A Survey of Digital Image Watermarking Techniques Based on Discrete Cosine Transform

Almula B. Şahin*† and İnan Güler**

* Gazi University, Graduate School of Natural and Applied Sciences, Information Security Engineering Program

** Gazi University, Faculty of Technology, Electrical & Electronics

Corresponding Author: Almula.sahin@gmail.com

Review Paper Received: 05.09.2021 Revised: 25.09.2021 Accepted: 30.09.2021

Abstract - In this study, a literature review is presented to examine the Discrete Cosine Transform (DCT) based digital image watermarking techniques since 2010, apart from the very basic articles. General features of the digital watermarking, frequency domain & spatial domain watermarking techniques, DCT and various watermarking researches with DCT in last decade were stated. The studies were classified according to the application methods of DCT, features of the watermarking technique, watermark extraction method, robustness, and usage area. Results have shown that DCT has increased the robustness of watermarking by performing with a union of several methods from simple to complex. In this case, the main purpose of this study can be considered as making a compilation of DCT techniques and preparing an information note that can be a reference for those working in this field. For the future studies to improve watermarking with DCT, a combination between machine learning and optimization techniques would be preferred.

Keywords - Digital watermarking; Discrete Cosine Transform; Watermark; Frequency Domain; Image Watermarking.

1. Introduction

Today, with the advancing technology, it is getting easier to produce images, audio & video, publish these data and reach the data. Extensive data breach generates unauthorized access and raises problems on the use of data in art, advertising, and even medical fields. To aim of protecting copyright and information, some shielding techniques without any perceptual distortion are applied to digital data [1]. One of such techniques is the watermark dates back to early 1200s. At first, watermark that was targeted to protect the originality of some precious paper, such as money, was a fragile method [2]. Digital watermarking can be applied to all digital data types such as audio, image, and video. The purpose of digital watermarking is to embed special information of the actual digital as watermark into the cover image inconspicuously. The general watermarking algorithm is given in Figure 1.

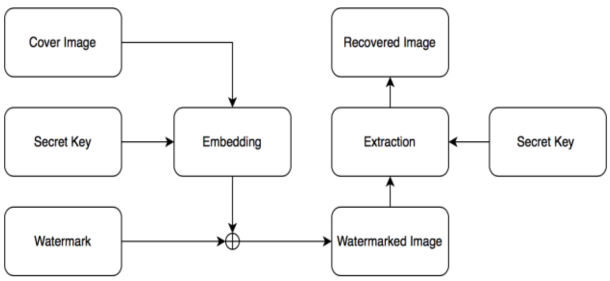

Figure 1: Watermark Algorithm.

Thanks to the technique, proof of ownership, authentication, preventing unauthorized copying and document accuracy can be provided by [3],

[4], [5]. The success and performance of the technique are measured by storage capacity, robustness, and the effect on the cover image. Since the suggested watermarking technique should ensure three objectives of information security: confidentiality, integrity, and availability; frequency domain transformers are more often preferred for images. One of the frequency domain transform techniques is Discrete Cosine Transform (DCT) which enables a watermark to be embedded in a cover image [6], [7]. By combining different methods with DCT more useful techniques are generated. These methods are differentiated according to the type of watermark, robustness, remarkability, the complexity of the method, and the capacity of the process. As a benefit of this variation, DCT will have an improving impact to evaluate image watermarking. For this reason, watermarking based on DCT is a significant method to investigate. In order to understand the main idea behind it, several researches should be examined to arrange an overall aspect. In this study, various image watermarking techniques developed and combined by DCT were examined and analyzed according to their properties.

2. Image Watermarking Techniques

Digital watermarking is a stenography method to embed a watermark that is defined to preserve the originality and integrity of the actual image. Main usage areas of image watermarking are attestation of ownership, copy prevention and control, electronic advertising, forensic issues, media archiving, network broadcasting and digital library [1]. Watermark is the significant component of overall method. For this reason, watermark should be a reversible method. Generally recovering the watermark with a minimum distortion is a goal. To achieve it watermark should be survived after encryption, decryption, geometric manipulation, and compression [8]. On the other hand, according to the aim of methodology watermark can be survived or destroyed. As a result, the method of watermarking is classified as fragile and robust. Fragile watermark that is significantly destroyed after any modification is used in authentication-targeted applications in order to preserve the integrity of the content. It is used to prove deliberate manipulations in the image. Robust watermarking is generally used in copyright applications. In robust watermarking method, it is not possible to change or remove the watermark from the watermarked image without damaging the cover image [9]. By using robust and fragile watermark techniques together integrity and copyright protection can be achieved simultaneously [10].

Apart from that, watermarking application character is also the key feature to classify a proposed method. Application character can be defined as blind, semi-blind and non-blind. Blind watermarking, also known as public watermarking, uses only the secret key to remove the watermark, so it is a compelling method. While semi-blind watermarking is to detect whether the watermark is in the image. It does not require the original image, is frequently used in applications such as copyright control and aims to identify the original recipient of the pirated copy. However, non-blind watermarking, also known as private watermarking, requires the original cover image for watermark extraction in addition to watermarked image [11].

To accomplish these features watermarking method should be utilized. Image watermarking can be applied in both spatial domain and frequency domain. Since forming noticeable changes on the processed image, easy to damage the hided information, low capacity and less robustness, watermark techniques in spatial domain are less preferred methods for visual signals. On the other hand, watermark techniques in frequency domain are strong methods in terms of robustness and imperceptibility [12].

During image watermarking in the spatial domain, the pixels of the image are processed. A pseudo-random number sequence, that is, a noise pattern, is produced and embedded in the pixels of the image. The pattern consists of integers between {-1, 0, 1}. Spatial domain provides fast, easy and effective watermarking as long as no noise is applied, but they are powerless against attacks such as cropping [2]. In particular, these techniques involve challenging problems in terms of visibility, robustness and capacity [13]. The most common spatial domain techniques used in watermarking methods are Least Significant Bit Method, Single Value Decomposition, Patchwork Technique, and Arnold Transform.

Frequency domain ensures robust information hiding methods because they are applied on the coefficients of the cover image [14]. Discrete Wavelet Transform (ADD), Discrete Fourier Transform (AFD) and Discrete Cosine Transform are widely used frequency domain methods for watermarking.

To analyze the suggested method the performance of the watermarking should be evaluated. Performance can be calculated by normalized correlation and PSNR. While the image quality of the extracted watermark is calculated by normalized correlation; the error metric between the original cover image and the watermarked cover image is calculated by PSNR [15]. Normalized correlation (NC) is defined in Eqn (1). $f[i,j]$ original watermark, $f'[i,j]$ watermark after extraction and MxN represent the size of the watermark. With this equation, values between 0-1 are obtained; the closer result is to 1, the higher the similarity.

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(f[i,j] * f'[i,j])}{\sum_{i=1}^{M}\sum_{j=1}^{N}(f'[i,j])^2} \quad (1)$$

For PSNR, MSE must be calculated first. MSE is specified in Eqn (2), where K(n,m) original cover image, D(n,m) watermarked image, and MxN represent the size of the image.

$$MSE = \frac{1}{M * N}\sum_{n=1}^{M}\sum_{m=1}^{N}[D(n,m) - K(n,m)]^2 \quad (2)$$

Using MSE, PSNR value of the system is calculated by Eqn (3). S represents the maximum number of image pixel. The higher PSNR value is better image quality [16].

$$PSNR = 10 * \log_{10}\frac{S^2}{MSE} \quad (3)$$

Since the system can be exposed to some intentional or unintentional actions, proposed watermarking method should be survived under several actions. To analyze its strengthened, robustness should be examined by attacks. These attacks can be segmented into active and passive attacks. Masking attacks, such as cropping, scaling and rotating, targeting the cover image, and robustness attacks, such as filtering, noise, and compression, aiming to damage the watermark can be exampled to active attacks. On the contrary, passive attacks are intentional or unintentional watermark extraction attacks that are not aimed to destroy the cover image or the watermark [17], [18].

3. Discrete Cosine Transform

For frequency based watermarking DCT is frequently used method. In order to understand Discrete Cosine Transform (DCT), first Discrete Fourier Transform (DFT) should be described. DFT is a transformation method that allows generating the coefficients of a non-periodic signal. As a result of DFT, signal becomes both periodic and discrete in the frequency domain [2]. DFT of signal Z with size N is defined in Eqn (4), inverse DFT is defined in Eqn (5):

$$X(k) = \sum_{n=0}^{N-1} x(n)W_N^{nk} \quad (4)$$

$$x(n) = \frac{1}{N}\sum_{n=0}^{N-1} X(k) W_N^{-nk} \quad (5)$$

$W_N = \exp\left(-\frac{j2\pi}{N}\right)$ *and* $j = \sqrt{-1}$ [19].

DCT is similar to DFT. However, although only real values are used in the time domain, DFT separates the signal into real and imaginary parts, so it is necessary to parse again for an operation to be performed in the time domain. On the other hand, by only generating real parts, DCT eliminates additional parsing processes [20]. Thus, DCT reduces the number of operations by more than half of the number of operations implemented in DFT [12]. 2-dimensional DFT with size NxN is stated in Eqn (6), and the inverse DCT is defined in Eqn (7) [12]:

$$F(u,v) = c(u)c(v)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f(i,j)\cos\left[\frac{(2i+1)u\pi}{2N}\right]\cos\left[\frac{(2j+1)u\pi}{2N}\right] \quad (6)$$

$$c(u) = \begin{cases}\sqrt{1/N}, & u = 0\\ \sqrt{2/N}, & u \neq 0\end{cases} \qquad c(v) = \begin{cases}\sqrt{1/N}, & v = 0\\ \sqrt{2/N}, & v \neq 0\end{cases}$$

$$f(i,j) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} c(u)c(v)F(u,v)\cos\left[\frac{(2i+1)u\pi}{2N}\right]\cos\left[\frac{(2j+1)u\pi}{2N}\right] \quad (7)$$

To illustrate DCT, if 8x8 array is considered, low frequencies are collected in the upper left area, and high frequencies are collected in the lower right area. Figure 2 illustrates 8x8 DCT output according the stated manner. While low frequency is the region carrying the high energy of the image; high frequency is carrying the low energy of the image, which can often be ignored [21]. As a result of the modifications made to the low frequency domain, serious visual differences are observed in the cover image [22]. Therefore, high frequency coefficients are vulnerable to various attacks [23].

4. Watermark Methods Based on Discrete Cosine Transform

In the literature, numerous studies have been carried out for image watermarking based on DCT. The majority of these studies are combined with various methods to enhance robustness, security and imperceptibility.

Spatial domain transforms, such as Single Value Decomposition (SVD) and Arnold Transform, can be combined frequency domain transforms, to develop watermarking methods that are low in complexity but high in robustness and imperceptibility.

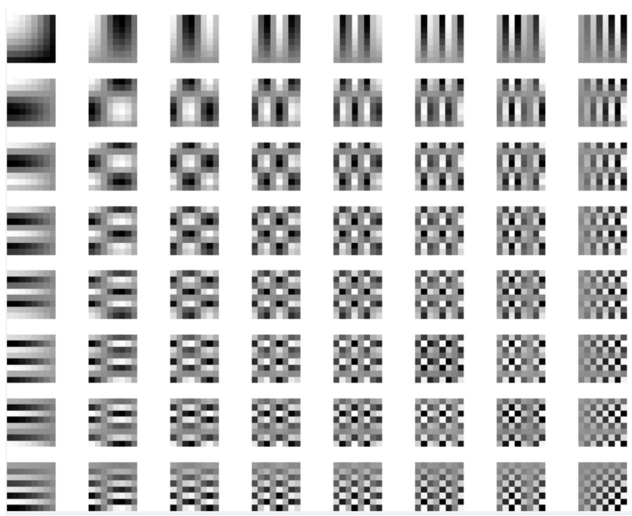

Figure 2: Outputs of 8x8 DCT [24]

4.1.Image Watermarking With Spatial Domain Transformers Based On Discrete Cosine Transform

SVD is a powerful and convenient matrix decomposition; although it is applied in the spatial domain, with small changes implemented on singular values enables indiscernibility feature [25]. As an example of SVD and DCT combination Roy and Pal [22] offer a gray scale image watermarking method. In their method, the main image was separated into 8x8 blocks and DCT was applied. Meanwhile, watermark is scrambled by Arnold Transform. Afterward, SVD is applied to both scrambled watermark and transformed cover image then coefficients of watermark are embedded to coefficients of the cover image. Obtained data blocks were converted back into image blocks with reverse DCT to generate watermarked image. In order to extract the watermark, the watermarked image is split into blocks and DCT, SVD and inverse Arnold Transform are applied respectively. Since the method does not require the original cover image to extract the watermark, it is classified as semi-blind watermark. To analyze the proposed method Lena, Pepper and Baboon images are selected. Performance analysis is calculated with PSNR and NC values. After Lena is watermarked PSNR 50.5281dB and NC 0.9945 are calculated. Robustness analysis is implemented with Gaussian filter, compression, rotation and cropping attacks. NC results range from 0.7651 to 0.9905.

Another method is applied in the spatial domain Principal Component Analysis (PCA). PCA which enables computation of dominant vectors representing a given data set is indicated with SVD calculation method. Besides PCA allows eliminating the linear dependence of the data. Watermarking technique with PCA and DCT on a color image presented by Saboori and Hosseini [3]. RGB image is converted to YCbCr image and linear dependence coefficient is calculated, and YCbCr image is converted to an 8x8 matrix. DCT is applied to each block, a vector is created by choosing low frequency coefficients from the blocks, and PCA is applied to the resulting vector. The watermark is also converted to a vector which is embedded in PCA output of the cover image. Reverse PCA is applied to the obtained vector and the coefficients are added to low frequencies of DCT blocks then to obtain the watermarked image reverse DCT is applied. Both watermarked image and original cover image are used to extract the watermark. Therefore, it has the feature of non-blind watermark. Colorful Lena image is selected to analyze the method. PNSR is calculated as 40.08dB and NC is 1 as the performance analysis. Rotation, filtering and compression attacks are carried on for the robustness analysis with NC results between 0.3123 and 1. With this proposed method, 64x64 watermark can be embedded in 512x512 cover image. According to the robustness analysis, SVD provides more durability than PCA.

Furthermore, spatial domain digital image watermarking is also performed for cryptology purposes. Watermark can be encrypted to add extra security to the method. Hash function is a widely used encryption method. While SVD and PCA methods are parsing the signal into different vectors Hash function is encrypting the signal by mapping random integers [26]. Al- Shehhi et al. [27] propose a method for dual fragile and robust watermarks to ensure copyright and authentication. With the aim of copyright DCT method in the frequency domain is applied on robust watermark, while for authentication Hash function is implemented in the spatial domain to provide random encoding on fragile watermark. The system is tested with RGB satellite images. Besides PSNR value is greater than 40dB and NC value is greater than 0.99 are calculated. While spatial domain transformation in the application gives the system a fragility feature, its effect is around 0.1%. In the presented method, attack analysis was not performed. This method provides two types of watermark: fragile watermark for authentication purposes to prevent unauthorized copying or modification of satellite images, and robust watermark with DCT for copyright control. However, as stated in the method, DCT is not used directly for the fragile watermark.

During the watermarking process, spatial domain not only provides complex methods but also bit-based conditional decomposition. Cai-Yin et al. [28] design a CMYK color model image-based watermarking technique. CMYK color is parsed into the color components. Yellow component is separated into blocks and DCT is applied. The content information of watermark is embedded in the coefficients created in the frequency domain with different algorithms according to 1-0 bit values. After Fast Fourier Transform is performed to black component, DCT is implemented to the structural template of watermark and DCT coefficients are embedded to black component. Yellow component and black components are combined with spatial visual masking technique according to brightness, edges, texture and contrast properties. 300 images in 6 different color categories were used to analyze the method. PSNR value of these images is calculated as higher than 35dB.

4.2.Image Watermarking with Discrete Wavelet Transform Based on Discrete Cosine Transform

Hybrid modeling of DCT and DWT is a widely used technique for image watermarking. Distinguishing an image by the human eye is executed by Human Visual System (HVS). To detect by HVS image must have enough contrast. Therefore, edges and textures rather than smooth areas attract more attention by HVS [13]. As entropy increases, the image becomes smoother and becomes out of focus [23]. For watermarking, both low visibility and high processing power methods should be used, taking into account of HVS [7]. For this reason, entropy is a key feature of a noticeable change. Thanks to DWT, image signals can be divided into low and high frequency subbands, which makes it easier to embed watermarks according to the entropy of the system. Moreover, watermarking applied to high frequency coefficients including edges and textures provides more capacity [29]. Xia et al. [30] compare DCT and DWT in their study; DCT is fragile for compression, re-scaling and high noise variant attacks has proposed. However, after this study Jabber and Tuieb [29] establish that during dual use of DWT and DCT, PSNR value of DCT is significantly higher than DWT. Hazim et al. [31] state that the combined use of DCT and DWT increases the robustness and performance of watermark. In the literature, there are various methods developed by combining DCT, DWT and different techniques.

Xiaomin and Fengyuan [32] present a method to embed a color watermark on a color image. The pixels of watermark are scrambled with Arnold Transform. Meanwhile, the low frequency component is obtained by separating the red component from RGB cover image and applied DWT. 8x8 blocks are obtained by performing 8x8 DCT to the low frequency component. The scrambled watermark is embedded in the resulting blocks and reverse DCT and reverse DWT are applied. Combining watermarked red image component with unprocessed green and blue image components generates the watermarked image. To extract the watermark, watermarked image is separated into its red component and DCT and inverse Arnold Transform are applied respectively. Since watermarked image is used during the extraction process, the method has the feature of semi-blind watermark. PSNR value is calculated as 43.7989dB and NC as 1. In order to test the robustness of the presented method, NC values are calculated after filtering, scaling, noise, cropping and rotation attacks, and results are ranged in 0.6501 - 1. The proposed method is most fragile for noise attacks.

Apart from that Zhang and Wei [33] propose a combination of DWT, DCT, Generalized Arnold Transform and SVD based on Particle Swarm Optimization (PSO). While Generalized Arnold Transform increases the security of the method by using more keys to mix the data comparing to Arnold Transform, embedding factor matrix is obtained by PSO during SVD process gains the system robustness. PSO is an optimization method used to get a random value; often used in dynamic and multi-target environments. The proposed method is primarily allocated to the real part of cover image in frequency domain by DCT. After arranging coefficients, 3-level DWT is enforced on each and third-lowest frequency coefficient (LL3) and third-highest frequency coefficient (HH3) are obtained. SVD is applied to low frequency and high frequency subbands one by one. Meanwhile, after watermark is formed into a meaningless index with Generalized Arnold Transform, DCT and 2-level DWT are applied respectively to obtain second-lowest coefficient (LL2). SVD is also performed to LL2. Three different diagonal matrices are obtained from the cover image and watermark after SVD are combined into a single diagonal matrix with the help of a key produced with PSO. At the end of the process, watermarked image is generated by applying reverse SVD, reverse DWT and reverse DCT respectively. Embedding processes are applied one by one to recover the watermark; consequently, HH3 and LL3 subbands are obtained after DWT. With these two subbands and reverse SVD, reverse DWT and reverse DCT two different copies of the watermark are obtained. For the sake of capacity, it is designed to embed maximum 256x256 watermark in 512x512 cover image. Since the key and watermarked image are sufficient to extract watermark, the proposed method represents blind watermark feature. Gray test images such as Lena, Barbra, Goldhill and Boat are used in the analysis of technique. PNSR value between watermarked image and original image is calculated for the imperceptibility measurement, as 48.9906dB for Lena. NC value of watermark is 1. For robustness analysis, compression, cropping, Gaussian filter, scaling, 45-degree rotation and sharpening attacks are applied and NC values are calculated in the range of 0.9617-0.9997. For this reason, Generalized Arnold Transform provides greater robustness than traditional Arnold Transform.

4.3. Image Watermarking with Complex Algebra and Machine Learning Based on Discrete Cosine Transform

While robustness of the system is increased with DCT, to strengthen the imperceptibility of the process difficult-to-solve techniques such as complex algebraic algorithms and machine learning methods can be executed on watermarking.

Horng et al. [34] proposed a watermarking technique that is intended to be used in online public services. The purpose of the technique is authentication, data integrity and security. After brightness masking is applied to the gray-scale cover image, DCT and 4-block DCT are applied respectively. SVD is applied to DCT performed watermark and coefficients of DCT performed cover image to generate decomposed vectors. Optimization based on genetic algorithm is applied to obtained SVD vectors to frame a map for watermark embedding on cover image. Afterward by inverse DCT watermarked image is composed. During the watermark extraction process, the map generated by the genetic algorithm is used as the secret key. Therefore, suggested method is blind watermark. For the robustness analysis, gray scale 256x1024 Lena as cover image and 256x256 watermark are selected. NC is calculated as 0.81. Robustness analysis is performed with Gaussian filter, JPEG compression and cropping attacks that generate NC values in the range of 0.6041-0.7676.

Benoraira et al. [35] present blind watermark method using Random Permutation Technique with DCT and a secret key. To implement, cover image is converted to entropy dependent one-dimensional matrix by Zig Zag method. The obtained matrix is decomposed into two different series of related coefficients and DCT is performed to each of them. Watermark is embedded in two different frequency series by using Random Permutation Technique depending on the secret key. Finally by performing reverse DCT and reverse Zig Zag to produced frequency series forms watermarked image. Since a secret key is required during the watermark recovery, it shows blind watermark feature. For performance analysis 512x512 gray scale Lena image is chosen. After the embedding process PSNR value between original cover image and modified cover image is calculated as 45dB. For robustness analysis, watermarked image is suffered by JPEG compression, filtering and noise attacks, results with PNSR higher than 42dB. Attacks indicate that while it is robust to cropping and compression attacks, it is fragile to rotation attacks.

Another proposed method with modern algebra is watermarking technique based on the Local Ring is presented by Jamal et al. [36]. In the proposed method, watermark is encrypted in an S-set created by Local Ring and Finite Field (Galois Field) method. To decompose into complex values of the cover image and obtain low and medium frequency coefficients DCT is applied. Most significant four bits of each pixel of S-set are embedded in least significant four coefficients of cover image after DCT. Original cover image is involved in reproducing watermark, thereby shows non-blind watermark feature. Although watermark S-set created by Local Ring and Finite Field is increased the complexity of technique, it reduces the detectability probability. The method is analyzed with Lena, Pepper and Baboon images. After original Lena image is watermarked, PNSR value is calculated as 46.5741dB. As a result of exposing compression, noise and clipping attacks, noise attack shows the most fragile impact with PSNR value 18.3259dB. Since the numerical results of the post-attack similarity analyzes are in the range of 40-79%, the method is classified as semi-fragile watermark.

Kernel Extreme Learning Machine (KELM) and Differential Evaluation (DE) DCT based watermarking method presented by Vishwakarma & Sisaudia [23] can be given as an example of watermarking techniques by machine learning and modern algebra based on DCT. KELM is used for a single-layer feed-forward neural network application. It expresses a core matrix with unique results. Besides DE is executed for multiple scaling coefficient optimizations. In the proposed method, cover image is divided into 8x8 blocks and their entropies are calculated. Watermark is converted to a 1-D binary array. According to the increasing entropy, number of coefficients that calculates by two times size of the watermark array is selected and DCT is applied to each block. 3x3 matrices are created by choosing the coefficients according to the Zig-Zag manner that provides the entropy sequence of blocks. The lowest frequency coefficient of each matrix are summed and used as a training dataset of KELM. With DE, unique scaling coefficients are generated for each block. Each bit of the watermark is embedded using an algorithm that changes according to its binary value based on KELM output and the scaling factor. Afterward, inverse Zig Zag transform and inverse DCT are performed to generate watermarked image. To recover watermark after embedding processes are applied to watermarked image, even coefficients decomposed by DCT and learning dataset of KELM are formed a watermark sequence. Watermark recovered by transforming the sequence to 2-D. Proposed method has semi-blind watermark feature since cover image and learning dataset are required for extraction. Moreover, the capacity of the system is suitable for 512x512 cover image and 32x32 watermark. Gray scale Lena is used for analysis, after watermarking PNSR and NC are calculated 44.9dB and 1 respectively. Gaussian filter, JPEG compression and 180-degree rotation attacks are performed for robustness test. As a result of the attacks, NC is calculated between 0.6255 and 1, which indicates the less robustness for 180-degree rotation attacks.

Lastly Tarhouni et al. [11] present a blind watermarking method based on DCT and Speed-up Robust Feature (SURF). SURF is a feature detector and descriptor algorithm that provides computer-based object recognition, classification, and recording. In the proposed method, SURF enables the watermark to be recovered with little damage, even if the watermarked image is manipulated, thanks to the feature matrix it creates. For embedding RGB cover image is transformed to YCbCr color space and decomposed into Y, Cb and Cr coefficients. Y coefficient is converted into 8x8 blocks and 2D DCT is applied to all blocks. Resulting frequency series are aligned according to Zig Zag manner to select middle frequencies. Watermark is embedded in least significant bits of selected middle frequencies. After embedding reverse Zig Zag , reverse DCT, YCbCr coefficients composition and RGB transformation are applied respectively to generate watermarked image. Coefficients used in watermarking algorithm and SURF feature matrix forms the secret key. For this reason it demonstrates blind watermark manner. To applicate the proposed method RGB Lena image is selected, and as a result of process, PSNR value is calculated as 44.9dB while NC is 1. In the robustness analysis, JPEG compression, Gaussian filter, scaling and 5 degree rotation attacks are performed and NC values are calculated in the range of 0.8-1.0. That shows the method is less robust to rotation attacks.

5. Evaluations and Conclusions

DCT based watermarking techniques in literature were reviewed and evaluated in Table 1. Methods, feature of watermark, the reliability of the process and the results of robustness analysis were reviewed. Pros and cons of these studies were analyzed. The result of this review shows that

- DCT has been involved in watermarking processes with a combination of different methods instead of single use. A union of several methods enhanced the strength of watermarking techniques based on DCT.
- The proposed methods differed in terms of usage areas and robustness.
- In fragile watermarking, DCT was not preferred because of its high robustness.
- Blind, semi-blind and non-blind watermarks, which are classified according to watermark recovery method, can be developed by DCT based methods.
- The character of watermark extraction is not directly related to robustness.
- Complex algebraic methods were frequently executed for blind watermark to generate a secret key that would be used for watermark extraction.
- For robustness analysis only active attacks were applied by the researchers. Passive attacks can be a future study.
- After watermark process and PSNR values between watermarked cover image and cover image were calculated higher than 35dB.
- Meanwhile NC values between watermark and extracted watermark were calculated between 0.81-1.00.
- The highest distortion in extracted watermark was captured with the combination of DCT and spatial domain transforms under rotation attacks.
- A certain result of attack effect cannot be obtained due to diversity of the impacts on proposed methods.

In conclusion, various methods that could be performed in watermarking based on DCT for different usage areas were specified. Thanks to its feature of separating the image into coefficients in frequency domain, DCT increased the robustness of watermarking. However, it should be highlighted that DCT was not single use method in watermarking; it should be combined with several methods to increase the quality of process.

STUDY	WATERMARK TYPE	TYPE OF IMAGE	METHODS	PSNR, NC VALUE AFTER WATERMARKING	NC VALUES AFTER ATTACKS
Roy and Pal [22]	Semi-blind, robust	Lena, colored	8x8 DCT, Arnold Transform, SVD	50.5281 dB, 0.9945	• 20-degree rotation 0.7651, • Gaussian filter 0.9018, • JPEG compression 0.9414, • Cropping 0.9905
Saboori and Hosseini [3]	Non-blind, robust	Lena, RGB	DCT, PCA	40.0800 dB, 1	• Rotation 0.3123, • Gaussian filter 1, • JPEG compression 0.9502
Al-Shehhi et al. [27]	Semi-blind, fragile	Satellite image, RGB	DCT, Hash function	40,0000 dB, 0.9900	Robustness analysis is not performed.
Cai-yin et al. [28]	N/A	300 different CMYK image	DCT, Fast Fourier Transform, Spatial Visual Masking	35,0000 dB, N/A	Robustness analysis is not performed.
Xiaomin and Fengyuan [32]	Semi-blind, robust	RGB image	DCT, DWT, Arnold Transform	43.7989 dB, 1	• Filtering 0.9958, • Scalling 1, • Noise 0.6501, • Cropping 0.7756, • Rotation 0.9567
Zhang and Wei [33]	Semi-blind, robust	Lena, gray-scale	DCT, DWT, Generalized Arnold Transform, Particle Swarm Optimization	48.9906 dB, 1	• Compression 0.9997, • Cropping 0.9702, • Gaussian filter 0.9711, • Scalling 0.9976, • 45-degree rotation 0.9805, • Sharpening 0.9617
Horng et al. [34]	Blind, robust	Lena, gray-scale	DCT, SVD, Genetic Algorithm	N/A, 0.8100	• Gaussian filter 0.6041, • JPEG compression 0.6667, • Cropping 0.7676
Benoraira et al. [35]	Blind, robust	Lena, gray-scale	DCT, Random Permutation	45.0000 dB, N/A	• JPEG compression, • Noise • Filtering > 42 dB
Jamal et al. [36]	Non-blind, robust	Lena, colored	DCT, Local Ring, Finite Field	46.5741 dB, 0.9437	• JPEG compression, • Noise, • Cropping
Vishwakarma and Sisaudia [23]	Semi-blind, robust	Lena, gray-scale	DCT, KELM, DE	44.9000 dB, 1	• Gaussian filter 1, • JPEG Compression 1, • 180-degree rotation 0.6255
Tarhouni et al. [11]	Blind, robust	Lena, RGB	DCT, SURF, YCbCr Transform	44.9000 dB, 1	• JPEG compression 0.9800, • Gaussian 1, • Scalling 1, • Rotation 0.8000

Table 1: Summary of Literature Survey

Especially from last three years' studies, machine learning and optimization techniques would be frequently used methods for future studies in watermarking based on DCT.

References

[1]. K. Singh, "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images", Multimedia Tools and Applications, vol. 76, no. 6, pp. 8881–8900, 2016.

[2]. M. Begum and M. S. Uddin, "Digital Image Watermarking Techniques: A Review", Information, vol. 11, no. 2, p. 110, 2020.

[3]. A. Saboori and S. A. Hosseini, "A new method for digital watermarking based on combination of DCT and PCA", 22nd Telecommunications Forum Telfor (TELFOR), 2014.

[4]. J. Seitz and T. Jahnke, "Digital Watermarking", Digital Watermarking for Digital Media, pp. 1–29, 2005.

[5]. M. Arnold, M. Schmucker, and S. D. Wolthusen, "Techniques and applications of digital watermarking and content protection", Boston: Artech House, 2003.

[6]. C. T. Yen and Y. J. Huang, "Frequency domain digital watermark recognition using image code sequences with a back-propagation neural network", Multimedia Tools and Applications, vol. 75, no. 16, pp. 9745–9755, 2015.

[7]. H. U. Seo, Q. Wei, S. G. Kwon, and K. I. Sohng, "Medical Image Watermarking using bit threshold map based on just noticeable distortion in discrete cosine transform", Technology and Health Care, vol. 25, pp. 367–375, 2017.

[8]. M. Irany, "A high-capacity reversible multiple watermarking scheme-applications to images, medical data, and Biometrics", M.S. thesis, University of Toronto Graduate Department of Electrical and Computer Engineering, Toronto, 2011. Accessed on: Sept. 5, 2021. [Online]. Available: https://tspace.library.utoronto.ca/bitstream/1807/29530/6/MehrbanyIrany_Behrang_201106_MASc_thesis.pdf

[9]. A. T. Abdel-Hamid and S. Tahar, "Fragile IP watermarking techniques", 2008 NASA/ESA Conference on Adaptive Hardware and Systems, 2008, pp. 513-519, doi: 10.1109/AHS.2008.73

[10]. S. M. Mousavi, A. Naghsh, and S. A. Abu-Bakar, "Watermarking techniques used in medical images: A survey", Journal of Digital Imaging, vol. 27, no. 6, pp. 714–729, 2014.

[11]. N. Tarhouni, M. Charfeddine, and C. Ben Amar, "Novel and Robust Image Watermarking for copyright protection and Integrity Control", Circuits, Systems, and Signal Processing, vol. 39, no. 10, pp. 5059–5103, 2020.

[12]. Y. M. Li, D. Wei, and L. Zhang, "Double-encrypted watermarking algorithm based on cosine transform and fractional Fourier transform in invariant wavelet domain", Information Sciences, vol. 551, pp. 205–227, 2021.

[13]. M. A. Nematollahi, C. Vorakulpipat, and H. G. Rosales, "Digital Watermarking - techniques and trends: Mohammad Ali Nematollahi", Springer, 2018. [Online]. Available: https://www.springer.com/gp/book/9789811020940. [Accessed: 04-Sep-2021].

[14]. L. Verma and S. Pratap Singh Chauhan, "A review on Digital Image Watermarking using transformation and optimization techniques", 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2020.

[15]. K. Chaitanya, D. E. S. Reddy, and D. K. G. Rao, "Digital color image watermarking in RGB planes using DWT-DCT-SVD coefficients", International Journal of Computer Science and Information Technologies, vol. 5, no. 2, 2013.

[16]. T. Veldhuizen, Measures of image quality, 1993. [Online]. Available: https://homepages.inf.ed.ac.uk/rbf/CVonline/LOCAL_COPIES/VELDHUIZEN/node18.html. [Accessed: 04-Sep-2021].

[17]. J. Cox, M. L. Miller, and J. A. Bloom, "Watermark security", Digital Watermarking, pp. 279–317, 2002.

[18]. K. Mahmoud, S. Datta, and J. Flint, "Frequency Domain Watermarking: An Overview," The International Arab Journal of Information Technology, vol. 2, 2005.

[19]. I. Ito, "A new pseudo-spectral method using the discrete cosine transform", Journal of Imaging, vol. 6, no. 4, p. 15, 2020. Accessed on: Sept. 5. 2021. [Online]. Available doi: 10.3390/jimaging6040015

[20]. M. Gupta and A. K. Garg, " Analysis Of Image Compression Algorithm Using DCT," International Journal of Engineering Research and Applications, vol. 2, no. 1, 2012.

[21]. B. Kaur, A. Kaur, and J. Singh, "Steganographic Approach For Hiding Image In Dct Domain," International Journal of Advances in Engineering & Technology, vol. 1, no. 3, pp. 72–78, 2011.

[22]. S. Roy and A. K. Pal, "An indirect watermark hiding in discrete cosine transform–singular value decomposition domain for copyright protection", Royal Society Open Science, vol. 4, no. 6, p. 170326, 2017.

[23]. V. P. Vishwakarma and V. Sisaudia, “Gray-scale image watermarking based on DE-KELM in DCT domain”, Procedia Computer Science, vol. 132, pp. 1012–1020, 2018.

[24]. X. Huo, “Sparse image representation via combined transforms”, Ph.D dissertation, Stanford University Department of Statistics, California, 1999. Accessed on: Sept. 5, 2021. [Online]. Available: https://statistics.stanford.edu/sites/g/files/sbiybj6031/f/1999-18.pdf

[25]. A. Fita and B. Endebu, “Watermarking Colored Digital Image Using Singular Value Decomposition for Data Protection,” Journal of Mathematical and Statiscal Analysis, vol. 1, no. 2, 2019.

[26]. J. S. Coron, Y. Dodis, C. Malinaud, and P. Puniya, “Merkle-Damgård Revisited: How to construct a hash function,” Advances in Cryptology – CRYPTO 2005, pp. 430–448, 2005.

[27]. S. Al-Shehhi, M. Al-Muhairi, D. Abuoeida, H. Al-Ahmed, N. Werghi, and A. Kunhu, “Robust and fragile watermarking scheme based on DCT and hash function for color satellite images”, 6th IEEE International Conference on Developments in eSystems Engineering, 2013.

[28]. W. Cai-Yin, K. Xiang-Wei, and L. Chao, “Process color watermarking: The use of visual masking and dot gain correction”, Multimedia Tools and Applications, vol. 76, no. 15, pp. 16291–16314, 2016.

[29]. K. Jabbar and M. B. Tuieb, “Compare between DCT and DWT for digital watermarking in color image”, Information and Knowledge Management, 2015. [Online]. Available: https://www.iiste.org/Journals/index.php/IKM/article/view/23907. [Accessed: 04-Sep-2021].

[30]. X. G. Xia, C. Boncelet, and G. Arce, “Wavelet transform based watermark for digital images”, Optics Express, vol. 3, no. 12, p. 497, 1998.

[31]. N. Hazim, K. L. Hammed, and Z. Saeb, “Image watermarking with hybrid approach using discrete wavelet transform(dwt)–discrete cosine transforms (DCT)”, International Journal of Advance Engineering and Research Development, vol. 3, no. 02, 2015.

[32]. Xiaomin and Z. Fengyuan, “Double-color digital image watermarking technology based on double transform domain”, IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), 2020.

[33]. Zhang, Lina, and D. Wei, “Dual dct-dwt-svd digital watermarking algorithm based on particle swarm optimization”, Multimedia Tools and Applications, vol. 78, no. 19, pp. 28003–28023, 2019.

[34]. S. J. Horng, D. Rosiyadi, P. Fan, X. Wang, and M. K. Khan, “An adaptive watermarking scheme for e-government document images”, Multimedia Tools and Applications, vol. 72, no. 3, pp. 3085–3103, 2013.

[35]. Benoraira, K. Benmahammed, and N. Boucenna, “Blind image watermarking technique based on differential embedding in DWT and DCT domains”, EURASIP Journal on Advances in Signal Processing, vol. 2015, no. 1, 2015.

[36]. S. S. Jamal, T. Shah, S. Farwa, and M. U. Khan, “A new technique of frequency domain watermarking based on a local ring”, Wireless Networks, vol. 25, no. 4, pp. 1491–1503, 2017.