A Recent Survey of DCT Based Digital Image Watermarking Theories and Techniques: A Review

Ranjeet Kumar Singh[1(✉)] and Anil Kumar Singh[2]

[1] National Institute of Technology, Jamshedpur 831014, Jharkhand, India
2014rsca002@gmail.com
[2] School of Management Sciences, Varanasi 221011, Uttar Pradesh, India
singhanilkumar@zoho.com

Abstract. Digital image watermarking is one of the most discussed research areas. It plays an essential role in the field of digital information authentication and security. Based on the study of watermarking systems, image watermarking is divided into two modules: One is watermark embedding, and the other is watermark extraction. This paper reviews the theoretical and experimental analysis and performance measurement of a representative digital image watermarking system in spatial and transforms domains. The key characteristics of a digital image watermarking scheme are robustness, capacity, imperceptibility, the security of the hiding place, and false positive of the watermarking algorithm. Comparison of the different watermarking techniques employing the discrete cosine transform (DCT) is given. This paper presents various details of the algorithm of digital image watermark embedding and extraction process in a different domain and also explains their advantages and disadvantages.

Keywords: Discrete cosine transformation · Digital encryption · Image processing · Watermarking

1 Introduction

In the contemporary era of digital information sharing, it is only desirable to have a robust and safe ecosystem for it to thrive. The main advantage of exchanging data on digital media is the accuracy with which information can be passed on [1]. Digital image watermarking provides security against unauthorized access and confirms digital data ownership [2]. Cryptography is one of the approaches available for information protection and system security. In a conventional cryptographic system, the encrypted information can be decrypted only by an authentic user who would be aware of the decryption key. But in a situation when this information is deciphered by a hacker or any other unintended person, we are left with minimal choices to shield the information and track its illegal distribution. It is a significant shortcoming of conventional cryptography. Watermarking is one efficient way to protect intellectual property and overcome the issue above. Watermarking is an approach which is used to embed information into a cover image to provide authentication of the digital data. It facilitates ownership of digital information.

A. K. Luhach et al. (Eds.): ICAICR 2019, CCIS 1075, pp. 431–440, 2019.
https://doi.org/10.1007/978-981-15-0108-1_40

Some of the watermarking applications are given below [3, 4]:

- **Copyright Protection:** To secure intellectual property, the owner of data can hide watermark information used for authentication of data. The hidden watermark is treated as a piece of evidence, e.g., in case of willful infringements of copyright.
- **Fingerprinting:** To search for the source of protected copies, the authentic user can use a mechanism which is known as fingerprinting. By using this technique, the genuine user can hide different watermark data as replicas of the data that are delivered to different users. Fingerprints can be matched by inserting a serial number, and this serial number can be used to validate the authentic user for the data concerned.
- **Copy protection:** The data hid in the watermark can manipulate the recording devices for copy protection of digital data. In such a situation, the watermark denotes a copy-prohibited bit, and watermark sensors in the recorder determine if the data input to the recorder is saved or not.
- **Data Hiding:** Watermark approach is useful in transmitting secret information. Since many data admins do not use the encryption facilities, users can hide information in other data.
- **Medical safety:** Hiding the patient's identity and their medical conditions that are usually stored in images could be a useful safety measure.
- **Non-perceptibility:** Non-perceptibility refers to the watermark embedded into information that cannot be seen by users. It will be identifiable only through dedicated circuits.
- **Robustness:** Watermark, which is presented in the original data, can continue its existence even after a different image processing attack. The watermark is robust and can defend itself against image processing attacks. Image processing attacks can be classified mainly into rotation, scaling, and noise.

1.1 Classification of Digital Watermarking

Digital watermarking is a mechanism used to embed data, known as a watermark, into multimedia or a digital object. The insertion process is such that the hidden information can be detected later and recovered to assert the object. The digital items in which the watermark information is inserted are generally known as the host signals, the original, or simply, the work.

Figure 1 depicts the various forms of watermarks. Watermarks are classified into four broad categories, viz., video, audio, image, and text. Based on human perception, watermarking can be classified into a visible, invisible-robust, invisible-fragile, and dual watermark. Visible watermarking is robust, but the area of application is small and limited. In invisible watermarking, the watermark cannot be detected by the human eye. Only the authentic user knows the watermark. Another user cannot identify the watermark, and they have no means to change the watermark. A robust watermarking technique is generally used to sign copyright of digital content. The hidden and inserted watermark data can resist several forms of images processing.

Any signal processing attack does not damage the watermark data, and it can be detected for official certifications. Integrity protection fragile watermarking is typically

used because it is very complex to alter the signal. In the case of the invisible-fragile watermarking scheme, the watermark information is inserted in a way that any change or manipulation of the picture results in ruining the watermark. In case of the dual watermarking scheme, it is a combined approach of the visible watermarking and the invisible watermarking schemes. Here, the watermarks are the blend of visible watermarks and the invisible watermarks. The invisible watermark is used in this case to back up the visible watermark.

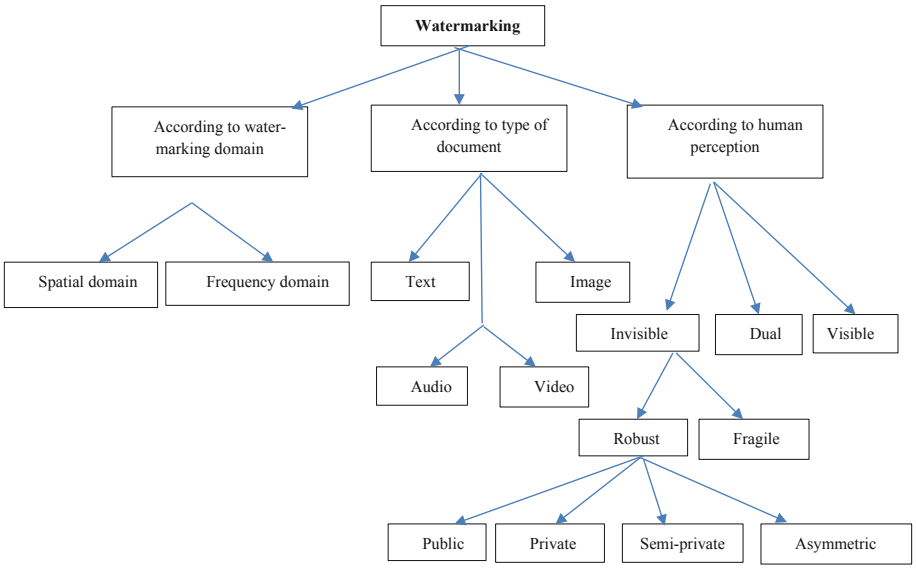

Fig. 1. Different watermarking schemes

Robust watermarking is categorized as follows:

- **Private watermarking scheme:** In the case of private watermarking, we need the host image for detection of watermark. Private watermarking is classified into two types: Type I system and Type II system.
- **Type-I systems** recover the watermark information from the tested, and probably, the tattered image. The host image is required to find the locality of the watermark data in the disrupted image.
- **Type-II systems** need a duplicate of the inserted watermark data for watermark identification, and they are capable of expressing whether a piece of specified watermark information in the verified image exists or not.

Both the schemes are used to create knowledge about the embedding key (Private Key). The embedding key is private data that inserts the watermark into the cover object.

- **Semi-private watermarking:** In this scheme of watermarking, the original image is not required for the detection of the watermark. It gives information about the watermark, which is present or not in the watermarked image.
- **Public watermarking:** Also known as the blind watermarking, there is no need for the cover image and inserted watermark for the watermark extraction procedure. This watermarking scheme requires a more complex watermark technology, and its field of application is wide.
- **Asymmetric watermarking:** This watermarking is known as public-key watermarking. In contrast to the public watermarking mechanism, in this scheme, everyone knows the detection scheme and the detection key. The knowledge about the public key either prevents finding the private key, or it restricts the removal of the watermark.

1.2 Copyright Protection Watermarking and Tampering Tip Watermarking

Watermarking is basically a process of imbibing certain media inside the original information [5]. In copyright protected watermarking, an authentic user would want other users to see the watermark data; then the watermark data can be seen by other users after embedding watermark data to the original information. According to the watermarking domain, it is mainly divided into spatial and frequency domain. In case of a spatial domain watermarking, watermark information is directly put together with the cover image. One of the spatial domain watermarking schemes is the LSB (Least significant bits) mechanism. In this mechanism, the watermark information is inserted into the least significant bits of the cover image. But the spatial domain watermarking suffers a serious issue of limited sturdiness [6]. In the frequency domain scheme, the watermark information is added to the original image. Image transform is then used to modify the image coefficients. Normally, masking based transformed domain techniques are more robust than LSB mechanism from the image processing attacks such as compression and cropping viewpoint.

2 Discrete Cosine Transform (DCT)

Another transform domain watermarking approach is a discrete cosine transform (DCT). Compared to the discrete Fourier transform (DFT), DCT is a better digital watermarking technique because it involves only the orthogonal transformation of real numbers, unlike the DFT where a digital image is computed as a part of a complex number. DCT has the advantage of high-compression ratio and low error-rates [7]. Based on frequency components, this approach allows dividing an image into three parts, viz., low, high, and middle-frequency bands. We can insert watermark in any frequency band. The literature survey discloses that usually the middle frequency components are used to add watermark because, in the middle-frequency component, the information stored in watermark often cannot be scattered. If the watermark is rooted in a low-frequency component, the mechanism tends to be resistant against malicious image-processing attacks, but it is a daunting task to hide the watermark. But

in case of the watermark embedded in a high-frequency band, i.e., a perceptually insignificant component, watermark hiding scheme is more straightforward. However, the system is less resistant to image processing attacks [8–11]. The equations given below describe the 2D-DCT and 2D-IDCT. 2D-DCT (two-dimensional discrete cosine transform) *F [u, v]* of a digital image matrix *f [m, n]* is:

$$F[U,V] = \sum_{n=1}^{N}\sum_{m=1}^{M}[u,v]\, f[m,n] \cos\frac{\pi(2m-1)(u-1)}{2M}\cos\frac{\pi(2n-1)(v-1)}{2N}$$

Where,

$$[u,v] = \begin{cases} \frac{1}{\sqrt{MN}} & When\ u = 1\ and\ v = 1 \\ \sqrt{\frac{2}{MN}} & When\ u = 1\ and\ v \geq 2\ or\ v = 1\ and\ u \geq 2 \\ \sqrt{\frac{4}{MN}} & else \end{cases}$$

Where, *w [u, v]* is known as weight factor of the transform, *n* and *v* vary from 1 to N, and *m* and *u* vary from 1 to M.

Liu et al. [7] developed a novel watermarking algorithm by a serial amalgamation of fractal encoding and discrete cosine transformation (DCT) techniques. Through this dual encryption method, the authors proposed an improved DCT encryption technique. A cover image is first encoded using the fractal encoding, followed by the second encryption of the encoded parameters using DCT. With the help of only two dimensions of scaling and offset, and applying three types of attacks, the authors tested their technique to conclude that this new embedded technique is more robust and effective.

Roy and Pal [12] came up with a DCT technique, embedded with a repetition code approach of color watermarking for copyright ownership and validation. The authors eliminated the 'blocking artifact,' a significant drawback of the block-based DCT, by making use of zigzag scanning of each RGB component's DCT block. The purpose of this work was to use the error correcting code (ECC), called the repetition code for preserving one watermark bit in every decomposed non-overlapping RGB component's block. This multiple image watermarking technique demonstrated an imperceptibility property and yielded higher PSNR value and better robustness. But these benefits were achieved only at the price of higher computational complexities.

Singh et al. [13] made use of a hybrid scheme comprising of SVD, DCT, and nonsubsampled contourlet transform (NSCT) to derive a robust, high capacity, and imperceptible watermarking of confidential medical images. In this algorithm, the electronic patient record (the secret message) is rooted into the sub-band of the cover image (the medical image) with a chosen gain factor, resulting in an improved capacity, imperceptibility, and robustness. They determined that clubbing NSCT and SVD with DCT yields a more secure and high-quality image watermarking.

Zear et al. [14] made use of multiple watermarking schemes comprising of DCT, DWT, and SVD for application in the healthcare industry. They went on to use the Back Propagation Neural Network (BPNN) on the recovered image watermark to suppress noise residuals on the recommended grayscale image for watermarking.

2.1 Inverse Discrete Cosine Transform (DCT)

The two-dimensional (2D) inverse discrete cosine transform (IDCT) is defined in below equation:

$$f[m,n] = \sum_{v=1}^{N}\sum_{u=1}^{M} w[u,v]F[u,v]\cos\frac{\pi(2m-1)(u-1)}{2M}\cos\frac{\pi(2n-1)(v-1)}{2N}$$

W [u, v] = Fore mentioned weight factor

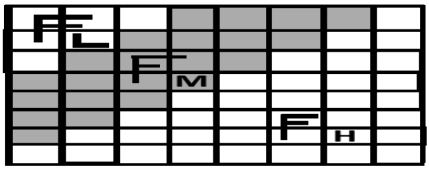

Fig. 2. Various frequency regions in the DCT domain

In Fig. 2, the DCT blocks having low-frequency components are depicted by FL, elements having high-frequency bands are represented by FH, and the middle-frequency bands are represented by FM [15].

In recent years, a lot of digital image watermarking schemes have been proposed to provide security and authentication to multimedia data. Various watermarking approaches have so far been suggested for images. Some DCT based image watermarking algorithms are jotted in the following literature survey.

Al-Baloshi et al. [11], addressed a DCT based image watermarking approach for image security and authentication. In their approach, the watermark was used as a form of visually meaningful binary pattern. Here authors divided the original image into N × N block size, then applied DCT on each block and inserted each DCT block to 1-bit of the watermark.

Al-Afandy et al. [16] proposed a DSWT and DCT based watermarking technique. Initially, the original image is converted its red, green, and blue (RGB) component, and DCT is applied to each color component. DCT output is divided into four sub-bands by using Discrete Stationary Wavelet Transform (DSWT). These frequency bands are represented by A, H, V, and D matrices with the same image size. Here, the watermark is inserted in matrix A.

A new blind multiple watermark scheme was presented by Ahmed N. Al-Gindy et al. [17], where two watermarks are used. Two vectors are created by two watermarks, and then they are merged. Low-frequency bands of the DCT Domain are chosen for insertion of watermark data. The cover image is divided into 8 × 8 block size, and sixteen coefficients of the host image of 8 × 8 sub-blocks are used for the addition of sixteen bits of the merged watermarks.

Nowadays, a binary watermark scheme has found utility in image security. Gindya et al. [18] explained the binary watermarking in a color image. In this technique, the

host image is converted into its RGB components, and the green component is chosen for watermarking. The green part is distributed into 8 × 8 sub-blocks, and DCT is applied on each block. The low-frequency component is selected for watermarking. Firstly, the watermark image is scrambled with the help of a private key and then changed to a vector. Before the commencement of the inserting scheme, the binary watermark vector is shifted with a specific shift for each time. This algorithm provides dual level security. First, the watermark is scrambled, and then another watermark is inserted in a particular color component.

For providing more robustness and protection to the digital content, several YC_bC_r color space-based watermarking is available. A. Al-Gindy et al. [18] had focused on the binary watermarking scheme in color image. The original colored image is converted into its RGB components to YC_bC_r color space. Y–channel is used for watermarking. First, the Y-channel ID has divided into N × N block sizes, and DCT is used on each block. The authors in this paper elected low-frequency component for embedding watermarks.

Arnold Cat Map is a widely used robust and efficient technique in image watermarking [19]. A combined approach of YC_oC_g-R color space and Arnold transform for data security was proposed by Moosazadeh and Ekbatanifard [20]. The authors used Arnold transform for multi-level security. The encryption of the watermark image was done by using Arnold transformations five times. The cover picture was transformed into its RGB color components. Then the RGB was converted to YC_oC_g-R and then separated the Y, C_o and C_g components. The Y component of the image was also scrambled by using Arnold transformations and turning its 8 × 8 block size. DCT is applied on each block to find a low-frequency band for insertion of a watermark.

Badran et al. [21] had explained the image watermarking algorithm based on the Expectation Maximization (EM) algorithm, which was used for image segmentation and DCT methods. All image segments used were divided into 8 × 8 block sizes and randomly reordered. The DCT was applied on each block, and a pseudorandom sequence of real numbers was inserted in each image segment of the DCT domain.

Gupta et al. [22] explained a new watermarking scheme built on DCT and LSFR. The host image was divided into N × N blocks size, and DCT was applied on each block. The watermark was converted in a bit sequence and stored in a one-dimensional array. Next, a pseudo-random number was generated by using a Linear Feedback Shift Register (LFSR). Here, the watermark bit was added to the low-frequency component.

Shuifa et al. [23] through their paper presented a binary image watermarking technique. First, the cover image was filtered by a Gaussian filter and then divided it into 8 × 8 blocks size. By applying DCT on each block and calculating the average DCT, the DC component of the whole image for block selecting and watermark data are inserted in these blocks.

The basic idea of DCT based image watermarking approach:

Embedding Process

Step 1: Select the watermark image and host image.
Step 2: Divide the original image into N × N blocks size.
Step 3: convert the original message and watermark image into double.
Step 4: Determine the size of Host image and watermark image.

Step 5: Find the numbers of the block in the host image, i.e., Max message size.
Step 6: Find the length of the watermark message.
Step 7: If the length of the host image message > length of watermark message gives an error
Step 8: Pad the watermark message.
Step 9: Apply DCT in each block
Step 10: Chose the middle-frequency band for embedding the watermark.
Step 11: Watermarked image.

Recovery process

Step 1: Chose a watermarked image and divided N × N blocks size.
Step 2: convert the watermarked image and watermark image into double.
Step 3: Determine the size of the watermarked image and watermark image in the form of several rows and columns.
Step 4: Find the maximum length of the watermarked image.
Step 5: Apply the DCT of each block and applying the inverse embedding procedure to get recover watermark (Fig. 3).

Fig. 3. (a) Original image (b) Watermark image (c) Watermarked image (d) Recovered watermark image

The main advantage of the DCT based image watermarking is that the watermark is embedded into the color channels of the original image. There are two critical issues in DCT based image watermarking. First, by selecting the high-frequency component, the filtering operation can remove the watermark information from the image. The next question is based on how much data modifications were made on DCT coefficients to insert the watermark data. These variations made on factors influence the hiddenness of the watermark information's and destroy the image to a huge extent.

3 Conclusion

In this paper authors explain the detailed working of discrete cosine transformation-based image watermarking for the purpose of providing the security and authentication of digital data. The detailed updated survey of DCT based watermarking is shown in this paper. Basically, DCT decomposes a matrix or a image matrix into low, high, and middle frequency components. Most of the research work carried out so far used middle frequency component for watermark embedding because human eye is less receptive to identifying changes in this component.

References

1. Singh, R.K., Kumar, B., Shaw, D.K., Khan, D.A.: Level by level image compression-encryption algorithm based on quantum chaos map. J. King Saud Univ.-Comput. Inf. Sci. (2018)
2. Singh, R.K., Shaw, D.K., Sahoo, J.: A secure and robust block based DWT-SVD image watermarking approach. J. Inf. Optim. Sci. **38**, 911–925 (2017)
3. Cox, I.J., Miller, M.L., Bloom, J.A., Honsinger, C.: Digital Watermarking. Morgan Kaufmann, San Francisco (2002)
4. Xuehua, J.: Digital watermarking and its application in image copyright protection. In: International Conference on Intelligent Computation Technology and Automation, pp. 114–117. IEEE (2010)
5. Singh, R.K., Shaw, D.K., Jha, S.K., Kumar, M.: A DWT-SVD based multiple watermarking scheme for image based data security. J. Inf. Optim. Sci. **39**, 67–81 (2018)
6. Singh, R.K., Shaw, D.K., Alam, M.J.: Experimental studies of LSB watermarking with different noise. Procedia Comput. Sci. **54**, 612–620 (2015)
7. Liu, S., Pan, Z., Song, H.: Digital image watermarking method based on DCT and fractal encoding. IET Image Process. **11**, 815–821 (2017)
8. Tewari, T.K., Saxena, V.: An improved and robust DCT based digital image watermarking scheme. Int. J. Comput. Appl. **3**, 28–32 (2010)
9. Bedi, S., Kumar, A., Kapoor, P.: Robust secure SVD based DCT-DWT oriented watermarking technique for image authentication. Int. J. Comput. **17**, 46.1–46.7 (2009)
10. Hernandez, J.R., Amado, M., Perez-Gonzalez, F.: DCT-domain watermarking techniques for still images: detector performance analysis and a new structure. IEEE Trans. Image Process. **9**, 55–68 (2000)
11. Al Baloshi, M., Al-Mualla, M.E.: A DCT-based watermarking technique for image authentication. In: International Conference on Computer Systems and Applications, pp. 754–760. IEEE (2007)
12. Roy, S., Pal, A.K.: A blind DCT based color watermarking algorithm for embedding multiple watermarks. AEU-Int. J. Electron. Commun. **72**, 149–161 (2016)
13. Singh, S., Singh, R., Singh, A.K., Siddiqui, T.J.: SVD-DCT based medical image watermarking in NSCT domain. In: Hassanien, A.E., Elhoseny, M., Kacprzyk, J. (eds.) Quantum Computing: An Environment for Intelligent Large Scale Real Application. SBD, vol. 33, pp. 467–488. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-63639-9_20
14. Zear, A., Singh, A.K., Kumar, P.: A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimed. Tools Appl. **77**, 4863–4882 (2018)
15. Li, Y.-L., Li, J.-P., Ren, Q.-B.: Based on chaotic encryption and SVD digital image watermarking. In: International Conference on Apperceiving Computing and Intelligence Analysis Proceeding, pp. 285–289. IEEE (2010)
16. Al-Afandy, K.A., Faragallah, O.S., El-Rabaie, E.-S.M., El-Samie, F.E.A., Elmhalawy, A.: A hybrid scheme for robust color image watermarking using DSWT in DCT domain. In: IEEE International Colloquium on Information Science and Technology, pp. 444–449. IEEE (2016)
17. Al-Gindy, A., Al-Ahmad, H., Qahwaji, R., Tawfik, A.: A novel blind Image watermarking technique for colour RGB images in the DCT domain using green channel. In: Mosharaka International Conference on Communications, Computers and Applications, pp. 26–31. IEEE (2008)

18. Al-Gindy, A., Al-Ahmad, H., Qahwaji, R., Tawfik, A.: Watermarking of colour images in the DCT domain using Y channel. In: International Conference on Computer Systems and Applications, pp. 1025–1028. IEEE (2009)
19. Kumar, B., Singh, R.K., Singh, A.K.: A noble watermarking scheme based on spatial domain approach with pixel exchange and compressive sensing. SSRN 3350904 (2019)
20. Moosazadeh, M., Ekbatanifard, G.: Robust image watermarking algorithm using DCT coefficients relation in YCoCg-R color space. In: IEEE Conference on Information and Knowledge Technology, pp. 263–267. IEEE (2016)
21. Badran, E.F., Ghobashy, A., El-Shennawy, K.: DCT-based digital image watermarking VIA image segmentation Techniques. In: 4th International Conference on Information and Communications Technology. IEEE (2006)
22. Gupta, G., Joshi, A.M., Sharma, K.: An efficient DCT based image watermarking scheme for protecting distribution rights. In: Eighth International Conference on Contemporary Computing, pp. 70–75. IEEE (2015)
23. Sun, S., Ling, J., Dong, F., Wan, J.: A new general binary image watermarking in DCT domain. In: International Seminar on Future BioMedical Information Engineering, pp. 34–36. IEEE (2008)