International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 33 العدد
Part 2 المجلد
January 2024 يناير
المجلة الدولية للعلوم والتقنية
ISTJ
تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

Digital Image Watermarking Methods Based on Transformation Techniques: A Comparative Study

Rabha O. Abd-Elsalam [1], Sahar Q. Saleh [2]

Department of Computer Science-Faculty of Arts and Sciences
Tocra University, Benghazi -Libya [1]
Department of Computer Science -Taiz University - Taiz, Yemen [2]
rabha.omar@uob.edu.ly, sahar.qasim2009@gmail.com

Abstract

Digital watermarking is one of the data-hiding methods, which embeds the watermark data into the digital multimedia content. The two important requirements for watermarking methods are imperceptibility and robustness. This paper presents a comparative study of transformation techniques, which are discrete wavelet transform, discrete cosine transform, and discrete Fourier transform that have been used in the field of digital image watermarking. The paper uses the peak signal-to-noise ratio measure as a basic metric for comparing the transparency attribute of the watermarking methods. Whereas the correlation coefficient metric is adapted to test the resistivity of the watermarking methods to different attacks. Moreover, the paper examines the combination of the singular value decomposition technique with the other transformation techniques in terms of exploring whether the combination will enhance the result or not. The experimental results show that the discrete wavelet transform and the discrete wavelet transform combined with the singular value decomposition outperform the state-of-the-art method and enhance both the imperceptibility and the robustness with less computational time when the watermarked image is not subjected to any attack.

International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 33 العدد
Part 2 المجلد
January 2024 يناير
المجلة الدولية للعلوم والتقنية
ISTJ
تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

Keywords—Image watermarking; robustness; imperceptibility; singular values decomposition; discrete wavelet transform; discrete cosine transform; discrete Fourier transform.

طرق وضع العلامات المائية على الصور الرقمية بناءً على تقنيات التحويل (دراسة مقارنة)

رابحة عمر عبدالسلام محمد [1]، سحر قاسم قائد صالح [2]
قسم الحاسوب–كلية الاداب والعلوم– توكرة – جامعة بنغازي– ليبيا [1]
قسم علوم الحاسوب – جامعة تعز – تعز، اليمن [2]
sahar.qasim2009@gmail.com , rabha.omar@uob.edu.ly1

الملخص

تعد العلامة المائية الرقمية إحدى طرق إخفاء البيانات، والتي تقوم بدمج بيانات العلامة المائية في محتوى الوسائط المتعددة الرقمية. المتطلبان المهمان لطرق وضع العلامات المائية هما عدم القدرة على الإدراك والمتانة. يقدم هذا البحث دراسة مقارنة لتقنيات التحويل، وهي تحويل الموجات المنفصلة (discrete wavelet transform)، تحويل جيب التمام المنفصل (discrete cosine transform)، وتحويل فورييه المنفصل (discrete Fourier transform) حيث تم استخدام هذه التقنيات في مجال العلامات المائية للصور الرقمية. يستخدم هذا البحث مقياس ذروة نسبة الإشارة إلى الضوضاء (peak signal–to–noise ratio) كمقياس أساسي لمقارنة سمة الشفافية لطرق وضع العلامات المائية. كما تم استخدام مقياس معامل الارتباط (correlation coefficient) لاختبار مقاومة طرق وضع العلامة المائية للهجمات المختلفة. علاوة على ذلك، تم بحث طريقة الجمع بين تقنية تحليل القيمة المفردة (singular value decomposition) مع تقنيات التحويل الثلاثة من أجل استكشاف ما إذا كان الجمع سيعزز النتيجة أم لا. تظهر النتائج التجريبية أن تحويل الموجات المنفصلة وتحويل الموجات المنفصلة جنبًا إلى جنب مع تحليل القيمة

تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

المفردة يتفوقان على أحدث طريقة في الدراسات السابقة ويعززان كلاً من عدم القدرة على الإدراك والمتانة مع وقت حسابي أقل وذلك عندما لا تتعرض الصورة ذات العلامة المائية إلى أي نوع من الهجوم.

الكلمات المفتاحية: العلامة المائية للصورة، المتانة، عدم القدرة على الإدراك، تحليل القيم المفردة، تحويل الموجات المنفصلة، تحويل جيب التمام المنفصل، تحويل فوريه المنفصل.

INTRODUCTION

The rapid development of the Internet and communications media has led to the availability of digital multimedia such as images, audio, and video that has become suitable for sharing digital information. As a result of the popularity of the Internet, it is easy to access digital media, make illegal changes, duplicate, distribute, and reproduce digital information without any degradation of quality. This has led to the development of many methods that concern copyright issues. Watermarking, cryptography, and steganography are different techniques that resolve the issues of trusted communication and digital data integrity [1]. Digital watermarking is a data-hiding technique, which embeds either watermark data or a digital signature into digital multimedia content. The watermark can be obtained or detected from the multimedia file to identify the owner of the copyright. Watermarking methods ensure authentication, tamper resistance, integration, and content verification of the media [2]. It is difficult to remove a watermark by converting the watermarked data into other file formats. Thus, it is probable to gain information about the data transformation from the watermark after a given attack. Digital watermarking methods can also be used to survive compression, digital-to-analog conversion, re-encryption, decryption, and file format changes, in addition to other kinds of data loss [3].

تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

Watermarking and steganography are data-hiding methods where they hide secret data in the cover media. However, there is a difference between these two methods. Steganography hides the existence of the secret data. This method fails when the presence of secret data is detected, contrary to the watermarking method, where the presence of secret data can be identified [4]. The goal of watermarking is to make the secret data hard to manipulate or remove. On the other hand, cryptography does not conceal the presence of secret data but ciphers the data in such a way that it looks useless to hackers when deciphered with the appropriate key[5, 6].

A digital watermarking method consists of a cover image, a watermark image, an encoding algorithm, and a decoding algorithm. Figure 1 depicts the block diagram of the digital watermarking method. Different algorithms have been presented in the literature to keep the digital images [7-10]. The watermark embedding methods can be categorized into two groups: spatial-domain and frequency-domain methods. Spatial-domain embedding methods are easy to implement and have a short execution time. However, these methods are usually vulnerable and fragile when subjected to various attacks. Contrary to the frequency-domain methods that are robust against many attacks because more information has been embedded in the image. Frequency-domain methods embed the watermark in the transform coefficients, for instance, discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete Fourier transform (DFT), finite ridgelet transform (FRT), wavelet packet transform (WPT), and singular value decomposition (SVD) [11-19]. The execution time of frequency-domain methods is longer than that of spatial-domain methods.

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

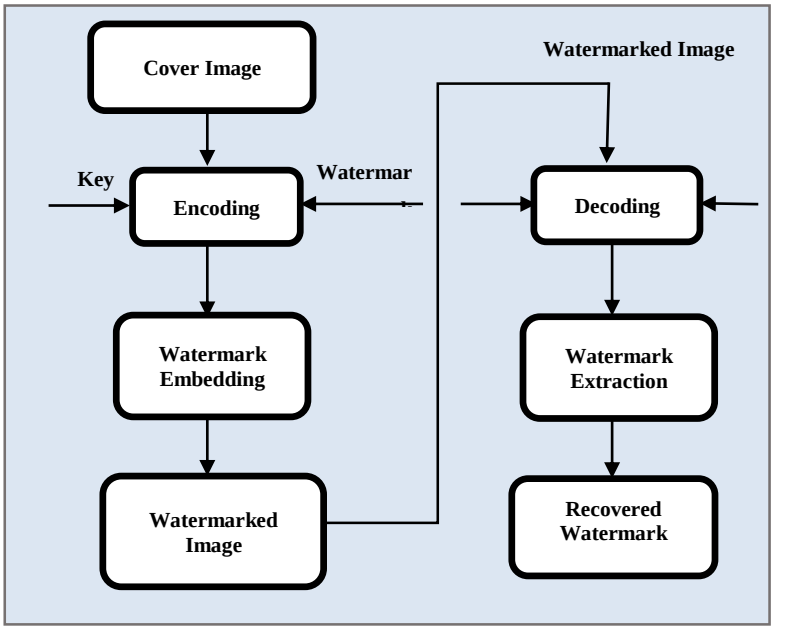

Figure 1. The block diagram of digital watermarking technique.

Digital watermarking algorithms can be classified based on robustness criteria into three groups: fragile, semi-fragile, and robust [3, 20]. Fragile watermarking methods are easy to implement but are unable to resist signal processing attacks. Fragile watermarks are used for the integrity protection of multimedia data when signature information is inserted. This watermark verifies if there is any tampering [21]. Semi-fragile watermarking methods sense any unauthorized alteration. These methods can be used for image authentication [22]. Robust watermarking methods preserve the embedded watermark even if the watermarked image undergoes several attacks. These methods are suitable for copyright protection, fingerprinting, copy control, and broadcast monitoring [21].

Different applications, which use watermarking schemes, have several characteristics and requirements that need to be fulfilled.

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

The requirements considering legal copyright protection and ownership are mentioned below [23].

- Robustness: The watermark is kept and can be detected after some manipulation operations and attacks that have been applied to digital image watermarking systems.
- Imperceptibility: The human vision system should not be able to notice the embedded watermark in the original image. The watermark is embedded by using specialized procedures that maintain the quality of the image content.
- Capacity: The amount of information that can be concealed in the original image.
- Security: It is impossible to read, alter, or remove the watermark by an unauthorized person. However, the watermark must be correctly recovered by the authorized user.

Watermarking requirements conflict with each other. Thus, the watermarking schemes must maintain a good trade-off among these requirements. There are many watermarking systems in the spatial domain and transform domain that make efforts to balance inconsistent requirements [3, 24].

This paper is structured as follows: A background review is introduced in section 2, which includes a brief explanation of SVD, DWT, DCT, and DFT. Section 3 introduces the watermarking methods. The experimental results are displayed and discussed in section 4. In the end, this paper is concluded with some remarks on future work in section 5.

BACKGROUND REVIEW

A. Singular Values Decomposition

The SVD is an efficient tool used to analyze the digital image where the singular value of the image has good stability. Therefore, any slight alteration to the cover image does not have much effect

تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

on the image quality. The largest value of SVD causes the smallest change in the cover image. A digital image is represented as a two-dimensional matrix of non-negative values. The SVD tool factorizes a given image I with size M×N, where M≤ N, into three matrices: U, S, and V.

$$I=U*S*V^T \quad (1)$$

Where U and V are orthogonal matrices (U and V columns are left and right singular vectors, respectively, of an image I) and S is a diagonal matrix of singular values γ_j, $j=1, 2, ..., M$ whose diagonal entries satisfy:

$$\gamma_1 \geq \gamma_2 \geq \gamma_3 \geq \cdots \geq \gamma_r > \gamma_{r+1} = \cdots = \gamma_m = 0 \quad (2)$$

Where: r is the rank of I, which equals the number of non-zero singular values in S. The diagonal inputs of S are positive square roots of the eigen values of $I\,I^T$ or $I^T\,I$, and are namely the singular values of I.

As a result of the main characteristics of SVD, the watermark image can be embedded into the cover image by changing its singular values. A large change in the singular values of an image will not affect its visual properties [25].

B. **Discrete Wavelet Transform**

DWT has been widely used in the field of signal processing applications like internet communications media, video compression, pattern recognition, and image watermarking. The high corresponding between the wavelet domain and the human visual system (HVS) leads to the usage of such a technique in digital image watermarking. DWT has many attractive features; one of those attractive features is the multi-scale representation of function. DWT manages a given image by splitting it into four non-overlapping multi-resolution sub-bands: LL (A), LH (V), HL (H)

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

and HH (D). The LL sub-band represents the highest coarse level of the DWT coefficients (the image approximation), whereas the other sub-bands represent the lowest coarse level of the DWT coefficients (the image details). Figure 2 gives a pictorial illustration of such a concept. Another attractive feature of DWT is the similarity of the data structure concerning the resolution and the availability of decomposition at any level. To develop an alternative level of decomposition, DWT can be implemented as a multistage process. The LL sub-band decomposition process can be implemented recursively until it reaches the desired decomposition level specified by the application. DWT ignores the embedding of the watermark in LL sub-bands and uses the other sub-bands for embedding to reduce the image distortion [26].

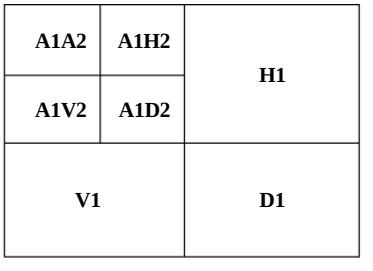

Figure 2**.** The structure of two-level wavelet

C. Discrete Cosine Transform

DCT technique converts the original signal to its basic frequency components. This technique manipulates and considers the image as a combination of sinusoids of various magnitudes and frequencies. The block-based DCT transform accomplishes the transformation process in two steps: segmenting the input image into non-overlapping blocks and then applying DCT to each block separately. The results are three frequency coefficient sets: low-frequency, mid-frequency, and high-frequency sub-bands. Two important facts are behind the usage of DCT in image watermarking.

تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

Firstly, much of the signal energy is contained in low-frequency sub-bands, which in turn contain the very significant visual attributes of the image. Secondly, high-frequency components are removed, usually through noise and compression attacks. Thus, the watermark is then reasonably embedded in the coefficients of the mid-frequency sub-bands, where the visual properties of the image do not distort and hence guarantee high-quality watermarking techniques [27].

D. **Discrete *Fourier Transform***

DFT transforms or converts the input images from one domain called the spatial domain to another domain called the frequency domain. DFT is considered one of the most significant image processing tools that is used to decompose the input image into its basic sine and cosine components. In the frequency domain image, every point represents a particular frequency contained in the spatial domain image. The image obtained after DFT is complex. DFT is computed using the fast Fourier transform (FFT) algorithm, accordingly, the DFT and FFT are often used interchangeably. DFT technique can be employed in a variety of applications, such as image reconstruction, image compression, image filtering, image analysis, and image watermarking [28].

WATERMARKING METHODS

Each watermarking method has two phases: the watermark embedding phase and the watermark extraction phase. This work uses DWT, DCT and DFT transformations. The SVD technique is combined with the other techniques to study the enhancement of the results of the watermarking method. The following subsections describe those methods.

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

A. **DWT Watermarking**

This section explains the watermarking method using DWT only.

1) Watermark embedding phas:Assume that the cover image A is an $M\times N$ gray-level image and the watermark W is an $X\times Y$ gray-level image. Firstly, the cover image is decomposed using the discrete wavelet transform of 1-level to get a multi-resolution representation of the image. The process of the watermark embedding is illustrated through the following steps:
   - Decompose the cover image A using the single-level Haar transformation.
   - Select a sub-band from the *H1*, *V1*, or *D1* sub-bands.
   - Change the coefficients of the selected sub-band in the cover image with the values of the watermark image $S'=S+\alpha W$, where S represents the coefficients values of the selected sub-band of the cover image, W represents the values of the watermark image, and αsignifies the scalar factor.
   - Obtain the watermarked image $W_A$by executing the single-level inverse discrete wavelet transform (IDWT) using the modified sub-band.

2) Watermark extraction phase:It is the reverse process of the watermark embedding phase. It can be described in the following steps:
   - Decompose the watermarked image W_A and the cover image A using the single-level Haar transformation.
   - Select the sub-band from *H1*, *V1*, or *D1* sub-bands.
   - Extract the watermark image from the selected sub-band $W' = (S' - S)/\alpha$ where W'denotes to the extracted watermark image, S' represents the coefficients of the sub-band of the watermarked image, $\mathcal{S}$ represents the

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

coefficients of the cover image sub-band and α is the value of the scalar factor.

B. **DWT-SVD Watermarking**

This watermarking method applies the singular values decomposition technique along with discrete wavelet transform. The process of watermarking goes through two main phases; watermark embedding and watermark extraction, which can be explained in the next sub-sections.

1) Watermark embedding phase: The steps of the embedding phase are described below.
   - Decompose the cover image *A* using the single-level Haar transformation.
   - Select a sub-band from the *H1*, *V1*, or *D1* sub-bands.
   - Apply SVD to the selected sub-band $A_b = U_b S_b V_b^T$ where b represents the selected sub-band. Additionally, apply SVD to the watermark image $W = U_w S_w V_w^T$ where W represents the watermark image.
   - Change the singular values of the selected sub-band in the cover image with the singular values of the watermark image $S_b' = S_b + \alpha S_w$, where S_b represents the singular values of the selected sub-band, S_w signifies the singular values of the watermark image, and α is the value of the scalar factor.
   - Reconstruct the sub-band using the new singular value matrix.
   - Obtain the watermarked image W_A by executing the IDWT using the modified sub-band.

2) Watermark extraction phase:The watermark extraction can be summarized as:

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

- Decompose the watermarked image W_A and the cover image *A* using the single-level Haar transformation.
- Select the sub-band from *H1*, *V1*, or *D1* sub-bands.
- Apply SVD to the selected sub-band of the watermarked image$W_{Ab} = U_b S_b' V_b^T$ and the cover image $A_b = U_b S_b V_b^T$.
- Extract the singular values of the watermark image from the selected sub-band $S_w' = (S_b' - S_b)/\alpha$.
- Construct the extracted watermark image using the singular vectors $W' = U_w S_w' V_w^T$.

C. ***DCT Watermarking***

This approach uses DCT transform for the watermarking scheme.

1) Watermark embedding phase: The steps of the embedding phase are described below.

- Split the cover image *A* into non-overlapped blocks where the block size is *2×2*.
- Apply DCT on each block of the cover image.
- Scramble the pixels of the watermark image *W* by using the Zig-Zag scan. It can be denoted by W_{scr}.
- Change the DCT coefficient of the pixel (2,2) in all blocks of the cover image with the values of the watermark image pixels W_{scr}.

$$Block(i)\_DCT(2,2) = Block(i)\_DCT(2,2) + \alpha * W_{scr}(i)$$

Where $i = 1,2, \dots, X \times Y$.

- Perform the inverse discrete cosine transform (IDCT) on each block.
- Obtain the watermarked image W_A by combining the blocks into one matrix.

2) Watermark extraction phase: The extraction process is the inverse of the embedding process. It can be implemented as follows.

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

- Divide the watermarked image W_A and the cover image A into non-overlapped blocks where the block size is *2×2*.
- Apply DCT on each block of the watermarked image W_A and the cover image *A*.
- Extract the scrambled watermark image W'_{scr}.
  $W'_{scr}(i) = Watermarked_{Block(i)_{DCT(2,2)}} - Cover\_Block(i)\_DCT(2,2)/\alpha$, where $i = 1,2,\dots,X \times Y$.
- Do the inverse Zig-Zag scan to get the extracted watermark image.

D. ***DCT-SVD Watermarking***

This watermarking method uses the DCT in addition to the SVD technique.

1) Watermark embedding phase: This phase can be summarized in the next steps:

- Split the cover image *A* into non-overlapped blocks where the block size is *2×2*.
- Apply the DCT and SVD respectively on each block of the cover image.
- Scramble the pixels of the watermark image by using the Zig- Zag scan.
- Change the singular values of the pixel (2, 2) in all blocks of the cover image with the values of the watermark image pixels W_{scr}.
  $Block(i)\_DCT\_SVD(2,2) = Block(i)\_DCT\_SVD(2,2) + \alpha * W_{scr}(i)$, where $i = 1,2,\dots,X \times Y$.
- Reconstruct the blocks using the new singular value matrices.
- Execute the IDCT on each block.
- Get the watermarked image W_A by combining the blocks into one matrix.

تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

2) Watermark extraction phase: This is the inverse process of embedding. Its steps are:

- Divide the watermarked image W_A and the cover Image A into non-overlapped blocks where the block size is *2×2*.
- Apply DCT and SVD respectively on each block of the cover image A and the watermarked image W_A.
- Extract the scrambled watermark image.

$$W'_{scr}(i) = Watermarked\_Block(i)\_DCT\_SVD(2,2) - Cover\_Block(i)\_DCT\_SVD(2,2)/\alpha,$$

where $i = 1,2,\dots,X \times Y$.

- Do the inverse Zig-Zag scan to get the extracted watermark image.

E. ***DFT Watermarking***

This method employs DFT for the watermarking scheme.

1) Watermark embedding Phase:This phase goes through the following steps:

- Divide the cover image A into non-overlapped blocks where the block size is 2×2.
- Apply DFT on each block of the cover image.
- Scramble the pixels of the watermark image W by using the Zig-Zag scan. It can be denoted by W_{scr}.
- Modify the DFT coefficient of the pixel (2,2) in all blocks of the cover image with the values of the watermark image pixels W_{scr}.

$$Block(i)\_DFT(2,2) = Block(i)\_DFT(2,2) + \alpha * W_{scr}(i)$$

where $i = 1,2,\dots,X \times Y$.

- Do the inverse discrete Fourier transform (IDFT) on each block.

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

- Get the watermarked image W_A by combining the blocks into one matrix.

2) Watermark extraction phase:This phase can be described in the following steps:
   - Split the watermarked image W_A and the cover image A into non-overlapped blocks where the block size is *2×2*.
   - Apply DFT on each block of the watermarked image W_A and the cover image *A*.
   - Extract the scrambled watermark image W'_{scr}. $W'_{scr}(i) = Watermarked\_Block(i)\_DFT(2,2) - Cover\_Block(i)\_DFT(2,2)/\alpha$, where $i = 1,2, \dots, X \times Y$.
   - Perform the inverse Zig-Zag scan to get the extracted watermark image.

F. **DFT-SVD Watermarking**

In this watermarking method, SVD is combined with DFT.

1) Watermark embedding phase: The watermark embedding steps are summarized as follows.
   - Divide the cover image *A* into non-overlapped blocks where the block size is *2×2*.
   - Apply DFT then apply SVD on each block of the cover image.
   - Scramble the pixels of the watermark image by using the Zig-Zag scan.
   - Modify the singular values of the pixel (2,2) in all blocks of the cover image with the values of the watermark image pixels W_{scr}. $Block(i)\_DFT\_SVD(2,2) = Block(i)\_DFT\_SVD(2,2) + \alpha * W_{scr}(i)$, where $i = 1,2, \dots, X \times Y$.
   - Reconstruct the blocks using the new singular value matrices.

تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

- Implement the IDFT on each block.
- Get the watermarked image W_A by combining the blocks into one matrix.

2) Watermark extraction phase: The steps of this reverse process to the embedding are implemented as follows.

- Split the watermarked image W_A and the cover Image A into non-overlapped blocks where the block size is 2×2.
- Apply DFT and SVD respectively on each block of the cover image A and the watermarked image W_A.
- Extract the scrambled watermark image.

$$W'_{scr}(i) = Watermarked\_Block(i)\_DFT\_SVD(2,2) - Cover\_Block(i)\_DFT\_SVD(2,2)/\alpha,$$
where $i = 1,2,\dots,X \times Y$.

- Perform the inverse Zig-Zag scan to get the extracted watermark image.

EXPERIMENTAL RESULTS

The presented watermarking methods using transformation techniques have been implemented in Matlab R2015a with Windows 11 edition environment on an Intel(R) Core(TM) i7 CPU with 16GB RAM. The performance of the watermarking methods was measured in terms of imperceptibility and robustness to various types of signal processing attacks. The imperceptibility requirement of the presented methods was evaluated using the peak signal-to-noise ratio (PSNR) metric. The value of PSNR must be infinite, but it is impossible for the watermarked image. Therefore, the large value of PSNR is desirable and indicates that the two images are very similar [29]. The PSNR for an image with $N\times N$ size is computed using the formula,

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

$$PSNR=10\times\log_{10}\left(\frac{255^2}{\frac{1}{N\times N}\sum_{i=1}^{N}\sum_{j=1}^{N}(A(i,j)-B(i,j))^2}\right) \quad (3)$$

Where A and B is the cover and watermarked images, respectively.

The robustness requirement of the presented methods was evaluated using the correlation coefficient (Cr) metric. The value of Cr must be one, but it is impossible for the extracted image. Therefore, a close value of Cr to one is required [30]. The Cr for an image with $N\times N$ size is computed using the formula,

$$C_r=\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(A_{ij}-\bar{A})(B_{ij}-\bar{B})}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}(A_{ij}-\bar{A})^2 * \sum_{i=1}^{N}\sum_{j=1}^{N}(B_{ij}-\bar{B})^2}} \quad (4)$$

Where $\bar{A}$ is the average value of the original watermark image, and $\bar{B}$ is the average value of the extracted watermark image.

Many experiments have been conducted to evaluate and compare the presented methods. The experiments were carried out using the Cameraman image with the size of 512×512 as the cover image whereas the watermark image was the CS logo Copyright big with the size 256×256. Additionally, the experiments were carried out on different values of scale factor for the former mentioned techniques to study its impact on the performance and the relation between PSNR and Cr. As soon as the value of scale factor increased, the value of Cr also increased whereas the value of PSNR decreased. The better values of the scale factor for the presented watermarking methods without any attack were recorded and shown in Table 1.

This paper presented three transformation techniques: DWT, DCT and FFT for watermarking methods. Additionally, these transformation techniques were combined with SVD technique to see if it can enhance the results. The DWT decomposes the image

تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

into 4 sub-bands. The human visual system is more sensitive to low-frequency therefore the HH (high-high) sub-band is chosen in this paper to save the quality of the cover image during embedding the watermark image. Table 1 show the results of the presented watermarking methods when the watermarked image was not subjected to any attack. DWT gave the best result for the *PSNR* metric, which is 49.1968 and took a short execution time equals to *0.4858* second. The *Cr* robustness metric is *0.9942*. DWT gave better results than the other methods for PSNR and execution time. It is simple to implement and supports imperceptibility, which ensures better PSNR values with less computational time. However, the DWT-SVD method slightly improved the value of the *Cr* metric reached up to 0.9996. The watermarking methods using DWT and DWT-SVD outperform the method BSVD-SVD in [19] without attack.

TABLE 1.THE RESULTS OF WATERMARKING METHODS USING TRANSFORMATION TECHNIQUES WITHOUT ANY TTACK.

Method	Scale Factor	PSNR	Cr	Execution Time (Second)
DWT	0.011	49.196800	0.994217	0.485897
DWT-SVD	0.011	46.269515	0.999623	1.125349
DCT	0.0085	46.604345	0.98996	114.965
DCT-SVD	0.0080	45.743502	0.979664	116.05028
DFT	0.04	40.022413	0.997121	24.359928
DFT-SVD	0.5	11.648529	0.966347	25.998924
BSVD-SVD [19]	0.01	45.8605	0.9975	7.900

Figures 3, 4 and 5 show the watermarked and extracted images of the presented watermarking methods. The first row in the Figure 3

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

shows the cover image and the watermark image respectively. Whereas the second row indicates the watermarked image (PSNR=49.1968) and the extracted image (CR=0.9942) respectively using the DWT method. The third row in Figure 3 shows the watermarked image (PSNR=46.2695) and the extracted image (CR=0.9996) respectively using the DWT-SVD method. As demonstrated in Figure 4, the second row shows the watermarked image (PSNR=46.6043) and the extracted image (CR=0.98996) respectively using the DCT method.

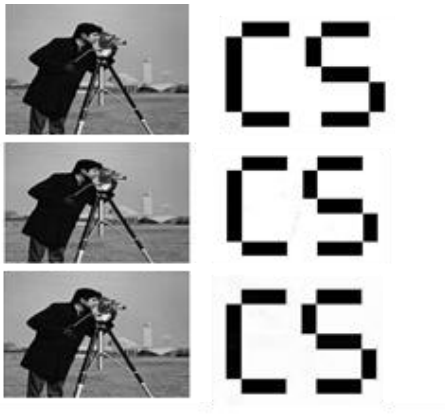

Figure 3. The first row indicates the cover image and the watermark image respectively. Whereas the second row shows the watermarked image (PSNR=49.1968) and the extracted image (CR=0.9942) respectively using DWT method. The third row shows the watermarked image (PSNR=46.2695) and the extracted image (CR=0.9996) respectively using DWT-SVD method

تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

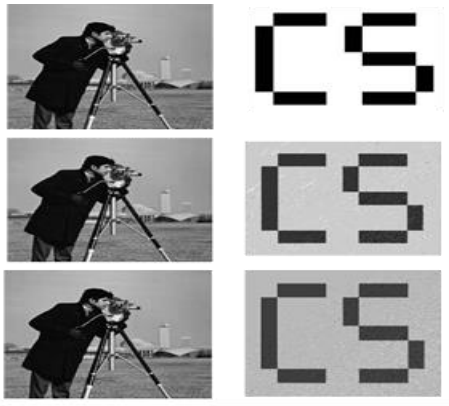

Figure 4. The first row shows the cover image and the watermark image respectively. Whereas the second row indicates the watermarked image (PSNR=46.6043) and the extracted image (CR=0.98996) respectively using DCT method. The third row shows the watermarked image (PSNR=45.7435) and the extracted image (CR=0.97966) respectively using DCT-SVD method

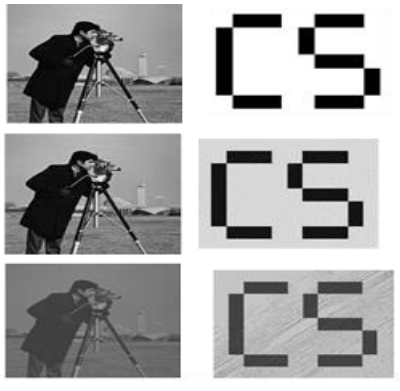

Figure 5. The first row indicates the cover image and the watermark image respectively. Whereas the second row shows the watermarked image (PSNR=40.0224) and the extracted image (CR=0.9971) respectively using DFT method. The third row shows the watermarked image (PSNR=11.6485) and the extracted image (CR=0.9663) respectively using DFT-SVD method

تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

Whereas the third row indicates the watermarked image (PSNR=45.7435) and the extracted image (CR=0.97966) respectively using the DCT-SVD method. In Figure 5, the second row shows the watermarked image (PSNR=40.0224) and the extracted image (CR=0.9971) respectively using the DFT method. Whereas the third row shows the watermarked image (PSNR=11.6485) and the extracted image (CR=0.9663) respectively using the DFT-SVD method.

The presented methods have been tested with different types of attacks. These attacks are, salt and pepper noise with a noise density of 0.05 that affects about 5% of image pixels, Gaussian white noise with zero mean and 0.01 variance, cropping noise with 50% of the image, blurring noise with the LPF window of size 3×3, and rotation noise with the 45 angle. Table 2 shows the results in terms of the different attacks on the watermarked image. The value of Cr is 0.6984, which was the best result with the DWT method when salt and pepper noise was applied to the watermarked image. The best result of Cr is 0.6297 with DFT when Gaussian noise was applied to the watermarked image. However, all the presented methods gave bad results in terms of Cr when blurring noise was applied to the watermarked image. Here, DFT-SVD gave the best result for Cr equals to 0.4028 when the cropping noise was applied to the watermarked image. The presented methods failed with rotation noise where they gave bad result. It has been noticed that the presented methods were not robust when the watermarked image was subjected to different attacks. Additionally, SVD did not enhance the result when it was combined with the other transformations. Figures 6, 7, 8, 9, 10 and 11 show the watermarked and extracted images of the presented transform methods with different attacks. Figure 6 and 7 show images using DWT and DWT-SVD methods respectively. Figure 8 and 9 indicate images

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

using DCT and DCT-SVD methods respectively. Figure 10 and 11 show images using DFT and DFT-SVD methods respectively.

Table 2 shows that the DWT method took a short execution time. This is because the DWT method decomposes the image into 4 sub-bands, each sub-band with the size of 256×256, and the watermark image is embedded into the HH sub-band. Whereas in the DFT and DCT methods, the cover image is decomposed into 256×256 non-overlapped blocks where each block has the 2×2 size and DCT or DFT was applied on each block.

TABLE2.THE RESULTS OF WATERMARKING METHODS USINGTRANSFORM DOMAIN WITH DIFFERENT ATTACKS.

Attack Type	Evaluation	DWT	DWT-SVD	DCT	DCT-SVD	DFT	DFT-SVD	BSVD-SVD [19]
Salt and Paper Noise	PSNR	18.113822	18.166280	18.127701	18.109918	16.03120	10.941994	-
	CR	0.698417	0.507351	0.016736	0.026779	0.542930	0.477558	-
	Time	0.604645	0.663309	162.519760	187.830695	32.607900	34.819199	-
Gaussian Noise	PSNR	20.381858	20.393768	20.334604	20.327465	17.063017	11.105026	20.3733
	CR	0.027291	0.502102	0.034343	0.000221	0.629705	0.252752	0.5124
	Time	0.607926	0.643754	169.103689	211.663708	36.111998	37.992596	7.176
Blurring Noise	PSNR	34.205850	34.258253	34.072731	33.964700	33.707079	15.227164	20.6968
	CR	-0.109111	-0.011889	-0.012842	-0.006958	0.060913	0.007518	0.1360
	Time	1.182370	1.359409	218.354622	326.614177	54.941644	63.035590	11.530
Cropping Noise	PSNR	7.940428	7.940240	7.940256	7.940112	7.939067	7.123138	7.8124
	CR	0.365021	-0.200416	0.127194	0.263104	0.394211	0.402806	0.2529
	Time	0.555928	0.632024	216.107113	283.525819	70.544024	76.232315	8.728
Rotation Noise	PSNR	9.300874	9.298014	9.317279	9.329769	9.347198	8.734331	6.5558
	CR	-0.015734	-0.094198	0.001358	0.010410	0.004910	0.015121	0.5281
	Time	0.637065	0.651289	218.784722	308.12861	36.200532	41. 20854	-

After scrambling the pixels of the watermark image by using the Zig-Zag scan, the values of the pixel (2,2) in each block have been changed with the values of the Scramble watermark. Additionally, the DCT method took a longer execution time than the DFT method. The MATLAB functions fft2 and dct were used to do discrete transformations on images. The dct function uses a direct

تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

method that calculates DCT. Here, the fft2 function is used to calculate the 2D fast Fourier transform of an image. It is a method that computes the DFT with reduced execution time. The fft2 function is an efficient and fast method that exploits some mathematical properties of the DFT that the DCT does not have.

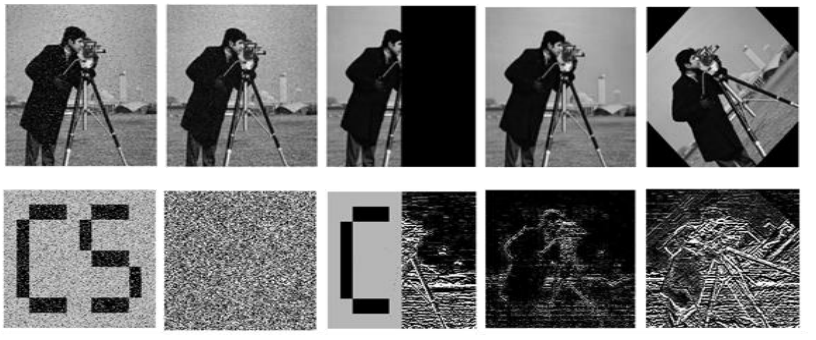

Figure 6.Shows images using the DWT method. The first row shows the watermarked image whereas the second row shows the extracted watermark with salt-paper-noise, Gaussian-noise, cropping-noise, blurring-noise, and rotation-noise, respectively

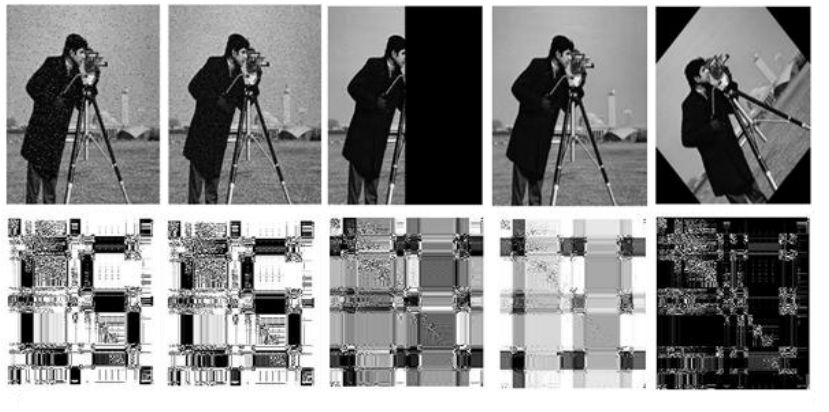

Figure 7. Shows images using the DWT-SVD method. The first row shows the watermarked image whereas the second row shows the extracted watermark with salt-paper-noise, Gaussian-noise, cropping-noise, blurring-noise, and rotation-noise, respectively

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

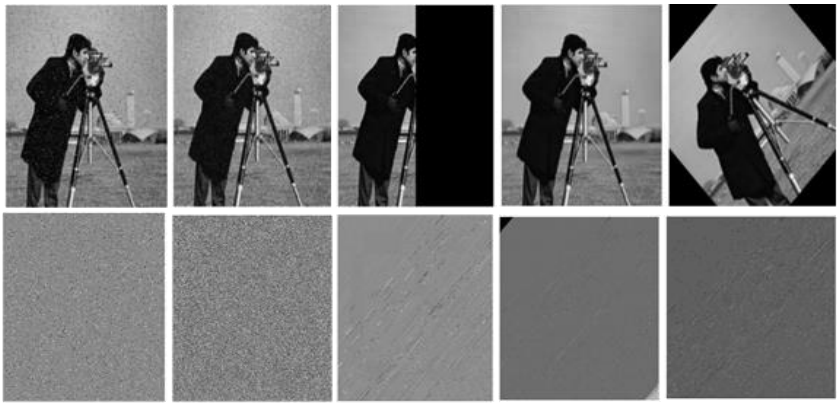

Figure 8.Shows images using the DCT method. The first row shows the watermarked image whereas the second row shows the extracted watermark with salt-paper-noise, Gaussian-noise, cropping-noise, blurring-noise, and rotation-noise, respectively.

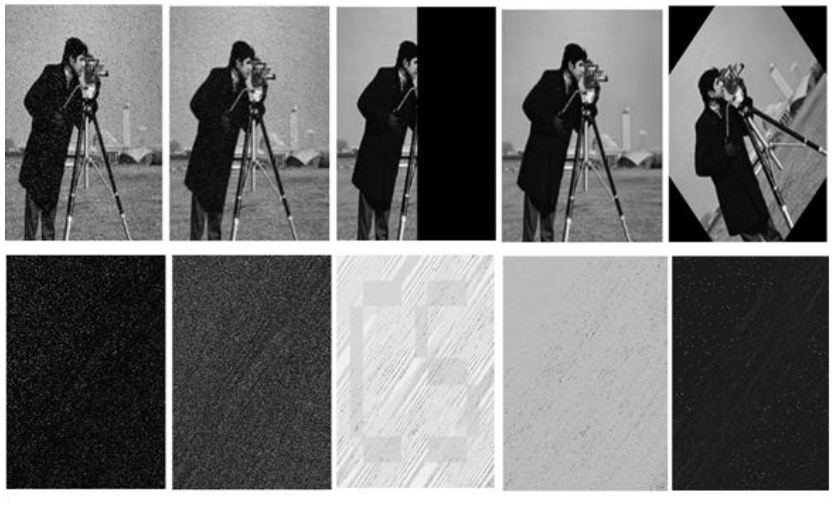

Figure 9. Shows images using the DCT-SVD method. The first row shows the watermarked image whereas the second row shows the extracted watermark with salt-paper-noise, Gaussian-noise, cropping-noise, blurring-noise, and rotation-noise, respectively.

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

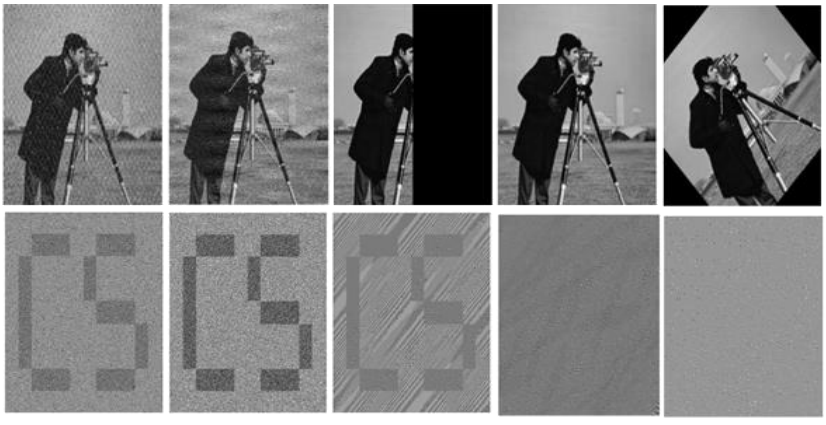

Figure 10. Shows images using the FFT method. The first row shows the watermarked image whereas the second row shows the extracted watermark with salt-paper-noise, Gaussian-noise, cropping-noise, blurring-noise, and rotation-noise, respectively

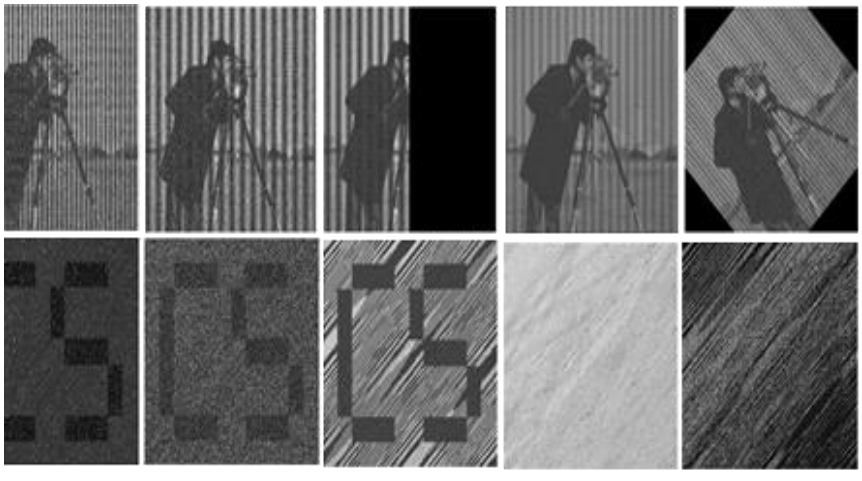

Figure 11.Shows images using the FFT-SVD method. The first row shows the watermarked image whereas the second row shows the extracted watermark with salt-paper-noise, Gaussian-noise, cropping-noise, blurring-noise, and rotation-noise, respectively

تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

CONCLUSION AND FUTURE WORK

The most important requirements of watermarking techniques are imperceptibility and robustness. Some of the watermarking applications require image quality and robustness like military and medical imagery. This paper presented some transformation techniques, which are DWT, DCT and DFT that are used in the field of digital image watermarking process. The performance of those techniques was compared individually and in combination with singular values decomposition. The findings showed that the DWT and DWT-SVD are the best methods, which support imperceptibility and high robustness. DWT and DWT-SVD ensure better PSNR and Cr values with less computational time when the watermarked image is not subjected to any attack. DWT and DWT-SVD outperform state-of-the-art method. The presented methods preserve imperceptibility, and when the watermarked image is subjected to different attacks, the methods will become fragile. Fragile watermarks are used for the integrity protection of multimedia data when signature information is inserted. This watermark verifies if there is any tampering.

In the future, an optimization method can be used to seek the appropriate scale factors that can improve the results, which preserve the image quality and robustness against different attacks.

REFERENCES

[1] L. Singh, A.K. Singh, & P.K. Singh, "Secure data hiding techniques: a survey." Multimedia Tools and Applications 79 (2020), pp. 15901-15921.

[2] H. Tao, L. Chongmin, J.M. Zain, & A.N. Abdalla, "Robust image watermarking theories and techniques: A review." Journal of applied research and technology 12.1 (2014), pp.122-138.

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

[3] M. Begum, M. S. Uddin, "Digital image watermarking techniques: a review." Information 11.2 (2020). pp. 110.
[4] I. J. Cox, M. L. Miller, J. A. Bloom, & C. Honsinger, Digital Watermarking. LNCS, (2002). vol. 53.
[5] R. Chamlawi, A. Khan, "Digital image authentication and recovery: employing integer transform based information embedding and extraction." Information Sciences 180.24 (2010). pp. 4909-4928.
[6] I. Cox, M. Miller, J. Bloom, J. Fridrich, & T. Kalker, Digital watermarking and steganography. Morgan kaufmann, (2007).
[7] T. V. Nguyen, J. C. Patra, "A simple ICA-based digital image watermarking scheme." Digital Signal Processing 18.5 (2008). pp. 762-776.
[8] S. D. Muyco, A. A. Hernandez, Least significant bit hash algorithm for digital image watermarking authentication. In: Proceedings of the 2019 5th International Conference on Computing and Artificial Intelligence. (2019). pp. 150-154.
[9] A. M. Zeki, A. A. Manaf, "A novel digital watermarking technique based on ISB (Intermediate Significant Bit)." World Academy of Science, Engineering and Technology 50 (2009). pp. 989-996.
[10] G. N. Mohammed, A. Yasin, & A. M. Zeki, Robust image watermarking based on dual intermediate significant bit (DISB). In: 2014 6th International Conference on Computer Science and Information Technology (CSIT). IEEE, (2014). pp. 18-22.
[11] Al-Otum, & H. M, "Secure and robust host-adapted color image watermarking using inter-layered wavelet-packets." Journal of Visual Communication and Image Representation 66 (2020). 102726.
[12] Al-Otum, H. M, "Image watermarking based on inter-tree coefficients differencing in paired wavelet-packets tree

تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

constructions." Multimedia Tools and Applications 78.16 (2019). Pp. 22909-22937.

[13] A. M. Ramos, J. A. P. Artiles, D. P. B. Chaves, & C. Pimentel, "A Fragile Image Watermarking Scheme in DWT Domain Using Chaotic Sequences and Error-Correcting Codes." Entropy 25.3 (2023). pp. 508.

[14] G. Azizoglu, A. N. Toprak, "A novel reversible fragile watermarking method in DWT domain for tamper localization and digital image authentication." Biomedical Signal Processing and Control 84 (2023). 105015.

[15] R. Thanki, P. Joshi, Robust Color Image Watermarking Scheme with High Payload Capacity using FRT-SVD. In: 2021 Sixth International Conference on Image Information Processing (ICIIP). IEEE, (2021). pp. 1-6.

[16] M. T. Gaata, An efficient image watermarking approach based on Fourier transform. International Journal of Computer Applications, 136(9) (2016). pp. 8-11.

[17] S. P. Singh, & G. Bhatnagar, A new robust watermarking system in integer DCT domain. Journal of Visual Communication and Image Representation, 53 (2018). pp. 86-101.

[18] V. P. Vishwakarma, & V. Sisaudia, Gray-scale image watermarking based on DE-KELM in DCT domain. Procedia computer science, 132 (2018). pp.1012-1020.

[19] A. F. Eldaoushy, M. I. Desouky, S. A. El-Dolil, A. S. El-Fishawy, & F. E. A. El-Samie, "Efficient hybrid digital image watermarking." Journal of Optics (2023). pp.1-15.

[20] S. Kumar, B. K. Singh, M. Yadav, "A recent survey on multimedia and database watermarking." Multimedia Tools and Applications 79 (2020). pp. 20149-20197.

تم استلام الورقة بتاريخ: 30/ 12/ 2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

[21] J. Liu, & X. He, A review study on digital watermarking. In: 2005 international conference on information and communication technologies. IEEE, (2005). pp. 337-341.

[22] J. Sang, & M. S. Alam, Fragility and robustness of binary-phase-only-filter-based fragile/semifragile digital image watermarking. IEEE Transactions on instrumentation and measurement, 57(3) (2008). pp. 595-606.

[23] G. Bhatnagar, & B. Raman, Wavelet packet transform-based robust video watermarking technique. Sadhana, 37 (2012). pp. 371-388.

[24] A. Khan, & S. A. Malik, A high capacity reversible watermarking approach for authenticating images: exploiting down-sampling, histogram processing, and block selection. Information Sciences, 256 (2014). pp. 162-183.

[25] A. Furqan, & M. Kumar, Study and analysis of robust DWT-SVD domain based digital image watermarking technique using MATLAB. In: 2015 IEEE International Conference on Computational Intelligence & Communication Technology. IEEE, (2015). pp. 638-644.

[26] C. C. Lai, & C. C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition." IEEE Transactions on instrumentation and measurement 59.11 (2010). pp. 3060-3063.

[27] X. B. Kang, F. Zhao, G. Lin, & Y. Chen, "A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength." Multimedia Tools and Applications 77 (2018). pp. 13197-13224.

[28] K. Fares, K. Amine, & E. Salah, "A robust blind color image watermarking based on Fourier transform domain." Optik 208 (2020). 164562.

تم استلام الورقة بتاريخ: 30/ 12/2023م وتم نشرها على الموقع بتاريخ: 30/ 1 /2024م

[29] K. Heylen, & T. Dams, An image watermark tutorial tool using Matlab. In: Mathematics of Data/Image Pattern Recognition, Compression, and Encryption with Applications XI. SPIE, (2008). pp. 109-120.

[30] A. Susanto, C.A. Sari, & E.H. Rachmawanto, Hybrid method using HWT-DCT for image watermarking. In: 2017 5th International Conference on Cyber and IT Service Management (CITSM). IEEE, (2017). pp. 1-5.

[31] B. Ahmed, S. Saleh, & K. Mahar. An Optimized Watermarking Technique Using Wavelet Packet and Singular Value Decomposition. In: International Conference on Recent Advances in Computer Systems. Atlantis Press, (2015). pp. 124-129.

[32] P. Singh, S. Agarwal, & A. Pandey. A hybrid DWT-SVD based robust watermarking scheme for color images and its comparative performance in YIQ and YUV Color Spaces. In: 2013 3rd IEEE International Advance Computing Conference (IACC). IEEE, (2013). pp. 1213-1218.

[33] C. Priya, C. Ramya. "Robust and secure video watermarking based on cellular automata and singular value decomposition for copyright protection." Circuits,Systems, and Signal Processing 40 (2021). pp. 2464-2493.

[34] H. Guo, N.D. Georganas. "Jointly verifying ownership of an image using digital watermarking." Multimedia Tools and Applications 27 (2005). pp. 323-349.