Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 12, No. 3, September 2024, pp. 516~529
ISSN: 2089-3272, DOI: 10.52549/ijeei.v12i3.5710

Efficient Invisible Color Image Watermarking Based on Chaos

Samia BELKACEM[1], Noureddine MESSAOUDI[2]
[1]University of M'hamed BOUGARA, Faculty of Technology, Department of Electrical Systems Engineering, LIMOSE Laboratory, 3500 Boumerdes, Algéria.
[2]University of M'hamed BOUGARA, Faculty of Technology, Department of Electrical Systems Engineering, LIST Laboratory, 35000 Boumerdes, Algeria

Article Info

Article historys:

Received Jul 13, 2024
Revised Aug 4, 2024
Accepted Aug 25, 2024

Keywords:

Attacks
Chaotic map
Copyright protection
Digital image watermarking
DWT
HVS
NTSC
Reverse self-reference image

ABSTRACT

Several difficulties are faced in developing a robust and transparent color image watermarking system, which requires the blending of the human visual system (HVS) during its design. Therefore, employing masks that take into account the features of HVSs has become a very effective tool for boosting robustness requirements without significant alterations in image imperceptibility. The present article offers watermarking strategy for colored images employing a reverse self-reference image in conjunction with the HVS constraint. A color image first undergoes conversion through the Red, Green, and Blue (RGB) format to the National Television Systems Committee (NTSC) space. The reference image is derived from the luminance channel through the discrete wavelet transform (DWT) domain. However, the chaotic map serves to generate the watermark, and a 2D torus automorphism is subsequently used to scramble the watermark. Therefore, the watermark is scrambled and placed in the reference image. Moreover, the detecting phase involves the host image, where the reference image is extracted from both the host and the image with a watermark, and the correlation is subsequently used to assess the similarity between the retrieved and the introduced watermark. The proposed watermarking scheme can retain the watermarked image's perceptibility justified by the PSNR. In addition, it achieves high robustness to withstand a wide array of attacks.

Corresponding Author:

BELKACEM Samia
Faculty of Technology, Department of Electrical Systems Engineering, LIMOSE Laboratory
M'hamed BOUGARA University
3500 Boumerdes, Algéria.
Email: Email: s.belkacem@univ-boumerdes.dz

1. INTRODUCTION

Digital watermarking, also known as watermarking, is a developed approach in the realm of information security technology; it is mostly utilized on open networks for copyright protection, content authentication, and integrity attestation [1]. Among recognized platforms such as LinkedIn and Facebook, digital images are the most popular data-sharing media [2], where image watermarking serves as a solution to prevent unauthorized use of the intellectual property of unlawful end users.

There are three types of watermarking techniques: The first kind of watermarking is called robust, the second kind is semi-fragile, and the final kind is called fragile. Watermarking methods that are semi-fragile or fragile may both be completely changed or altered. Moreover, robust watermarking methods must be resistant to common attacks [3].

Depending on the processing domain, there are two groups of image watermarking approaches. The watermark is consequently inserted by changing the elements of the original signal or image in the spatial domain [4]. However, employing any of the recognized transformation approaches in the transform domain field, including Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DCT), or radon transform, either the watermark or the owner's image, or both, are transformed [5]. The DWT-based watermarking approach is commonly employed due to its effectiveness when compared to other transformations, as this approach has several advantages [6]. Copyright is embedded in the frequency domain since it is more resistant to common attacks. However, the spatial domain is adopted in the watermarking process because it has the greatest payload capacity [7]. However, their combination has been widely discussed recently.

In addition, it has several characteristics, such as invisibility, robustness and recoverability [8]. These requirements involve a three-dimensional trade-off relationship. A trade-off occurs between the other two dimensions if one dimension is fixed [9].

Instead of adopting random insertion locations, the watermark could be inserted in those regions of an image that are the most perceptually meaningful based on human visual characteristics [10]. In light of this ideas, using perceptual masks that take the HVS's properties into consideration seems to be a successful method for enhancing a watermark's robustness without compromising image quality. While the embedded watermark is practically undetectable by the human eye, and the conventional image processing technologies must not be able to remove the incorporated watermark [11].

Most watermarking approaches in the literature are based on pseudorandom sequences. However, an effective substitute for pseudorandom watermarking sequences for watermarking and encryption procedures is sequences provided by iterations of chaotic maps. Additionally, it represents a very susceptible system to its initial state and seed, where even minor changes can cause significant changes in chaos after a number of repetitions [12], and the system will run in different orbits, which are difficult to analyze and calculate [13].

Color images offer a greater capacity for embedding compared to grayscale photos due to their higher number of channels [14]. RGB color images consist of three color channels, each of which is an eight-bit grayscale image [7]. Nevertheless, the RGB color space is suitable for image display but is not an optimal solution for computer image analysis [15]. The major issue of the RGB color spaces is its strong correlation between each of its components [16]. To overcome this problem, color space selection is a critical stage in watermarking-based applications.

The proposed solution for RGB image watermarking involves separating intensity components from color components by using the National Television Systems Committee (NTSC) space. Three elements make up the image data in the NTSC format: brightness (Y), hue (I), and saturation (Q) (color information) [17]. Grayscale information is represented by the luminance component, while chromatic properties are represented by the I and Q components together [18].

As mentioned earlier, Luminance is more sensitive to the human eye than chrominance [19]. It has become important to exploit the characteristics of the HVS to more effectively hide a robust watermark [10].

Liu et al. [20] developed an image-based self-reference to design a watermarking scheme when the higher-frequency DWT band is zeroed during the watermark embedding steps. In addition, study on the human visual system (HVS) reveals that most of the energy for an image is focused at low frequencies as well as the human eye is sensitive to adjustments at this frequencies [19]. With respect to human eye properties, a reverse self-reference image is conceived for watermark embedding by eliminating the low-frequency DWT band.

This work uses a perceptual model-based robust watermarking color image approach in the DWT domain obtained from reverse self-reference images and a permuted chaotic watermark.

In the following section of this paper. Section 2 reviews related works on color image watermarking approaches. In Section 3, we quickly explore the approaches employed, namely, the RGB and YIQ color spaces, watermark generation, wavelet decomposition, and reverse reference image extraction. We address the proposed watermarking strategies in Section 4. Section 5 outlines the discussion of the achieved findings, and Section 6 draws conclusions.

2. PREVIOUS WORK

There are numerous color spaces, and the selection of an appropriate space for image watermarking should be determined by several critical issues depending on the needs of the intended application. Previous related studies have offered a variety of strategies for embedding watermarks in color spaces.

Employing the RGB color space to include the watermark in the image, as in the work of Visanavi et al., singular value decomposition (SVD) is applied to the blue channel of the host image, and the watermark is embedded in this latter [21]. Mohamed et al. exploited the RGB color space to create a blind watermarking technique based on the integration of a watermark utilizing both the discrete wavelet transform (DWT) and the discrete cosine transform (DCT). A self-adaptive color selection method is employed to choose between the blue and the green channels of the image that can function as the host for the embedding process [22].

Nevertheless, Sun et al. carried out studies on YIQ color space watermarking for colored images, employing a discrete wavelet transform to embed the watermark in both the Y and Q components [23]. In the work of Su et al., the encoded watermark was adaptively injected into the luminance channel related to the YIQ color space using the integer wavelet transform (IWT) domain. The proposed method makes it possible to extract a watermark without using the host image or original watermark [24]. In the work of Gunjal et al., the watermark was inserted in the YIQ space using the I component in the two domains DCT/DWT, and they concluded that the Q channel's PSNR (peak signal-to-noise ratio) and normalized correlation (NC) values are superior to those for the Y and I channels in terms of the PSNR and NC, respectively [25]. A study conducted by Liu et al. suggested a unique blind color watermarking technique based on the integer discrete wavelet transform (IDWT), in which the color host image is converted into the YIQ color space. After that, the secured watermark was simply added to the Y luminance channel of the colored image [26]. In the work of Dey et al., the watermark hiding process is performed on the retrieved Q component of the YIQ space, where the two-level DWT is applied, and the watermark should be present at the stage of detection. The host and the watermarked image's imperceptibility is gauged using the peack signal to noise ratio(PSNR) metric. Moreover, the normalized correlation (NC) serves the purpose to measure how much the produced watermarks reflect the initial inserted watermark [27].

3. METHODS

In this section, we will outline the various tools required to implement our own color image watermarking concept. We first define several concepts.

3.1. RGB and YIQ color spaces

We first define some concepts related to the YIQ color space.

The RGB color space is the most popular color system in digital data processing field., but it presents very high correlations between pixel values, which is not suggested for image watermarking. Although the RGB color space can be transcribed to the YIQ color system, where the Y component represents intensity, while the I and Q components provide color information [24].

The following equations are used to convey the RGB color system into the YIQ color space:

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.29900 & 0.587000 & 0.11400 \\ 0.595716 & -0.274453 & -0.321263 \\ 0.2110 & -0.522591 & 0.311135 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{1}$$

To determine the RGB values associated with YIQ, the inverse matrix method is used according to the equation below:

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 & 0.9563 & 0.6210 \\ 1 & -0.2721 & -0.6474 \\ 1 & -1.1070 & 1.7046 \end{bmatrix} \begin{bmatrix} Y \\ I \\ Q \end{bmatrix} \tag{2}$$

3.2. Watermark generation

The creation of the watermark signal involves a process that comprises three distinct stages. Initially, a one-dimensional chaotic signal is created. The 2-D base watermark is then produced by warping the 1-D signal. Finally, the permutation of the watermark 2-D is performed. More information on the watermark generation process is provided in the subsections that follow.

3.2.1. 1-D chaotic signal generation

A logistic map is a primary instances of a map that is chaotic and has been described by [28]:

$$X_{n+1} = \lambda \cdot X_n \cdot (1 - X_n) \tag{3}$$

$0 \leq X_n \leq 1$, and$0 \leq \lambda \leq 4$, where λ represents the bifurcation parameter. Based on its value, the system's behavior might change greatly. When $3.57 \leq \lambda \leq 4$, the obtained sequence is nonconvergent, nonperiodic, and extremely sensitive to the starting value [29].

3.2.2. Two dimentionnal watermark construction

A two-dimensional (2D) watermark w of size m×n is formed by considering a sequence X_n of size m×n, and we establish a threshold T_w; if a sequence element is larger than the threshold, it is replaced with 1; otherwise, it is replaced with 0 according to the formula below:

$$w(i,j) = \begin{cases} 1 & if \quad w(i,j) \geq T_w \\ 0 & if \quad w(i,j) < T_w \end{cases} \tag{4}$$

As a result, we obtain the expected mark.

3.2.3. Scrambling of the watermark

Processing security is improved by scrambling or encrypting data before embedding watermarking. To increase security and robustness, before the embedding stage, the watermark image must be shuffled or encrypted [16]. Image scrambling can be performed with any reversible mapping. The image is scrambled in this article using the two-dimensional automorphism transformation, which is defined as [30]:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k' & k'+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \operatorname{mod} N \tag{5}$$

To demonstrate the effect of the scrambling method by using two-dimensional automorphism transformation, we use the image called the watch as an example, as shown in Fig. 1; however, the aim of scrambling in this work is to scramble the reconstructed 2D watermark. This means that all of the pixels at the watermark image coordinates are altered when equation (5) is applied.

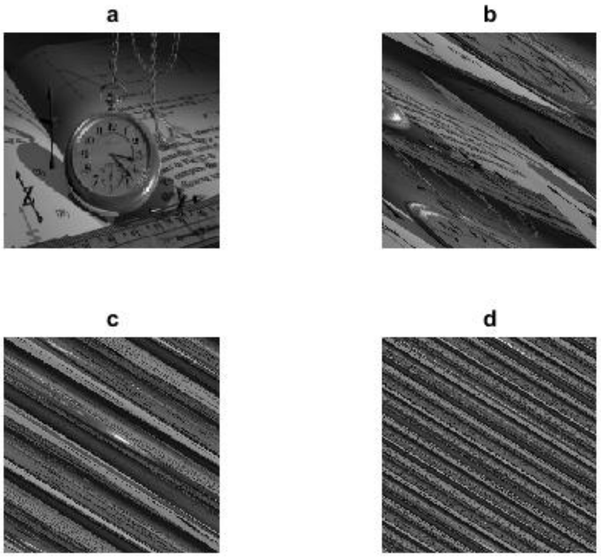

Figure 1. Example of a permuted image: (a) Watermark image; (b), (c), and (d) Permutation of the image; (a) After one, two, and three iterations, respectively

It is evident from Fig.1 that the coordinates of all the pixels in the watermark image undergo a change. The total number of alterations performed to the watermark image is retained as a secret element of information.

3.3. Wavelet transform

The DWT separates an image or signal throughout subbands according to the levels of the filter bank. The decomposition of images/signals produces a collection of wavelet-based basis functions. [31]. It can jointly offer time and frequency information [32]. The process of decomposition via the wavelet transform is depicted in Fig. 2.

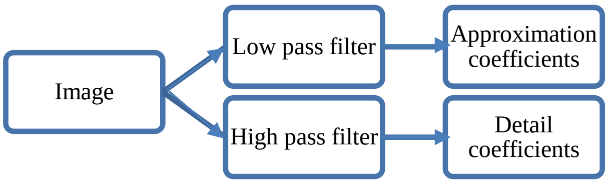

Figure 2. Image decomposition process in the wavelet transform

In order to obtain low-frequency (approximate coefficients) and high-frequency (detail coefficients) data, low-pass (LP) and high-pass (HP) filters, respectively, were used. Therefore, the approximation coefficients are further divided into a second-level approximation and detail coefficients. The same approach is thereafter followed for n-level decomposition, and so forth [33].

Fig. 3 shows an illustration of wavelet decomposition of an image on AC (approximate coefficients) and DC (detail coefficients) to single-level decomposition into four subbands named LL, HL, LH and HH, where LL provides the approximation coefficients, yet HL, LH, and HH design the detail coefficients.

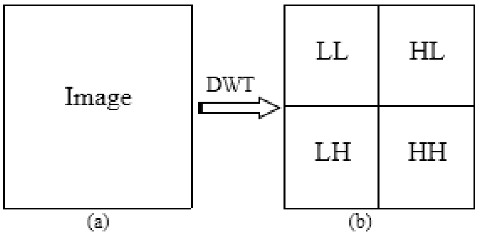

Figure 3. Image decomposition (a): Image, (b): LL, LH, HL, and HH sub-bands

3.4. How can reverse self-reference images be obtained?

A reverse self-reference image is obtained by removing the low-frequency DWT band, considering the characteristics of the human visual system.

The procedure for building the reverse self-reference image includes the following steps, as depicted in Fig. 4.

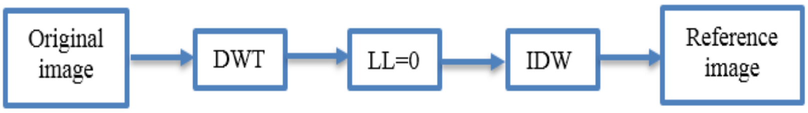

Figure 4. Framework of reverse reference image extraction

The initial step of the method involves decomposing the host image into a single level using a suitable wavelet mother. In the second stage, the low-frequency components are zeroed (LL=0). In the second stage, the low-frequency components are zeroed (LL=0). Ultimately, the reverse reference image is generated by applying a single level of the IDWT's reverse.

4. Proposed Watermarking Technique

Robust color image watermarking in the YIQ space-based watermark generated by a chaotic map is presented in this section. We will adress the embedding process in the color image and the detection process of the watermark.

The following list contains the abbreviations that are used in our watermarking scheme:

1) Im indicates a collection of digital images in grayscale that should be preserved to the size M×N, Im={ 〖Im〗 _ij∈[0,1,…,2^(L-1)]}, where L represents the binary bits of an image pixel with a gray level.
2) w is the watermark's element.
3) Iw represents the watermarked image.
4) Ref is the reference image.
5) Ref_w is the watermarked reverse self-reference image.
6) α is the scaling factor.
7) Y is the luminance component.
8) Yw is the watermarked luminance component.

4.1. Watermark embedding

The proposed watermark embedding approach is presented in Fig. 5 and can be summarized as follows:

Initially, the RGB color image was subjected to three color separations utilizing the NTSC format into YIQ space. Then, the luminance component Y is selected to extract the reverse self-reference image.

An identical-sized watermark to the Y channel is produced using the logistic map. Here, the watermark is first scrambled using permutation equation (5). The watermark is introduced into the reference image in the spatial domain in the additive way as follows:

$$Ref\_w=Ref+\alpha.w \qquad (6)$$

where α adjusts the watermark's insertion strength to achieve equilibrium between invisibility and resistance to attacks.

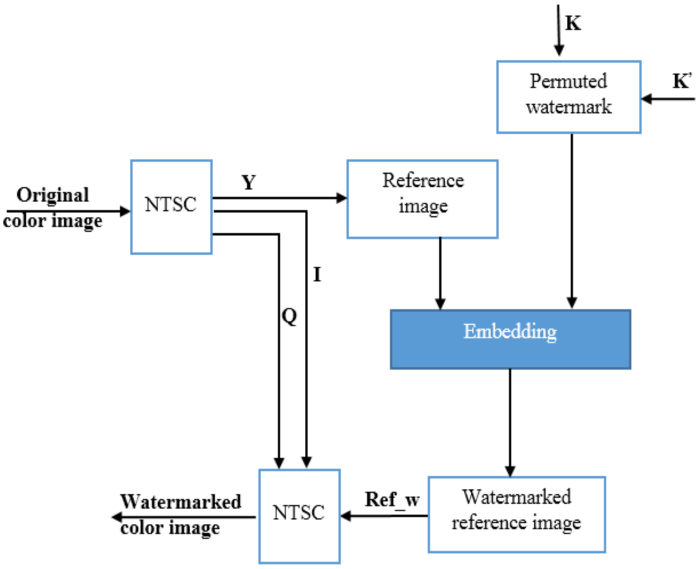

Figure 5. Framework of proposed watermark embedding

The watermarked reference image is decomposed into a 1-level DWT, and its low coefficients are subsequently replaced with the original AC obtained from the Y channel. Then, the inverse DWT is used to obtain the marked reference image. After watermarking the luminance image, we rebuild the color watermarked image (Iw), which is described by the triplet: the watermarked luminance Yw and the two original components Q and I.

4.2. Watermark detection

Watermark detection acts as a reversal technique of the embedding technique stated previously. In the process of detection, one needs to know the inserted mark and the host image, and the spatial domain is used to carry out the detection. Figure 6 in this work illustrates the detection method.

However, the original image and the watermarked image undergo changes into NTSCs, after which the luminance component is extracted. Therefore, we compute the correlation value between the embedded watermark generated by the secret keys (k & k') and then calculate the difference between the two reference images ($d = Yw - Y$) for getting the retrieved watermark.

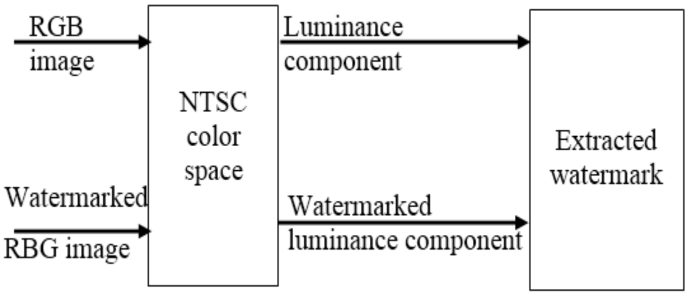

Figure 6. Framework of proposed watermark detection

The detector stage calculates the correlation between the retrieved watermark and the initially incorporated watermark, it helps in determining if the watermark is present in the image under consideration. An image is watermarked if the result is higher than the predetermined threshold value (th); if not, it is not watermarked.

For an effective watermarking scheme, establishing an appropriate threshold to reduce the number of false negatives and false positive alarms is crucial. However, the fixed threshold should be higher than the correlation value between the retrieved watermark and the watermarks produced randomly. In addition, the correlation must be much smaller than the correlation between the retrieved watermark and the watermark that was truly inserted [34].

4.3. Evaluation metrics

There are numerous metrics for evaluating watermark methods. To quantify the effectiveness of the detection performance in term of correlation metric, we use the following equation [35]:

$$\rho = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(w_{ij} - \overline{w}).(d_{ij} - \overline{d})}{(\sum_{i=1}^{M}\sum_{J=1}^{N}(w_{ij} - \overline{w})^{2}).(\sum_{i=1}^{M}\sum_{j=1}^{N}(d_{ij} - \overline{d})^{2})} \tag{7}$$

where d and w indicate the extracted and original watermarks, respectively, corresponding to $\overline{w}$ and $\bar{d}$, respectively, of their mean values.

Correlation value of 1 is required for perfect algorithms, and a good watermarking scheme should provide a ρvalue close to 0.7 [36].

The second criterion that we employ is the PSNR (Peack Signal to Noise Ratio) metric is applied to estimate the degradation of the watermarked image in contrast to the host image by measuring the distortion carried out by the insertion strategy.

The mean squared error (MSE) between the watermarked and original images is given by [36]:

$$MSE = \frac{1}{M \times N}\sum_{M}\sum_{N}(Y_{ij} - Yw_{ij})^{2} \tag{8}$$

This metric shows how much damage was caused to the watermarked images, where values close to 0 indicate less degradation;

$$PSNR = 10\,Log_{10}\frac{255^{2}}{MSE} \tag{9}$$

A low PSNR indicates high distortion. A human cannot detect any distortion when grayscale images are above 36 dB [37].

5. EXPERIMENTAL RESULTS

In the experiments, Daubechies (DB4) wavelet mother is used, a threshold value is fixed to 0.01, and a watermark strength of 0.5 is applied with iteration 3.

The commonly employed images Baboon, Watch pappers and f16 in RGB mode were 256×256 in size, are shown in Fig. 7 together with the logo watermark.

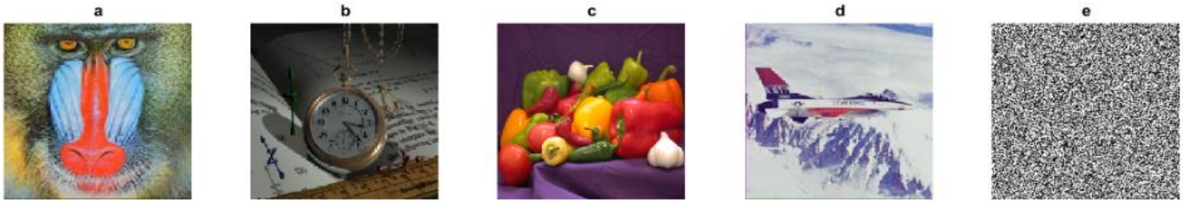

Figure 7: Image tests a): Baboon image, b) Watch image,c) Peppers iamge, d) f16 image, and e) Watermark

Imperceptibility and robustness are important aspects to take into consideration when assessing an image watermarking approach.

5.1. Perceptual evaluation

We first assessed the perceptual quality of the watermarked images by considering the reference image. For this purpose, we attempted displaying the same image twice: once utilizing the suggested technique named Method 1 and once without using the reference image designed by Method 2.

5.1.1. Visual quality

The watermarked images obtained with Method 1 and Method 2 are depicted in Fig. 8. We can certify that there is no obvious distinction between the original images and the watermarked images generated using the reference image. As a consequence, it is confirmed that the invisibility issue has been verified.

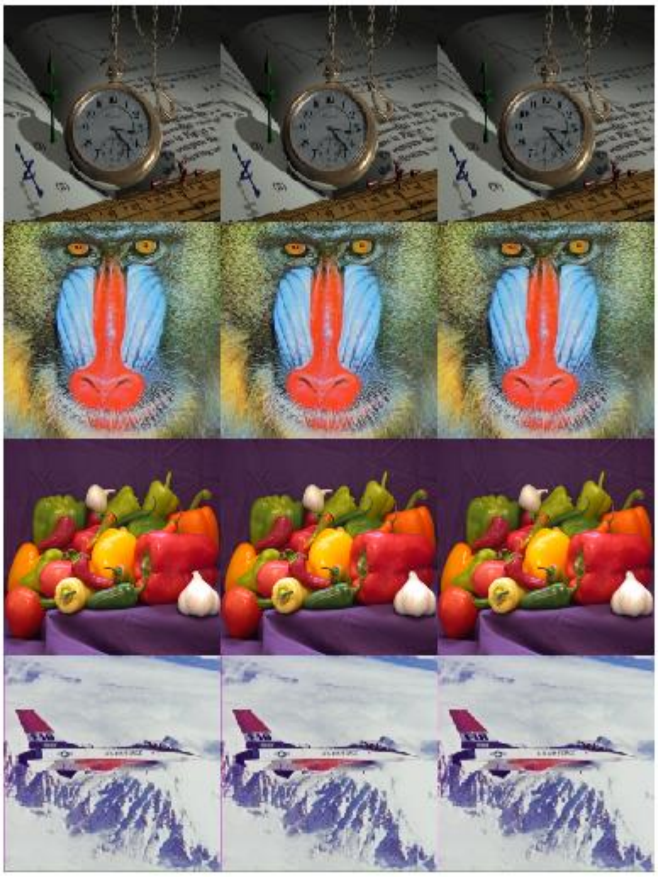

Figure 8. Invisibility comparison;from high to low : Watch, Baboon, Peppers and F16 images; from left to right:original images; watermarked image using reference image, watermarked image without reference image

5.1.2. Quantitative evaluation

The next phase entails evaluating the effectiveness of the suggested strategy. The variations in PSNR values for both approaches with changing scaling factor α for image F16 can be seen in Fig. 9 when α increases from 0.01 to 1.

According to Fig. 9, the invisibility decreases in terms of the PSNR as the embedding factor α increases. A comparison of the watermarked image's PSNR to that of the other watermarking approach (Method 1) showed that the proposed approach is superior. The difference in the values shows that our new algorithm performs better than before. The proposed solutions enable the use of a greater value of α without degrading the image quality. Therefore, we choose α =0.5, resulting in a PSNR=654.99dB for the watch watermarked image, to carry out our testing.

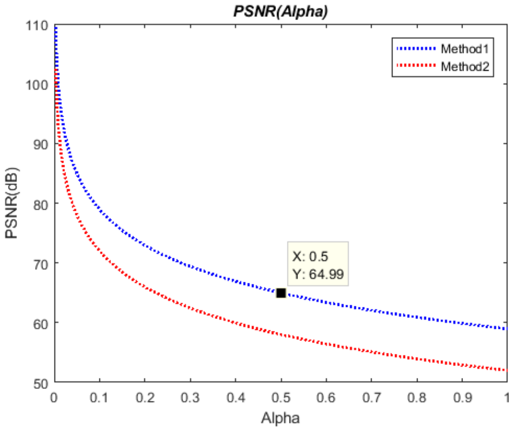

Figure 9. PSNR variation in the watermarked image f16

5.2. Robustness test

Several attacks were carried out after achieving the required fidelity to check the robustness of the suggested approach. In order to investigate the resistance of the suggested approach to attacks, including the common attacks such as compression attack, geometric attacks, filtering attack and noise attack.

Experiment 1: Uniqueness of the watermark

To evaluate the watermark's uniqueness, the image must be unaffected by any attack. Therefore, the response of the detector to the fixed watermark is much greater than that to the other watermarks and close to the value of one. The watermark detectors for 200 randomly generated watermarks are shown in Fig. 10. It is obvious that only one watermark matches the correct inserted watermark.

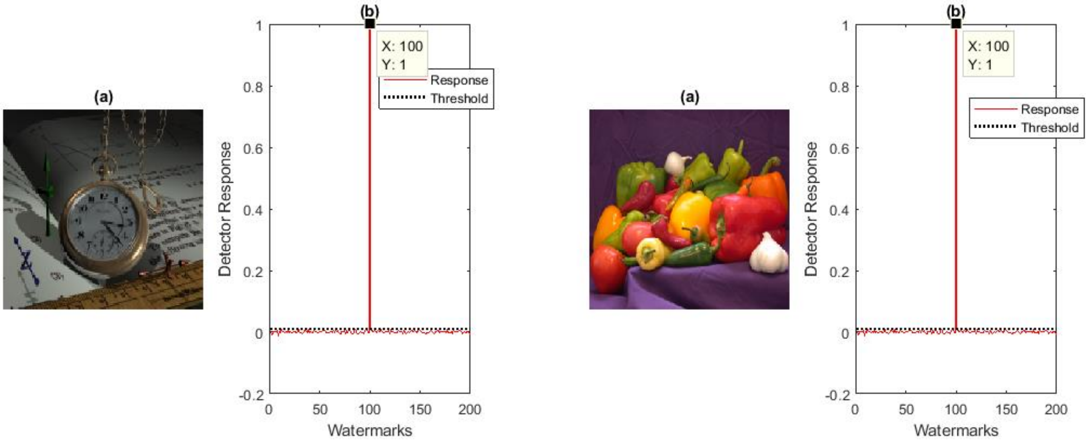

Figure 10. The watermarked image's detector response to 200 random watermarks

As can be seen in Fig. 10, the watermark number 100 resembles that introduced in the host images both for watch and peppers images. The correct embedded watermark produced a much greater response than the others, and the watermarking algorithm successfully managed to identify it from among 200 other watermarks.

Experiment 2: JPEG compression attack

The widely used threat is JPEG compression, to which the watermarked image should be resistant. The outcome of JPEG compression was evaluated at a compression quality of 50. The compressed image and the detector response are given in Fig. 11.

It is obvious that the quality of a watermarking image decreases when the quality factor decreases. From Fig. 11(b), we can see that the detector value at the inserted watermark (100) is above the threshold. After a JPEG attack, the suggested watermarking method was still able to identify the proper embedded watermark among 200 distinct watermarks.

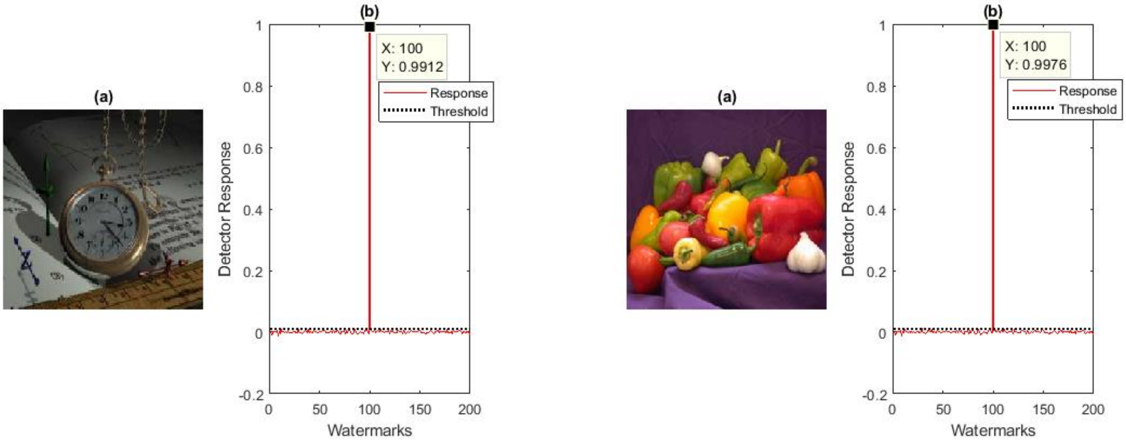

Figure 11. Attacked watermarked images and their responses to the detector of the watermarked image Watch for QF=50

Experiment 3: Rotation attack

This type of attack makes the watermark undetectable while maintaining it within the image. Fig. 12 shows the rotated image with a 60° angle and the detector response results.

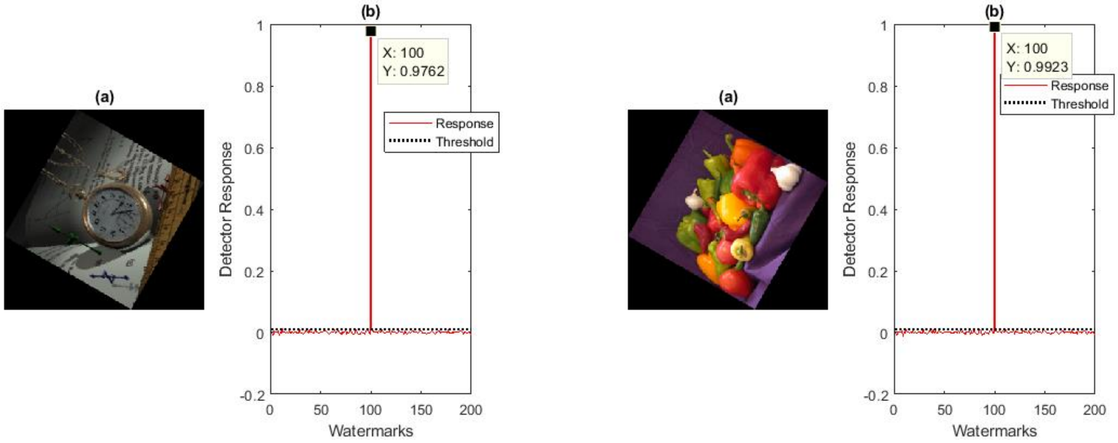

Figure 12. Rotation attack; a) Rotated images; b) Detector response

The correlation value with the truly inserted watermark (number 100) is above 0.7 for the rotated image with 60°.

Experiment 4: Cropping attack

When some parts are cropped from an image, the watermark may also be lost. Fig. 13 shows the rotated image and the corresponding detector response results for diagonal cropping.

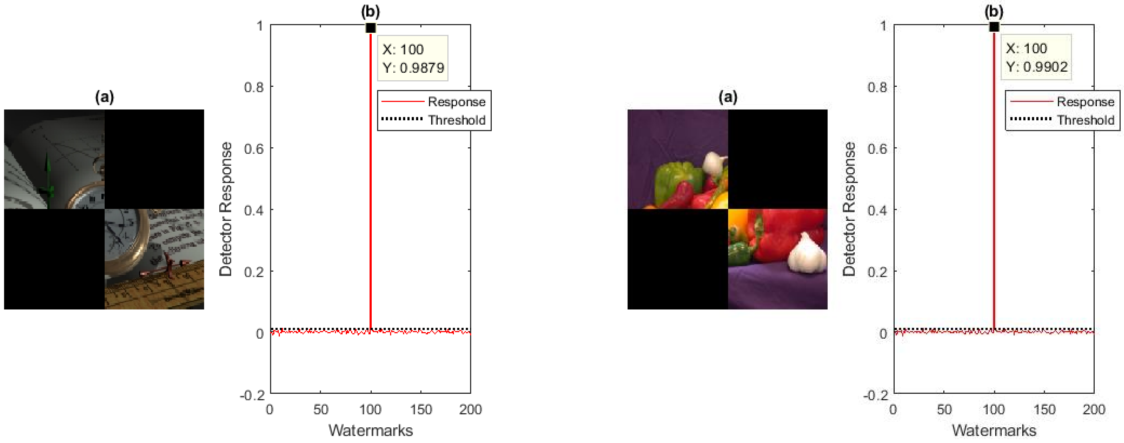

Figure 13. Cropping attack; a) Cropped images; b) Detector response

Fig. 13 shows that the detector value at the inserted watermark (100) is above the threshold. That is, the suggested watermarking algorithm continues to discover the proper embedded watermark among the 200 distinct watermarks.

Experiment 5: Median filter attack

Median filters, as their name implies, replace the center value pixel with the median value of the adjacent intensity values. This is done by ranking or sorting the pixels present in the image area covered by the filter. In light of this, a median filter is expected to affect or remove any watermark signals present in the image since watermark signals can be thought of as tiny changing signals inside their hosts [38]. The filtered watermarked image with a window size of 7×7×7 is shown in Fig. 14.

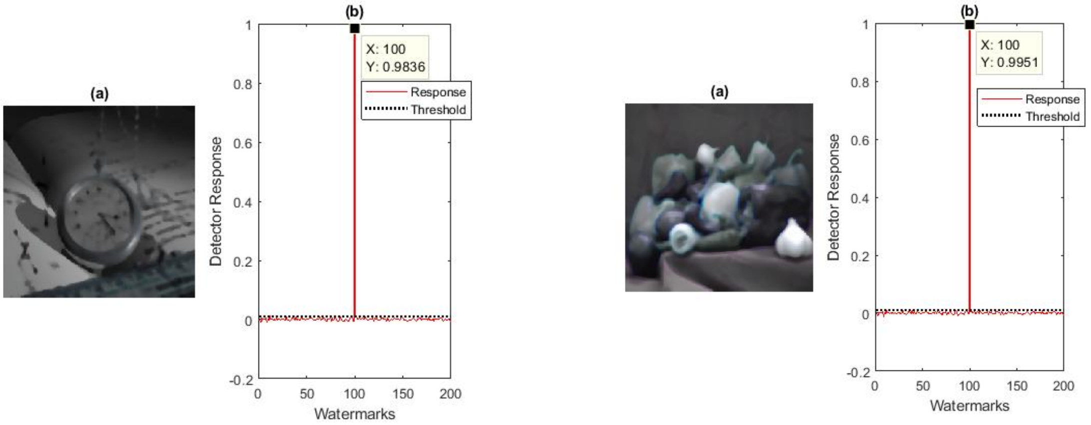

Figure 14. Median filter attack; a) Filtred images; b) Detector response

Fig. 14 shows that the detector value at the inserted watermark (100) is above the threshold. That is, after a median filter, the suggested watermarking method still managed to identify the proper embedded watermark among 200 distinct watermarks.

Experiment 6: Noise attacks

Salt and pepper noise are added to the watermarked image at density of 0.5, as shown in Fig15(a).

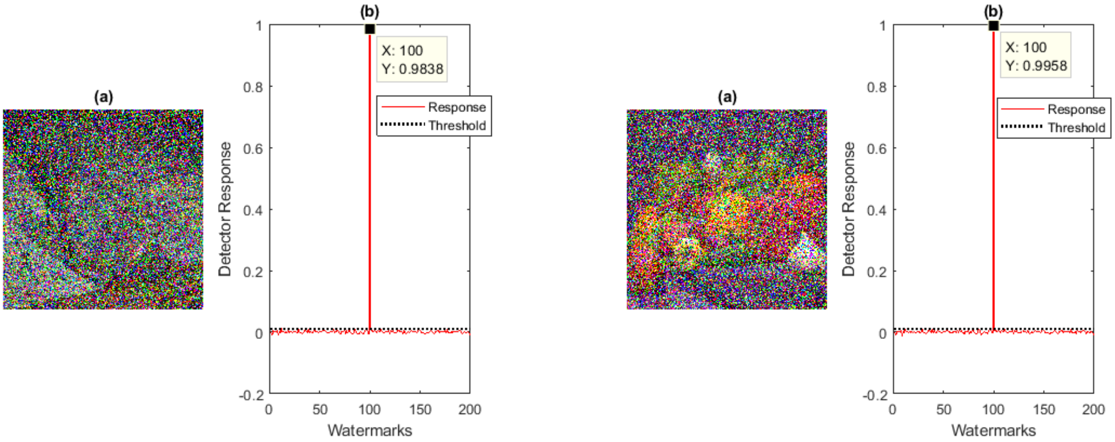

Figure 15. Salt and pepper noise attack; a) Noised images; b) Detector response

It is evident from Fig. 15(b) that the image quality is lost, yet the mark may still be detectable among 200 various watermarks. We can infer that the suggested scheme is highly effective at guaranteeing resilience against salt and pepper noises threats.

Experiment 7: Histogram Equalization

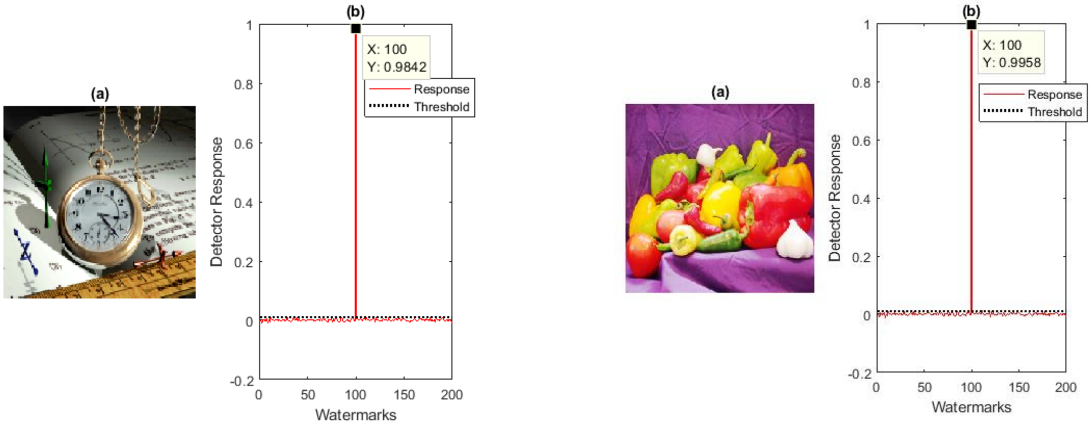

Figure 16. Histogram equalization attack; a) Attacked images; b) Detector responses

Histogram equalization is a technique for images processing that changes the histogram's intensity distribution to modify an image's contrast, as shown in Fig16(a). Although the image quality is lost in Fig. 16(b), the mark still be detected among the 200 watermarks. The recommended strategy is highly effective at assuring resilience against histogram equalization attack.

5.3. Discussion

Our experimental results, expressed by means of the peak signal-to-noise ratio (PSNR) and correlation coefficient, demonstrate that the embedded watermark seems practically invisible to the human eye, which satisfies the imperceptibility property regardless of the image nature. Before launching attacks, it can be noticed that the watermark was extracted perfectly with a correlation $\rho = 1$. Even though the correlation coefficient of the proposed method for a watermark number 100 is higher than the threshold and close to the value of one for all applied attacks, we can infer that the watermarked image is not impaired. Furthermore, our proposed scheme offers a great degree of robustness to withstand jpeg, rotation, cropping, median filtering, noise attacks, and histogram equalization. In overall, a superior outcome between invisibility and robustness is achieved through the use of a reverse self-reference image of the luminance component in the YIQ space.

6. CONCLUSION

In this research article, a DWT-based watermarking algorithm for color digital images according to HVS is highlighted. In the spatial domain, the watermark is applied, and the reverse self-reference image is extracted from the luminance component to make the watermark transparent without decreasing its vulnerability against multiple attacks. A comparison of watermarked images obtained with and without reference images in the spatial domain reveals the enhanced effectiveness of our current approach. produces excellent results in terms of the detector responses. Moreover, the suggested approach exhibits strong resilience versus various forms of attacks. Our proposed method provides an effective way to achieve efficient color image watermarking with a high degree of robustness. In this paper, the detection process of the inserted watermark is performed in a non-blind manner. Future work can explore a blind watermarking strategy to further improve the performance of our developed system.

REFERENCES

[1] S. Boujerfaoui, R. Riad, H. Douzi, F. Ros, and R. Harba, ‘Image Watermarking between Conventional and Learning-Based Techniques: A Literature Review’, *Electronics*, vol. 12, no. 1, p. 74, Dec. 2022, doi: 10.3390/electronics12010074.

[2] S.-J. Wöhnert, K. H. Wöhnert, E. Almamedov, C. Frank, and V. Skwarek, ‘A study on the use of perceptual hashing to detect manipulation of embedded messages in images’, Feb. 28, 2023, *arXiv*: arXiv:2303.00092. Accessed: Jul. 29, 2023. [Online]. Available: http://arxiv.org/abs/2303.00092

[1] S. Tyagi, H. V. Singh, R. Agarwal, and S. K. Gangwar, ‘Digital watermarking techniques for security applications’, in 2016 International Conference on Emerging Trends in Electrical Electronics & Sustainable Energy Systems (ICETEESES), Sultanpur, India: IEEE, Mar. 2016, pp. 379–382. doi: 10.1109/ICETEESES.2016.7581413.

[2] M. A. Jabaar and S. N. Alsaad, ‘Detection of Spliced Images in Social Media Application’, in 2021 7th International Conference on Contemporary Information Technology and Mathematics (ICCITM), Mosul, Iraq: IEEE, Aug. 2021, pp. 63–69. doi: 10.1109/ICCITM53167.2021.9677737.

[3] H. Khalid, D. Mohamed, and F. Mostapha, ‘Robust Color Images Watermarking Using New Fractional-Order Exponent Moments’, IEEE Access, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9383223

[4] F. Ernawan, D. Ariatmanto, and A. Firdaus, ‘An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients’, IEEE Access, vol. 9, pp. 45474–45485, 2021, doi: 10.1109/ACCESS.2021.3067245.

[5] 5. L. Verma and S. Pratap Singh Chauhan, ‘A Review on Digital Image Watermarking Using Transformation and Optimization Techniques’, in 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India: IEEE, Dec. 2020, pp. 1008–1012. doi: 10.1109/ICACCCN51052.2020.9362885.

[6] R. Safabakhsh, S. Zaboli, and A. Tabibiazar, ‘Digital watermarking on still images using wavelet transform’, in International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004., Las Vegas, NV, USA: IEEE, 2004, pp. 671-675 Vol.1. doi: 10.1109/ITCC.2004.1286543.

[7] D. R. I. M. Setiadi, ‘Improved payload capacity in LSB image steganography uses dilated hybrid edge detection’, J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 2, pp. 104–114, 2022, doi: https://doi.org/10.1016/j.jksuci.2019.12.007.

[8] Y. Zhaoning, L. Yan, and G. Tiegang, ‘A lossless self-recovery watermarking scheme with JPEG-LS compression’, J. Inf. Secur. Appl., vol. 58, p. 102733, May 2021, doi: 10.1016/j.jisa.2020.102733.

[9] V. M. Potdar, S. Han, and E. Chang, ‘A survey of digital image watermarking techniques’, in INDIN ’05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005., Aug. 2005, pp. 709–716. doi: 10.1109/INDIN.2005.1560462.

[10] S. Bagheri Baba Ahmadi, G. Zhang, S. Wei, and L. Boukela, ‘An intelligent and blind image watermarking scheme based on hybrid SVD transforms using human visual system characteristics’, Vis. Comput., vol. 37, no. 2, pp. 385–409, Feb. 2021, doi: 10.1007/s00371-020-01808-6.

[11] D. Jabeen, S. M. G. Monir, S. Noor, M. Rafiullah, and M. A. Jatoi, ‘Color image watermarking using spatio-chromatic complex Hadamard transform in sequency domain’, World J. Eng., vol. 19, no. 5, pp. 658–666, Aug. 2022, doi: 10.1108/WJE-03-2021-0176.

[12] S. Belkacem, Z. Dibi, A. Bouridane, and M. Laadjel, ‘Color Image Watermarking based on Chaotic Map’, in 2007 14th IEEE International Conference on Electronics, Circuits and Systems, Marrakech: IEEE, Dec. 2007, pp. 343–346. doi: 10.1109/ICECS.2007.4511000.

[13] D. Algarni, N. F. Soliman, H. A. Abdallah, and F. E. Abd El-Samie, ‘Encryption of ECG signals for telemedicine applications’, Multimed. Tools Appl., vol. 80, no. 7, pp. 10679–10703, Mar. 2021, doi: 10.1007/s11042-020-09369-5.

[14] M. Jamali, M. Bagheri, N. Karimi, and S. Samavi, ‘Robustness and Imperceptibility Enhancement in Watermarked Images by Color Transformation’. arXiv, Nov. 02, 2019. doi: 10.48550/arXiv.1911.00772.

[15] M. Kutter, F. D. Jordan, and F. Bossen, ‘Digital signature of color images using amplitude modulation’, presented at the Electronic Imaging ’97, I. K. Sethi and R. C. Jain, Eds., San Jose, CA, Jan. 1997, pp. 518–526. doi: 10.1117/12.263442.

[16] N. Ahmidi and R. Safabakhsh, ‘A novel DCT-based approach for secure color image watermarking’, in International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004., Las Vegas, NV, USA: IEEE, 2004, pp. 709-713 Vol.2. doi: 10.1109/ITCC.2004.1286738.

[17] 17. T. Singh, R. Lal Dua, S. Agrawal, and A. Acharya, ‘Detection of Defects in Glass Sheet using C. S. C based Segmentation Method’, Int. J. Comput. Appl., vol. 68, no. 14, pp. 29–32, Apr. 2013, doi: 10.5120/11650-7152.

[18] M. Khalili and D. Asatryan, ‘Color spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map’, IET Signal Process., vol. 7, no. 3, pp. 177–187, 2013, doi: 10.1049/iet-spr.2012.0380.

[19] M. N. Maatouk and N. E. B. Amara, ‘Adaptive Watermarking Algorithm of Color Images of Ancient Documents on YIQ-PCA Color Space’, in International Joint Conference, Á. Herrero, B. Baruque, J. Sedano, H. Quintián, and E. Corchado, Eds., in Advances in Intelligent Systems and Computing. Cham: Springer International Publishing, 2015, pp. 75–86. doi: 10.1007/978-3-319-19713-5_7.

[20] J.-L. Liu, D.-C. Lou, M.-C. Chang, and H.-K. Tso, ‘A robust watermarking scheme using self-reference image’, Comput. Stand. Interfaces, vol. 28, no. 3, pp. 356–367, Jan. 2006, doi: 10.1016/j.csi.2005.07.001.

[21] D. Vaishnavi and T. S. Subashini, ‘Robust and Invisible Image Watermarking in RGB Color Space Using SVD’, Procedia Comput. Sci., vol. 46, pp. 1770–1777, Jan. 2015, doi: 10.1016/j.procs.2015.02.130.

[22] Mohammed, ‘A blind and robust color image watermarking scheme based on DCT and DWT domains | SpringerLink’, 2023. https://link.springer.com/article/10.1007/s11042-023-14797-0 (accessed Aug. 11, 2023).

[23] G. Sun and Y. Yu, ‘DWT Based Watermarking Algorithm of Color Images’, in 2007 2nd IEEE Conference on Industrial Electronics and Applications, May 2007, pp. 1823–1826. doi: 10.1109/ICIEA.2007.4318725.

[24] Q. Su, X. Liu, and W. Yang, ‘A watermarking algorithm for color image based on YIQ color space and Integer Wavelet Transform’, in 2009 International Conference on Image Analysis and Signal Processing, Apr. 2009, pp. 70–73. doi: 10.1109/IASP.2009.5054573.

[25] B. L. Gunjal and S. N. Mali, ‘Secured color image watermarking technique in DWT-DCT domain’, Int. J. Comput. Sci. Eng. Inf. Technol. IJCSEIT, vol. 1, no. 3, 2011, [Online]. Available: https://arxiv.org/abs/1109.2325

[26] Q. Liu, ‘An Adaptive Blind Watermarking Algorithm for Color Image’, Indones. J. Electr. Eng. Comput. Sci., vol. 11, no. 1, Art. no. 1, Jan. 2013.

[27] E. Dey, S. Majumder, and A. Neelim Mazumder, ‘A new approach to color image watermarking based on joint DWT-SVD domain in YIQ color space’, in 2017 3rd International Conference on Electrical Information and Communication Technology (EICT), Dec. 2017, pp. 1–6. doi: 10.1109/EICT.2017.8275190.

[28] S. S. Jamal, T. Shah, and I. Hussain, ‘An efficient scheme for digital watermarking using chaotic map’, Nonlinear Dyn., vol. 73, no. 3, pp. 1469–1474, Aug. 2013, doi: 10.1007/s11071-013-0877-9.

[29] Mooney, J. G. Keating, and I. Pitas, ‘A comparative study of chaotic and white noise signals in digital watermarking’, Chaos Solitons Fractals, vol. 35, no. 5, pp. 913–921, Mar. 2008, doi: 10.1016/j.chaos.2006.05.073.

[30] Feng, X. Li, Y. Jie, C. Guo, and H. Fu, ‘A Novel semi fragile Digital Watermarking Scheme for Scrambled Image Authentication and Restoration’, Mob. Netw. Appl., vol. 25, no. 1, pp. 82–94, Feb. 2020, doi: 10.1007/s11036-018-1186-9.

[31] R. R. Nair and T. Singh, ‘Multi-sensor medical image fusion using pyramid-based DWT: a multi-resolution approach’, IET Image Process., vol. 13, no. 9, pp. 1447–1459, Jul. 2019, doi: 10.1049/iet-ipr.2018.6556.

[32] S. Mukhopadhyay, S. Biswas, A. Bardhan Roy, and N. Dey, ‘Wavelet Based QRS Complex Detection of ECG Signal’, arXiv e-prints. Sep. 01, 2012. doi: 10.48550/arXiv.1209.1563.

[33] M. Eshaghi and M. R. K. Mollaei, ‘A new algorithm for voice activity detection based on wavelet packets’, in 2008 Second International Conference on Electrical Engineering, Lahore, Pakistan: IEEE, Mar. 2008, pp. 1–4. doi: 10.1109/ICEE.2008.4553891.

[34] B. Plaaintz, W. S. Stiles, ‘Medical image Watermarking: A Study on Image Degradation’, Proceedings of the Australian Pattern Recognition Society (APRS) Workshop on Digital Image Computing (WDIC), Brisbane Australia, 2005.

[35] L. Sheugh and S. H. Alizadeh, ‘A note on pearson correlation coefficient as a metric of similarity in recommender system’, in 2015 AI & Robotics (IRANOPEN), Qazvin: IEEE, Apr. 2015, pp. 1–6. doi: 10.1109/RIOS.2015.7270736.

[36] S. Boujerfaoui, R. Riad, H. Douzi, F. Ros, and R. Harba, ‘Image Watermarking between Conventional and Learning-Based Techniques: A Literature Review’, Electronics, vol. 12, no. 1, p. 74, Dec. 2022, doi: 10.3390/electronics12010074.

[37] S.-J. Wöhnert, K. H. Wöhnert, E. Almamedov, C. Frank, and V. Skwarek, ‘A study on the use of perceptual hashing to detect manipulation of embedded messages in images’. arXiv, Feb. 28, 2023. Accessed: Jul. 29, 2023. [Online]. Available: http://arxiv.org/abs/2303.00092

[38] Song, C., Sudirman, S., Merabti, M., & Llewellyn-Jones, D. (2010). Analysis of Digital Image Watermark Attacks. 2010 7th IEEE Consumer Communications and Networking Conference, 1–5. https://doi.org/10.1109/CCNC.2010.5421631