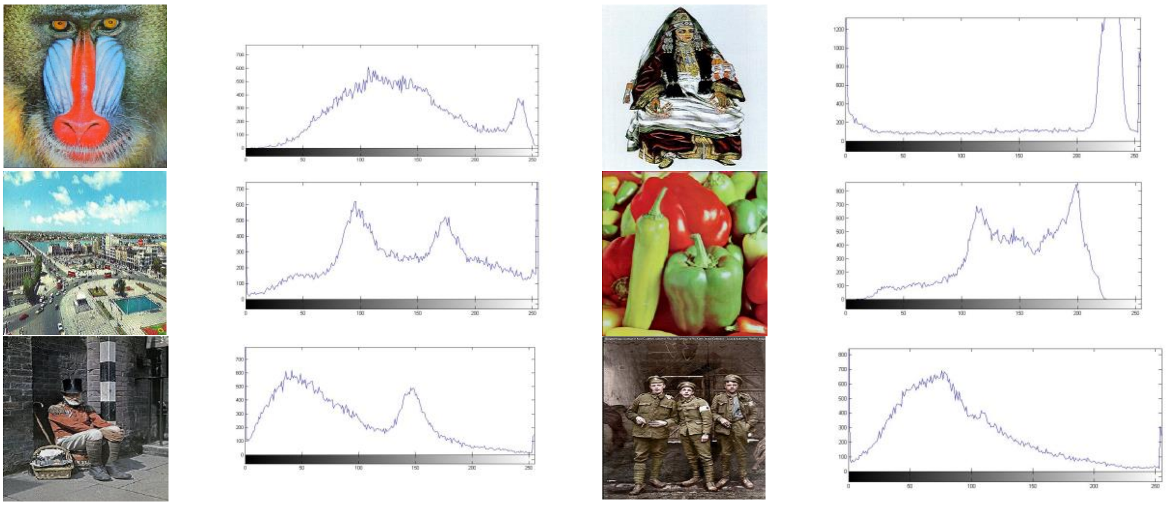
Figure 6 shows each color image along with its histogram. This will assist us in monitoring contrast and subtle differences during the processing stages of the proposed method, particularly after the embedding process. This will allow us to measure the embedding process's impact on the host and assess its effectiveness in producing an embedded image without visible flaws. The figure shows the approved images in the embedding stage and the histogram for each image.



Original image Histogram Original image Histogram

**Figure 6:** Original images with their histograms

On the other hand, after completing the embedding phase, it's important to examine the embedded image's histogram to determine the image differences between it before and after the embedding process. This would tell us how well the proposed method worked during the embedding process. Figure 7 displays the embedded images along with their respective histograms.



Original image Histogram Original image Histogram

**Figure 7:**Watermarked images with their histograms

In Figure 7, it is possible to see the difference between the histogram of the mounted image before and after the embedding process. The difference was very small because the embedding process didn't change the used images, and the resulting embedded image was of high quality to both the naked eye and the subjective scale. Table 2 displays the results of mean square error (MSE), and accuracy rate (AR) that were calculated by comparing the original image and the watermarked image.

**Table 2:** Quality measurments of watermarked images

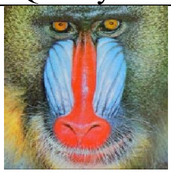
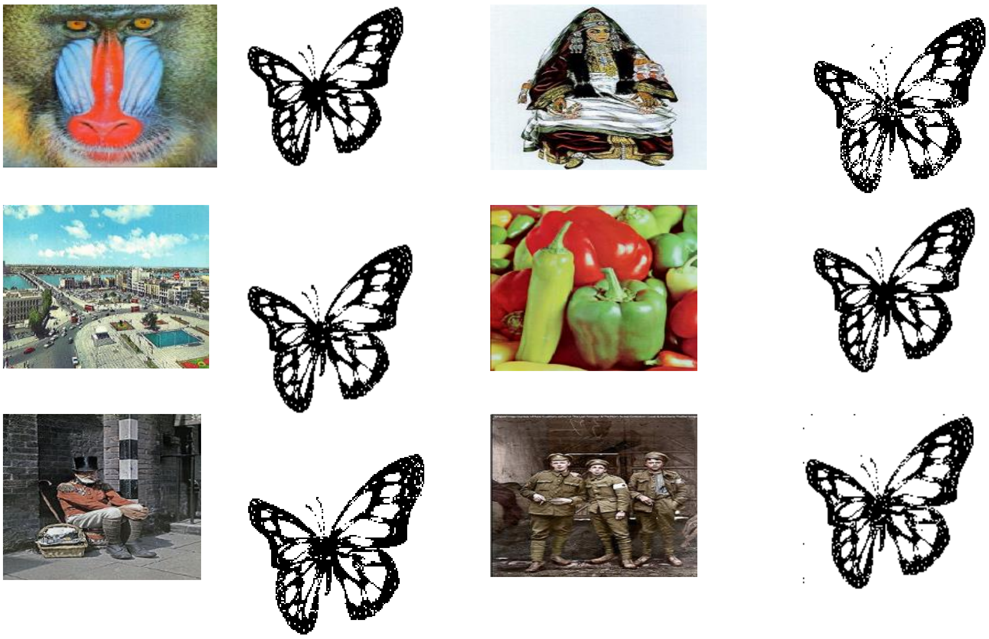
| **W$_i$** |  | | | | | |
|---|---|---|---|---|---|---|
| **PSNR** | 38.9110 | 40.1311 | 49.3310 | 44.3320 | 37.1019 | 39.8891 |
| **MSE** | 0.9760 | 0.6711 | 0.1993 | 0.1143 | 0.0981 | 0.0154 |
| **SSIM** | 0.9921 | 0.1130 | 0.2298 | 0.1290 | 0.9134 | 0.8321 |

Table 2 displays the most important results based on the used standards in this area. The results, despite the varying nature of the used images, demonstrate the success of the embedding process. On the other hand, the visible image is of high quality and doesn't show any signs that the host image has an invisible watermark.

On the other hand, the binary watermark was extracted from the host to determine whether the embedding process affected the quality of either image. Fig. 8 displays the host image after the embedded process and the binary watermark after the retrieval process.



Watermarked image | Extracted watermark | Watermarked image | Extracted watermark

**Figure 8:** Extracted watermark

The following are the results obtained after extracting the watermark from the host. The quality of the recovered watermark was calculated using the AR and MSE functions by comparing the original and the recovered watermark, as shown in Table 3.

**Table 3:** Quality measurment of extracted watermark

| | | | | | | |
|---|---|---|---|---|---|---|
| **Extracted watermark** | | | | | | |
| **Host** | Baboon | Bazaar | Circus man | Maroc | peppers | Soldiers |
| **AR** | 0.9792 | 0.1018 | 0.2120 | 0.1176 | 0.0213 | 0.0546 |
| **MSE** | 0.9760 | 0.6711 | 0.1993 | 0.1143 | 0.0981 | 0.0154 |

Overall, the watermark recovered and remained consistent across different images. This was because the host was different; the binary logo extracted from painted images was accompanied by a group of dark and sparsely colored areas, and the same thing happened with the binary images. The painted host's high quality prevented any dispersed color spots from appearing in the digital and high-texture images' watermarks. But if the quality of the retrieved watermark is different, that doesn't mean there's something wrong with the proposed method. This is because of the host's quality, and it doesn't hinder the process of finding and locating the manipulation later on. Fig. 9 demonstrates the use of image classification. Three groups of different images were formed based on the color nature of each image. The diversity of images in terms of color nature is considered an important factor in evaluating the ability of the proposed method to deal with different images.

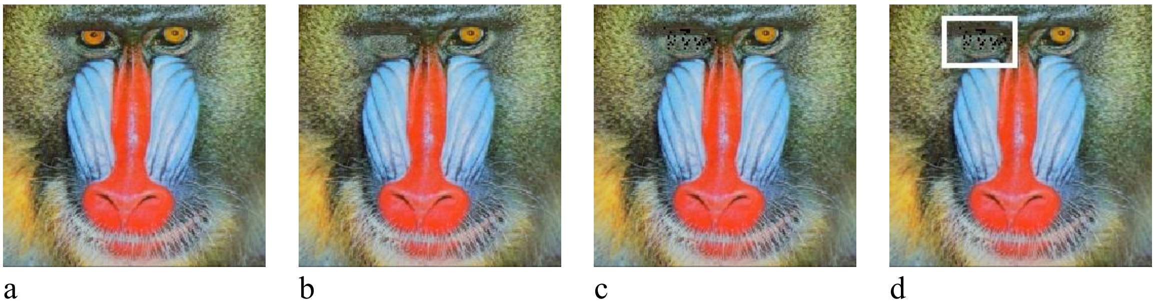


**Figure 9:** Alternation detection of (Baboon): a. authenticated, b. unauthenticated, c. alternation detection, d. alternation area(s) localization

The system performed the intended manipulation by hiding the eye features on the right side of the baboon's image, as shown in Fig. 9.b, which represents the forged image. It is important to note that the system recognized and identified the manipulation area in Figs. 9.c and d. The tampered area appears as a group of black-colored dots, indicating the image's unreliability.

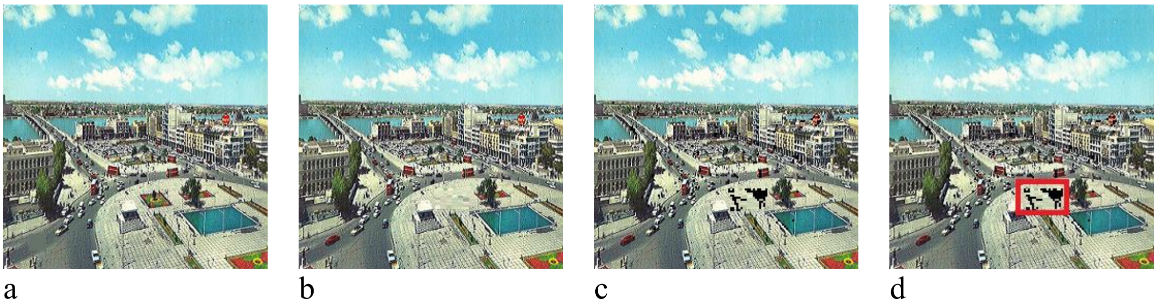


**Figure 10:** Alternation detection of (Bazaar): a. authenticated, b. unauthenticated, c. alternation detection, d. alternation area(s) localization

Figure 10.a represents the original (trusted) image; the square garden deletion in the Bazaar image, as seen in Fig. 10.b, served as a representation of the manipulation process. Here, it is worth noting the accuracy of the manipulation, even if it were not for the presence of Fig. 10.a. Given that Fig. 10.b is the forged image, and the system has demonstrated this in Figs. 10.c and d, it is impossible for the viewer to determine which of the two images the original is. Both images represent the identified tampering area. A black-colored block indicates the image's unreliability.

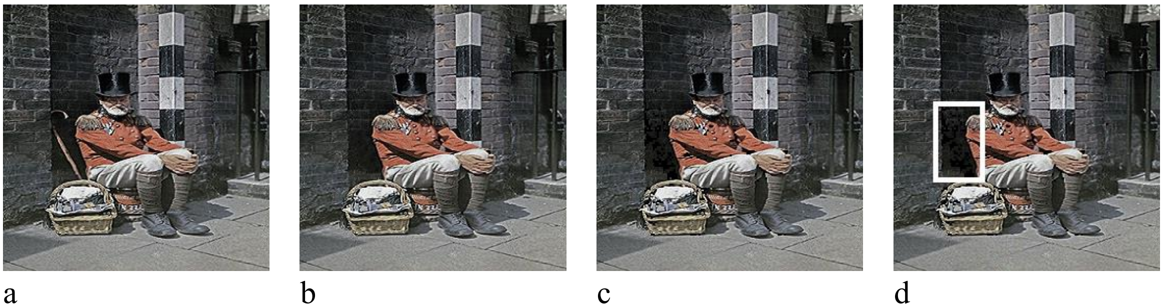


**Figure 11:**Alternation detection of (Circus man): a. authenticated, b. unauthenticated, c. alternation detection, d. alternation area(s) localization

Regarding Figure 11 above, it's difficult to distinguish between Fig. 11.a and b, which are the original picture and the fake one. The removed stick from the picture behind the circus performer serves as a symbol of manipulation in the original image, as shown in Fig. 11.b. In Figs. 11.c and d, the system obtained an unreliable image by identifying the tampered area. Note that Fig. 11's image is dark and slanted. The image turns black, making it challenging to discern the system-identified manipulation area. If you pay close attention, you will see a black color block that the system identified as the manipulation area.

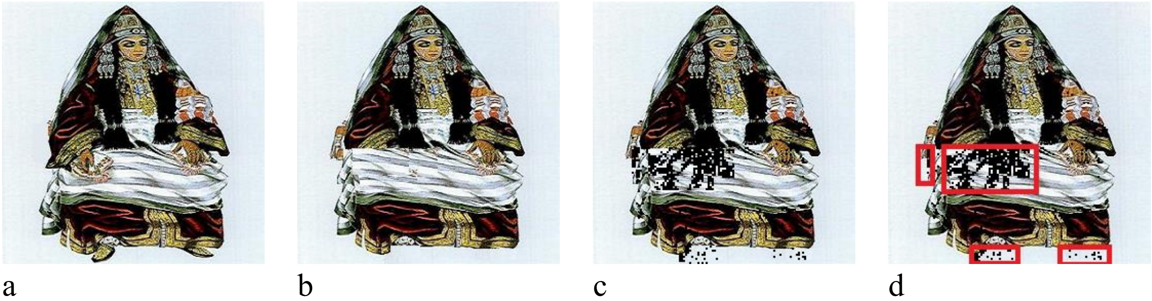


**Figure 12:** Alternation detection of (Maroc): a. an authenticated image, b. an unauthenticated image, c. alternation detection, d. alternation area(s) localization

The proposed system can detect the intended tampering area in Fig. 12, even if it is in multiple areas. The manipulation of four regions in the unreliable image, Fig. 12.b, involved masking the left hand. The right and left foot were not only removed, but it also copied and pasted a portion of the image from the left side of Fig. 12.a.

It's worth noting that the system recognized this manipulation, even when it encompassed multiple areas within a single image. This is evident in Figs. 12.c and d, where the system placed a black area, indicating the unreliability of the image in Fig. 12b.

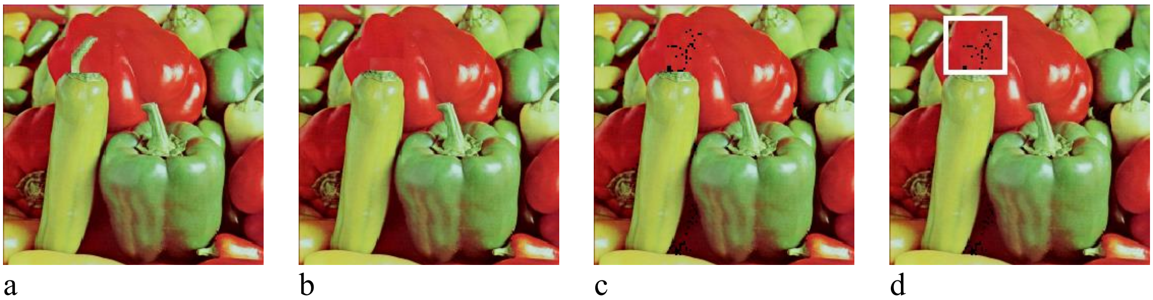


**Figure 13:**Alternation detection of (peppers): a. authenticated, b. unauthenticated, c. alternation detection, d. alternation area(s) localization

Figure 13 shows a portion of the peppers cut off on the left side of the image. Notice Figure 13.b, which represents the unreliable image. Both Figures. 13.c and d depict the manipulation area, which is represented by scattered black dots, demonstrating the unreliability of the picture in Figure 13.b.

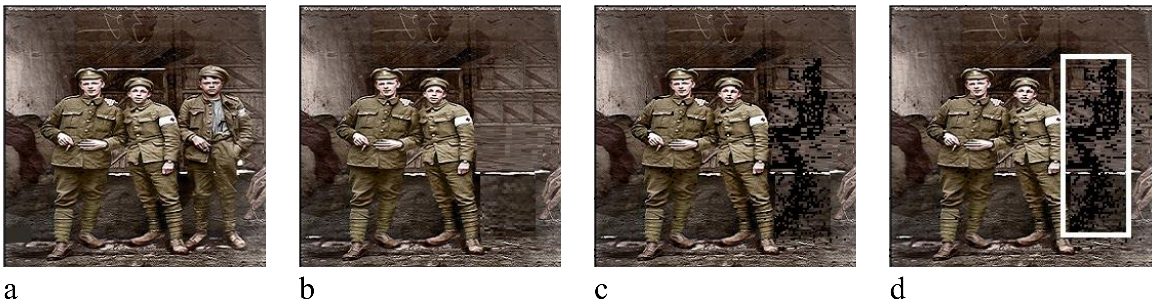


**Figure 14:** Alternation detection of (Soldiers): a. authenticated, b. unauthenticated, c. alternation detection, d. alternation area(s) localization

The deleted soldier in Figure 14 is located to the left of the original image in Fig. 14.a. If the viewer were able to identify which of the two photos is the original, it would take more time to determine which of the two photos (Fig. 14.a, b) is reliable and which is fake. The viewer can clearly identify the precise manipulation area in Figs. 14.c and d, even with the image's dark background due to its color. This is because Fig. 14.c, d depicts the intended manipulation area, while the forged image is unreliable. It's important to note that the proposed system's method relies solely on a digital watermark for authentication, eliminating the need for the original image. See Figure15.

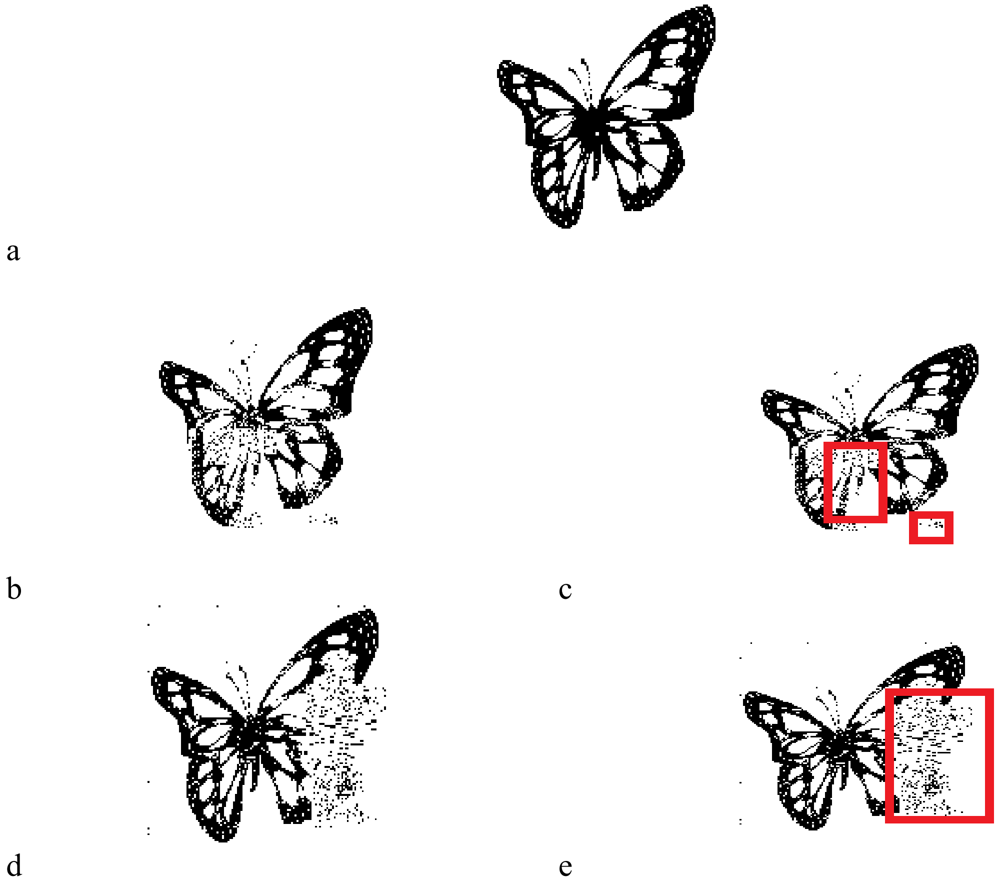


**Figure 15:** The recovered watermark after authentication proofing, a. original watermark, b. extracted watermark from unauthenticated image (soldiers), c. tampering area(s) of (soldiers), d. extracted watermark from unauthenticated image (Moroccan woman), e. tampering area(s) of (Moroccan woman)

As shown in Fig. 15, our proposed system's methodology is based on the principle that the intended manipulation will be recorded on the digital watermark hidden in the original image during the embedding phase, which is very similar to the carbon method used in handwriting on more than one piece of paper at the same time. This method was applied to the proposed system with great success, recording any tampering on the digital watermark, no matter how simple or small. Later, the image is printed to verify the authenticity of the watermark image through authentication.

## 7. Discussion and analysis

Based on the information in the references, it looks like watermarking is a common way to authenticate and protect digital photos, especially in sensitive applications like medical imaging. Watermarking uses a number of transformations, like the DCT and the DWT, as well as error correction codes and quantum-based algorithms. The specific needs of the application determine the type of watermarking to use, including its resistance to tampering and its ability to handle distortion. Also, some methods may work better with certain types of images or media, such as grayscale photos or films. Table 4 provides us with a comprehensive comparison of a group of watermark technologies based on key characteristics that are considered among the most important criteria for evaluating the quality of the used technology:

**Table 4:** A comparison of watermarking techniques based on the most common criteria

| Method | Key Features | Technique | Key Contributions | Strengths | Weaknesses |
|---|---|---|---|---|---|
| [14] | Hybrid approach | Combination of honey algorithm and blue monkey meta-heuristic algorithm | Check security and determine the best hiding location | High security | It requires resources, which increases time consumption |
| 15] | Reversible watermarking, quantum computing | Combination of most significant and least significant quits | Reversible watermarking using quantum computing | High security due to quantum computing | Limited to certain types of data |
| [16] | Fast processing, digital signal processing | Fast DCT algorithm | Fast processing for digital signal processing | High speed | Limited focus on security |
| [17] | Robustness, distortion control, error correction code | Dual watermarking in LWT domain using DCT and error correction code | Robustness with distortion control using error correction code | High robustness | Complexity may hinder practical implementation |
| [18] | Tamper detection, crypto-watermarking | Crypto-watermarking scheme | Tamper detection using crypto-watermarking | High tamper detection capability | Limited to certain types of data |
| [19] | Robustness, compression resistance | Blind watermarking approach against compression using 2D-DCT | Robustness with compression resistance using blind watermarking | High compression resistance | Limited to certain types of data |
| [20] | Hybrid approach, robustness, watermark strength | Discrete cosine transform, discrete wavelet transform, singular value decomposition | Hybrid approach with strong watermarking | High watermark strength | Complexity may hinder practical implementation |
| [21] | Blind and robust watermarking, copyright protection | Hybrid watermarking scheme in frequency and spatial domain | Blind and robust watermarking for copyright protection | High copyright protection | Limited to certain types of data |
| Our proposed method | Tamper detection, crypto-watermarking | Reversible logic gates with DCT | Tamper detection and localization of tampering area(s) | High tamper detection capability | Complex for implementation |

Most of the techniques use either a visible or an invisible watermark. Visible watermarks are better for copyright protection, while invisible watermarks are better for detecting tampering, as shown in Table 5 below, which compares the methods based on things like image type, embedded domain, robustness, invisibility, and capacity. DCT and DWT techniques use different embedding domains, such as spatial, frequency, and transform domains. When it comes to robustness, the approaches vary in how well they stand up to common assaults like compression, noise, and cropping. Capacity is about how much data can be added to an image without making it look bad, and imperceptibility is about how well the watermark can be hidden inside the image. Finally, most of the techniques mentioned do not use logic gates, unlike the proposed system, which relies heavily on that as a basis for work. The advantages of logic gates, when incorporated into security system design, constitute a significant contribution to this field. It will increase the system's complexity, reduce processing time, make guessing more difficult, and facilitate error updating and tracking.

**Table 5:** Comparison in terms of the performance of each method

| \|Method | Type of Image | Domain | Robustness | Imperceptibility | Capacity |
|---|---|---|---|---|---|
| [14] | Color image | Spatial | High | High | High |
| [15] | Gray scale | Quantum | High | High | Low |
| [16] | Gray scale | Spatial | Medium | High | High |
| [17] | Color medical image | Spatial-Freq. | High | Medium-High | Medium |
| [18] | Medical image | Spatial-Freq. | High | High | Medium |
| [19] | Fingerprint | Spatial-Freq. | High | High | Low |
| [20] | Gray scale | Spatial-Freq. | High | High | High |

## 8. Conclusion

A different method was proposed to prove the image's reliability. This method depends on the performance of two different systems, but it all works toward the same goal, which is to prove the image's reliability, verify it, and find any manipulations, if any. The first subsystem is responsible for creating a secret key. The embedding, retrieval, and verification processes use this key, which consists of a series of binary numbers. On the other hand, another subsystem works to add the digital (binary) watermark bits to the color image and define the frequency area. During the implementation phase of the DCT, the low profile was chosen randomly to obtain an embedded image that is distortion-free and of high quality. The results of applying the proposed method to color images of different colors were extracted; the proposed method could prove the image's reliability and determine where any manipulation occurred, if any. In the verification and proof stages, the proposed method depends on the original watermark. However, it is possible to come up with other ways to check the authenticity of an image without the original watermark.

## Acknowledgement

The author(s) would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad-Iraq for its support in the presented work, as well as Sfax University, National School of Electronics and Telecommunications of Sfax (ENET’COM), Sfax, Tunisia.

## References

**[1]** S. N. Mohammed, ”Color Image Steganography Using Gradient Selective Bezier Curves,” *Iraqi Journal of Science*, vol. 64, no. 7, pp. 3625-3641, 2023.

**[2]** M. B. Tuieb, A. S. Mahmood and F. N. Abbas, ”Fusion of DWT as a Novel Approach for Efficient Secured and Reversible Video Steganography,” *Journal of Physics: Conference Series*, vol. 2322, no. 2022, pp. 2322 – 012093, 2022.

**[3]** R. S. Salman, A. K. Farhan and A. A. Shakir, “Creation of S-Box Based One-Dimensional Chaotic Logistic Map Color Image Encryption Approach,” *International Journal of Intelligent Engineering and Systems*, vol. 15, no. 5, pp. 378–389, 2022.

**[4]** M. B. Tuieb, H. J. Serteep and D. M. Abed, ”Image steganography using Fresnelet transformations, stated coefficients and a pre-processed message,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 6, pp. 1683–1689, 2023.

**[5]** W. K. Ahmed and R. S. Mohammed, ”Lightweight Authentication Enhancement Using Arnold Chaotic Map and Markov-Chain for Internet of Things Applications,” *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 2, pp. 115–124, 2023.

**[6]** R. S. Mohammed, ”Design a Lightweight Authentication Encryption Based on Stream Cipher and Chaotic Maps with Sponge Structure for Internet of Things Applications,” *International Journal of Intelligent Engineering and Systems*, vol. 16, no.1, pp. 532–547, 2023.

**[7]** O. Y. Abdulhammed, ”A robust image steganography based on a novel technique by using improved DNA and modified chaotic approach,” *Journal Supercomputing*, vol. 80, no. 1, pp. 226-248, 2023.

**[8]** A. Mohammed, I. A. Saad and H. A. Hilal, ”Computation intelligent new approach for image steganography calculations,” *Materials Today: Proceedings*, vol. 65, no. 5, pp. 2752-2759, 2022.

**[9]** K. K. Jabbar and H. A. Hilal and R. S. Mohammed, “Text Cryptography Using Multiple Encryption Algorithms Based On Circular Queue Via Cloud Computing Environment,” *Journal of Theoretical And Applied Information Technology*, vol. 96. No. 12, pp. 3654-3663, 2018.

**[10]** K. K. Jabbar, F. Ghozzi and A. Fakhfakh, “Robust Color Image Encryption Scheme Based on RSA via DCT by Using an Advanced Logic Design Approach,” *Baghdad Science Journal*, vol. 20, no. 6, pp. 2593-2607, 2023.

**[11]** W. A. Shukur, L. K. Qurban and A. Aljuboori, “Digital Data Encryption Using a Proposed W-Method Based on AES and DES Algorithms,” *Baghdad Science Journal,* vol. 20, no. 4, pp. 1414-1424, 2023.

**[12]** K. K. Jabbar, M. B. Tuieb and S. A. Thajeel, “Digital Watermarking By Utilizing The Properties Of Self-Organization Map Based On Least Significant Bit And Most Significant Bit,” *International Journal of Electrical and Computer Engineering*, vol. 12, no. 6, pp. 6545–6558, 2021.

**[13]** G. Luo, L. Shi, T. Huang and Z. Shi, ”Quantum Image Reversible Watermarking Scheme Using A Combination Of The Most Significant Qubit And The Least Significant Quit,” *Journal of Engineering Science and Technology Review*, vol. 13, no. 3, pp. 52 – 58, 2020.

**[14]** O. Y. Abdulhammed, ”Improving Encryption Digital Watermark by Using Blue Monkey Algorithm,” *International Journal of Computing*, vol. 20, no. 1, pp. 129-136, 2021.

**[15]** A. K. Singh,” Robust and Distortion Control Dual Watermarking In LWT Domain Using DCT And Error Correction Code For Color Medical Image, ”*Multimedia Tools and Applications*, vol. 78, no. 2019, pp. 30523–30533, 2019.

**[16]** S. Borra and R. M. Thanki, “Crypto-Watermarking Scheme for Tamper Detection of Medical Images, ”*Computer Methods in Biomechanics and Biomedical Engineering*, vol. 8, no. 4, pp. 345–355, 2020.

**[17]** M. Lebcir, S. Awang and A. Benzian, “Robust Blind Watermarking Approach Against The Compression For Fingerprint Image Using 2D-DCT,” *Multimedia Tools and Applications*, vol. 81, no. 15, pp. 20561–20583, 2022.

**[18]** M. Begum, J. Ferdush and M. S. Uddin, ”A Hybrid Robust Watermarking System Based on Discrete Cosine Transform, Discrete Wavelet Transform and Singular Value Decomposition,” *Journal of King Saud University: Computer and Information Sciences*, vol. 34, no. 4, pp. 5856-5867, 2021.

**[19]** A. Alzahrani and N. A. Memon, ”Blind and Robust Watermarking Scheme in Hybrid

Domain for Copyright Protection of Medical Images," *IEEE Engineering In Medicine And Biology Society Section*, vol. 9, no. 2021, pp. 113714–113734, 2021.

**[20]** B. Mohammed, S. Hasan, Siddeeq Y. and O. Mohammed Salih," Image Authentication Based on Watermarking Approach: Review", *Asian Journal of Research in Computer Science,* vol. 9, no.3, pp. 34-51, 2021.

**[21]** V. Raj, S. Janakiraman, S. Rajagopalan and R. Amirtharajan, "Security Analysis of Reversible Logic Cryptography Design with LFSR Key on 32-Bit Microcontroller," *Microprocess. Microsystems*, vol. 84, 104265, 2021.