DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5747

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

DFT BASED DIGITAL IMAGE WATERMARKING: A SURVEY

Ningombam Jimson
Department of Computer Science,
Assam University, Silchar, Assam, India

K. Hemachandran
Professor, Department of Computer Science,
Assam University, Silchar, India

Abstract: Digital watermarking is a process in which a piece of information is embedded into a digital data. In this article we review the digital watermarking scheme of image which uses DFT to embed the watermark. Digital watermarking using DFT has attracted researchers due to the fact that watermark using DFT are RST invariant compared to other scheme using other transforms such as DCT or DWT. In the presented article, we tried to cover all the aspect of digital watermarking particularly on DFT based scheme. We also gave some terminology used in the digital image watermarking and briefly discuss the attacks involved in digital image watermarking.

Keywords: Digital image watermarking, Discrete Fourier transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), RST (Rotation Scale, Translation) invariant.

I. INTRODUCTION

The rise in the use of computer and the growth of digital network gave rise to the exchange of digital information which can be easily manipulated, copy or shared over a digital network. In order to secure the digital data in the form of audio, video or an image, various technique like cryptography, steganography and digital watermarking are used [1].Digital watermarking is like steganography which involve adding a bit of information to the digital data. The information hidden in a digital watermarking schemes can be a signature for proof of ownership or authenticity of the digital data. Transparency, robustness, and capacity are three main properties of digital image watermarking. Transparency means no visual artifact or no change in the digital data after the addition of the digital watermark, in other word both the watermarked image and original image should be similar in perceptual manner. Robustness means the capacity to detect the watermark after various intentional and unintentional attacks. Some of the common attacks involved in the watermarking are spatial filtering, lossy compression, geometric distortion etc. Lastly capacity is the amount of information that can be added to the digital data. The watermark should hold enough information to provide uniqueness of digital data which is watermarked. [1][2]. In this survey, we concentrate on the digital image watermarking using Discrete Fourier Transform

Generally, digital image watermarking scheme consists of an encoder and decoder. The block diagram of an encoder and decoder is given in Fig. 1 and Fig. 2. [1][2] [3][4].

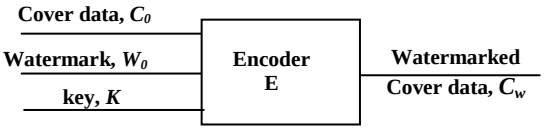

Figure1. Generic watermark encoder

An encoder is an algorithm for embedding the watermark information to a cover work or digital content. In an encoder, the watermark, W_0 (the information to be embedded) cover data C_0, the digital data or content in which the information to be embedded and a secret key K is used as an input. The output of the encoder is a watermarked cover data C_w. On the other hand, a decoder or an extractor is an algorithm or scheme in which the watermark information is decoded or extracted from the watermarked cover data. In a decoder, the watermarked data C_w, from which the information is to be extracted or decoded, the secret key K, which was used in the watermark encoding and the cover work C_0, are taken as inputs.

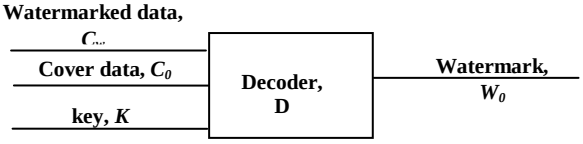

Figure 2. Generic watermark decoder

A digital watermark can be added at the pixel level i.e.spatial domain and in frequency domaini.e. the transform domain [1], [2], [3]. In the spatial domain, the watermark is added by modifying the pixel value of the original image. The main advantage watermarking in the spatial domain is they are low cost, low complexity, low system requirement and the main disadvantage is that they are not robust. In transform domain, the image are transform using some reversible transform like Discrete Cosine, Discrete Wavelet or Discrete Fourier transforms and corresponding transform coefficient are altered to add the watermark information. Each of this transformation has its own advantage and disadvantages e.g. DCT based watermarking are robust against compression and DWT image watermark can make use of the characteristic of Human Visual System (HVS) and in term of computational complexity, watermarking using DWT is higher than that of DCT. The advantage of DFT over other transform is that, watermarking scheme using DFT are rotation, scaling and translation invariant and hence the watermark can be decoded from the images which

have gone through geometric distortion unlike DCT and DWT in which it is difficult to overcome [3]. In the presented paper we mainly focus on the watermarking scheme utilizing DFT. The paper is organized into following sections in II we describe a brief details about the attacks on the digital image watermarking scheme, in III we describe some of the terminology used in digital watermarking and theoretical background of DFT is given in section IV and in section V we present the literature survey of the watermarking scheme using DFT.

II. ATTACKS ON DIGITAL IMAGE WATERMARKING

Attacks on the digital watermarking scheme can be defined as a process or manipulation for removing the watermark from the watermarked digital image. On the other hand, digital image watermarking scheme should be robust enough to withstand any kinds of attacks on a watermarked image and can be considered as the only goal of digital image watermarking. In order to develop a robust watermarked image one need to study about the attacks. Generally, attacks on the digital watermarking scheme can be categories into four as mentioned below [8], [9]:

A. Removal Attacks:

The main goal of this types of attacks is to completely removed watermark without key used in the watermark embedding. Some of the attacks included in this category are denoising, quantization (e.g. for compression), remodulation, and collusion attacks. The mentioned attacks don't succeedcompletely in removing the watermark from the watermarked image, but significantly affects the watermark. For performing a collusion attacks many copies of the watermarked image (each signed with a key) are obtained by the attacker and removal of the watermark is performed by averaging all the copies or a little part from each of the copies. In removal attack, one tries the optimized operation like denoising, quantization etc. to alter the watermark embedded without damaging the quality of the watermarked image.

B. Protocol Attacks

These types of attack create ambiguity of the watermarked data by attacking the entire concept of the watermark scheme. The concept of protocol attack is used in reversible watermarking. In this attack, the attacker subtracts its own watermark from the watermarked data and claim the ownership thus creating ambiguity with respect to the true ownership of data. The solution to this type of protocol attacks is to use one-way function to make the watermark signal dependent. Copy attack is another type of protocol attacks in which attacker estimate the watermark from the watermarked data and put it into some other digital data which is known as target data. The copy attacks can be term as successful if and only if it a valid watermark can be retrieved from the target without the knowledge of the watermarking key.

C. Geometric attacks

Geometric attacks distort the watermark which can render for all objectives and purposes of any watermarking application useless. This type of attack includes the image processing manipulation such as scaling, translation, and rotation. In recent trend in digital image watermarking, this type of attacks can be overcome by using transform invariant domain like Fourier-Mellin transform or making used of an additional template or specially designed watermark using auto-covariance function (ACF).

D. Cryptographic Attacks

The main intention of these type of watermarking attack is to understand the security measure taken while embedding the watermark in the digital image and finding out a process to remove or insert another misleading watermark. Brute Force attacks and oracle attack are the examples of cryptographic attacks. These types of attacks have high computational complexity.

III. TERMINOLOGY

The *embedded data* is the message which that one wants to send secretly, it is usually hidden in what is known as the *cover object*, producing a *stego object*. In order torestrict detection or recovery of the embedded data one uses a *stego key* during the embedding process. In the article regarding digital watermarking, the stego object is known as *watermarked data*.

In the light of purpose, a watermark can be fragile and robust. *Fragile watermarked* data are those in which the watermark is destroyed as soon as the cover object goes some change or modification. The purpose of this type of watermark is to know that the digital data has been changed or tampered with. Likewise in a *robust watermark*, the watermark is difficult or impossible to remove or separate from the watermarked data [4], [5]. This type of watermark is mainly used for copyright protection. On the basis of how the watermark is detected or recover one can classify watermark in a *blind* and *non-blind watermark*. A blind watermark can be detected without the information of the un-watermarked original data. Whereas in case of a non-blind watermark, for detection or extraction the original un-watermarked data or some information regarding the original data is required.

According to human perception, watermark can be classified into the visible and invisible watermark. *Visible watermark*s, as the name implies can be define in which the embedded watermark is perceptible along with the cover data in which it is embedded, these types of watermark can be easily perceptible or recognized easily by a human observer. In case of *invisible watermark*, the watermarks are added to the cover object in such a way that changes made to the pixels are not perceivable to a normal human observer and can only be decoded by using appropriate decoding algorithm[1] [2], [3], [4], [5]. Then there is dual watermark which is the combination of both visible and invisible watermark. A digital watermark can a private and public based on the permission given at the detection. In private watermark, only authorize person can detect the watermark and it is impossible for any unauthorized person to extract the watermark unlike public watermarking. A digital image watermark can be a source based in which a distinct watermark is added to the digital image to identify its owner and destination based in which different watermark are added while distributing the digital image and its main purpose is to identify the buyer in case of illegal redistribution[4].

IV. DISCRETE FOURIER TRANSFORM (DFT)

Mathematically, an image can be represented in the Cartesian grid as f(x, y) for $0 \le x \le M$ and $0 \le y \le N$, where M

and N are the dimensions of the image, then 2D DFT F(u, v) can be defined as [10]:

$$F(u,v) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} \quad (1)$$

The exponential term is the basis function corresponding to each point *F (u, v)* in the Fourier space. The above equation can be interpreted as *F (u, v)* is obtained by multiplying the spatial image with the corresponding basis function and summing up the result obtained. The basis function is the sine and cosine function. The inverse Fourier Transform is given by:

$$f(x,y) = \frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v)e^{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} \quad (2)$$

The output of a Fourier transform is complex number valued image which can be displayed using the real and imaginary part i.e. the magnitude and phase of the image which is given by

Magnitude M (u, v) = $\left|\, F(u, v) \,\right|$

Phase $\Phi(u, v) = \angle F(u, v)$

Both magnitude and phase hold some information regarding the image which has gone through DFT. The magnitude contains less information as compare to a phase of DFT making the phase more important than a magnitude of the DFT. The following figure demonstrates the same, here we took a grey image of Lena and Pepper, DFT is performed in both the images to get the respective magnitude and phase and we interchange the magnitude and phase of the two images to obtain a new image entirely.

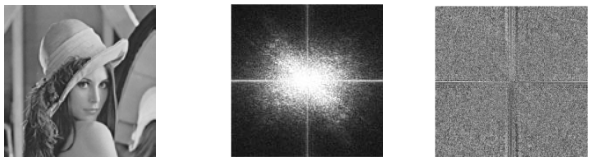

Figure4.Lena image and the corresponding magnitude and phase respectively.

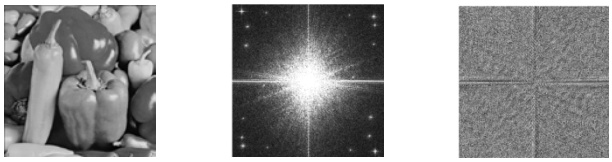

Figure 5.Pepper image and its corresponding DFT Magnitude and phase respectively

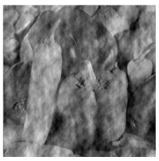

Figure6. Reconstructed image using the magnitude of Lena Image combine with the phase of Pepper image

Figure7.Reconstructed image using the magnitude of Pepper Image combine with the phase of Lena image

V. LITERATURE SURVEY

In 1998 Ruanaidh and Pun [10] introduced a watermarking scheme by exploiting the properties of Fourier Transform, in their scheme, watermarking were perform on the RST invariant domain which was achieved by using Fourier transform and Log-polar mapping (LPM). In their scheme the image is transformed using DFT and performing log-polar mapping on the magnitude of the DFT, they got the RST invariant domain in which the watermark is embedded. The watermark is embedded into the amplitude using spread spectrum modulation. The used of log-polar map cause severe damage to the image quality and watermark data. To overcome this, Ruanaidh and Pun proposed another scheme so that the original image is not hampered by LPM or ILPM so they decide to embed the watermark in RST invariant domain independently of the original image. In this scheme, they used the phase of the DFT to embed the watermark. They apply Fourier Mellin transform (FMT) to the watermark signal and DFT to the original image. Using the result obtained from the FMT and phase obtained from DFT of the original image they perform inverse DFT and this results is then added to the original image to get the watermark image. For watermark detection, they compute the difference between the original and watermarked image and DFT is perform to get the magnitude and FMT is performed to the resultant magnitude to get the RST invariant domain and from which watermark is detected. Kim et al. [11] proposed a watermarking scheme using invariant centroid and FMT. Unlike Ruanaidh and Pun in which they apply LPM to the frequency domain, they applied LPM in the spatial domain. They first calculated invariant centroid on the origin of LPM, to make the scheme invariance against scaling and translation. Rotation of image results in the cyclic shift in the LPM domain, so the magnitude spectrum of 2D DFT on LPM of an image is rotation invariant. Lin et al [12] proposed a scheme which was robust against RST attack. In order to achieve the robustness against RST attack, they exploit the translation invariant of DFT magnitude and LPM. In this scheme, the watermark is embedded along the log-radius axis computed by mapping the magnitude of DFT to the log-polar coordinate. The method lack robustness toward cropping and only favor the application in which the watermark is only to be detected and not decoded. Solachidis and Pitas [13], proposed blind watermarking scheme using DFT. The watermark was created using a pseudo-random sequence key and have the value of {1, -1}, the watermark form a ring of given width around mid-frequency region of the DFT magnitude. They used correlation for watermark detection correlation. In this scheme, the watermark was embedded in the mid-level frequencies because if they found out that if the watermark is embedded in the low-level frequencies then watermark invisibility was not achieved and if it is embedded in the higher frequencies then the watermark was not robust against compression.Peireira et al [14] proposed a scheme using the concept of a template which contains no information on itself. In this scheme, the watermark consists of two-part a spread spectrum signal and a template. The watermark signal is embedded using DFT along with a template. The purpose of the template is to understand the geometrical transform undergone by the watermarked image and to enable synchronization of the watermark. The main

advantage of template-based approach is the ability to address synchronization of a general affine transform for watermark detection. The main disadvantage of this that attacks have been developed to erase the template presence.Lick and Jordan [15] proposed a scheme in which a spread spectrum watermark is embedded in the DFT. In this scheme, the spread spectrum watermark is embedded along the circle centered on the zero frequency component of DFT magnitude. The presence of the watermark was found out using the correlation between the watermark and watermark image. Kang et al [16] proposed a template based watermarking scheme using both DWT and DFT. In their scheme, the watermark is embedded in the coefficient of the LL band of the DWT domain and a template in the middle-frequency component in the DFT domain in order to achieve robustness against JPEG compression and affine transform. The scheme was not robust against some common image processing attacks.Ganic et al [17] in their scheme, they embed multiple watermark using DFT. Circular watermarks is embedded in the low and high- frequency band and found out that the watermark embedded in high-frequency component is robust to rotation, cropping and if the watermark in low-frequency band is robust to JPEG compression, low pass filter etc. In addition, embedding the watermark in the low and high-frequency band can also resist attacks such as histogram equalization, contrast adjustment. Kusyk and Eskicioglu[18] proposed a watermarking in DFT domain which involve modifying multiple frequency bands to protect watermark from a wide range of attacks. The watermark was embedded three frequency band viz. low, high and mid. The proposed scheme was implemented on several cover image to test robustness and undergone a range of attacks and they found out that for a given range of attacks, the watermark extracted from low-frequency band have good visual quality for low pass filter, Gaussian Noise addition, JPEG compression, rotation, resizing and scaling whereas watermark extracted from high frequency was found robust against cropping, intensity adjustment histogram equalization, gamma correction. Chiu and Tsai [19] proposed a DFT based color watermarking scheme by coding and synchronization of coefficient peak value location in DFT domain. They embed watermark which circularly and symmetrically in the middle frequency by utilizing the combinational code to locate the peak and supplementary synchronization peak location. In extraction process in order to obtain the watermark first the position of the peak coefficient value are located and mapped into combinational operation. The embedded watermark was robust against print and scan operation. The performance of the scheme was not good as it don't consider human visual system. Content-based adaptive watermarking scheme which was embedded in the DFT domain is proposed by Xiajun and Ji[20]. In their scheme to extract feature point they used Harris corner detection this pointsis geometrically insignificant and therefore are capable of determining the de-synchronization attack by utilizing Delaunay-tessellation based triangle matching algorithm. However the presented scheme was not robust against flip rotation. They used both error correcting code and spread spectrum for detection accuracy. Polijcak et al [21] proposed a watermarking scheme where the watermark is embedded in the magnitude of the DFT using optimal radius and phase of the DFT is left untouched. In their scheme the watermark is sequence which have zero mean value and unit variance. In case of color image the luminance image is watermarked and other two chromatic component are unmodified. Ridzon and Levicky[22] proposed a scheme in which a watermark having circle symmetry which was form using LPM. In watermarking embedding, component of the peak Fourier spectrum of the cover image with value 1 are changed over by averaging over neighborhood 3×3 with an increase by the coefficient of amplification.Riad et al [23] proposed a scheme exploiting the concept of optimal radius as in Poljicakscheme [18] by embedding the watermarking in the magnitude of the Fourier transform and in watermark detection process, the watermarked image is preprocessed and presence of the watermark is detected using correlation between the optimal radius amplitude and watermark.

VI. CONCLUSION

In this survey, we gave an overview of watermarking using DFT and different kind of attacks on digital image watermarking. We presented a brief theoretical background of the DFT and some common terminology used in digital image watermarking. In our work, we tried to cover the details of the watermarking algorithm based on DFT. The DFT based watermarking scheme is invariant to RST attack in compared to other transform domain watermarking like DCT, DWT. DFT based image watermark scheme can be classified into template based approach, circular embedding using some radii.

VII. REFERENCES

[1]. Cox, I., Miller, M., Bloom, J., Fridrich, J., &Kalker, T. (2007). Digital watermarking and steganography. Morgan Kaufmann.

[2]. Arnold, M., Schmucker, M., &Wolthusen, S. D. (2002). Techniques and applications of digital watermarking and content protection. Artech House.

[3]. Potdar, V. M., Han, S., & Chang, E. (2005, August). A survey of digital image watermarking techniques. In Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on (pp. 709-716). IEEE.

[4]. Mohanty, S. P. (1999). Digital watermarking: A tutorial review. URL: http://www. csee. usf. edu/~ smohanty/research/Reports/WMSurvey1999Mohanty. pdf.

[5]. Chandramouli, R., Memon, N., &Rabbani, M. (2002). Digital watermarking. Encyclopedia of Imaging Science and Technology.

[6]. Mohanty, S. P., Sengupta, A., Guturu, P., &Kougianos, E. Everything You Want to Know About Watermarking.

[7]. Yu, B., & Jain, R. (2011). A Quick Glance at Digital Watermarking. In HTTP://WWW. CSE. WUSTL. EDU/~ JAIN/INDEX. HTML.

[8]. Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J. J., & Su, J. K. (2001). Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. IEEE communications Magazine, 39(8), 118-126.

[9]. Song, C., Sudirman, S., Merabti, M., & Llewellyn-Jones, D. (2010, January). Analysis of digital image watermark attacks. In Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE (pp. 1-5). IEEE.

[10]. Ruanaidh, J. J. O., & Pun, T. (1998). Rotation, scale and translation invariant spread spectrum digital image watermarking. Signal processing, 66(3), 303-317.

[11]. Kim, B. S., Choi, J. G., & Park, K. H. (2003, October). RST-resistant image watermarking using invariant centroid and reordered Fourier-Mellin transform. In International Workshop on Digital Watermarking (pp. 370-381). Springer, Berlin, Heidelberg.

[12]. Lin, C. Y., Wu, M., Bloom, J. A., Cox, I. J., Miller, M. L., &Lui, Y. M. (2001). Rotation, scale, and translation resilient watermarking for images. IEEE Transactions on image processing, 10(5), 767-782.

[13]. Solachidis, V., & Pitas, L. (2001). Circularly symmetric watermark embedding in 2-D DFT domain. IEEE transactions on image processing, 10(11), 1741-1753.

[14]. Pereira, S., Ruanaidh, J. J., Deguillaume, F., Csurka, G., & Pun, T. (1999, July). Template based recovery of Fourier-based watermarks using log-polar and log-log maps. In Multimedia Computing and Systems, 1999. IEEE International Conference on (Vol. 1, pp. 870-874). IEEE.

[15]. Licks, V., &Hordan, R. (2000). On digital image watermarking robust to geometric transformations. In Image Processing, 2000. Proceedings. 2000 International Conference on (Vol. 3, pp. 690-693). IEEE.

[16]. Kang, X., Huang, J., Shi, Y. Q., & Lin, Y. (2003). A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression. IEEE transactions on circuits and systems for video technology, 13(8), 776-786.

[17]. Ganic, E., &Eskicioglu, A. M. (2004). A DFT-based semi-blind multiple watermarking scheme for images. CUNY Brooklyn College, 2900.

[18]. Kusyk, J., &Eskicioglu, A. M. (2005, October). A semi-blind logo watermarking scheme for color images by comparison and modification of DFT coefficients. In Multimedia Systems and Applications VIII (Vol. 6015, p. 60150C). International Society for Optics and Photonics.

[19]. Chiu, Y. C., & Tsai, W. H. (2004). Copyright protection by watermarking for color images against rotation and scaling attacks using peak detection and synchronization in discrete Fourier transform domain. In Proceedings of Third Workshop on Digital Archives Technologies (pp. 207-213).

[20]. Qi, X., & Qi, J. (2007). A robust content-based digital image watermarking scheme. Signal processing, 87(6), 1264-1280.

[21]. Poljicak, A., Mandic, L., &Agic, D. (2011). Discrete Fourier transform-based watermarking method with an optimal implementation radius. Journal of Electronic Imaging, 20(3), 033008.

[22]. Ridzon, R., &Levicky, D. (2008, September). Robust digital watermarking in DFT and LPM domain. In ELMAR, 2008. 50th International Symposium (Vol. 2, pp. 651-654). IEEE.

[23]. Riad, R., Harba, R., Douzi, H., Ros, F., &Elhajji, M. (2016). Robust Fourier watermarking for id images on smart card plastic supports. Advances In Electrical and Computer Engineering, 16(4), 23-30.