manuscript receive 10 November 2021
revised: 15 December 2021
accepted: 21 January 2022

A Review study on Digital Image Watermarking Techniques

Razieh Keshavarzian
Department of Electrical Engineering, Heris Branch, Islamic Azad University, Heris, Iran.
Email: ra.keshavarzian@iau.ac.ir

Abstract Digital watermarking has been an effective technique for copy protection, copyright protection, medical application, data authentication, fingerprinting and other applications over recent years. In this technique, certain information called watermark is embedded inside the original data. The main data can be an image, video, audio and text. Requirements of a watermarking system will be different depending on the type of the host media and for what purpose it is used. In this article, a study on digital image watermarking is presented. In the study, general concepts of watermarking, different types of digital image watermarking, and the watermark embedding and extraction techniques are discussed in brief.

Keywords Copyright protection, Digital image watermarking, Robustness, Watermark embedding

1. Introduction

The recent growth of the digital multimedia technology and the internet usage allow users to copy, transmit, distribute and store information more easily. This advantage makes challenging the issue of how to protect the copyright [1]. The copyright protection includes the authentication of an object (text, image and video) ownership, and the identification of its illegal copies. Techniques are needed to prevent copying, fake and unauthorized distribution of images and videos [2]. Digital watermarking is an effective technique to protect the copyright of digital media [1]. In this technique, certain information called watermark is hidden inside the original data. At any time, the hidden information can be extracted and used to prove ownership, to authenticate data, or to obtain some information related to copyright [3]. In the case of digital images, watermarking consists of signing an image with a signature or message in such a way that the message is hidden in the image and there is no visible difference between the original and the signed images [4, 5]. In general, the watermarking technique consists of embedding a hidden signal called watermark inside the original data [6]. It should be noted that hiding information in the image may degrade its quality. Therefore, one of the important goals of the watermarking techniques is to minimize the quality degradation [7]. In other words, these techniques try to embed information in the image in such a way that there is a minimum visible difference between the original image and the watermarked image [4]. On the other hand, in order to make the watermark resistant against various attacks, the amount of embedded information should be increased. Meanwhile, as the amount of information embedded in the image increases,

its quality decreases. Therefore, it should be establish the balance between the robustness and the imperceptibility of the watermark.
The rest of the paper is organized as follows: In section 2, different types of image watermarking are presented. In section 3, embedding and extracting processes of image watermarking are explained. In section 4, some of the image watermarking algorithms are reviewed. Finally, the conclusions are provided in section 5.

2. Types of Image Watermarking

A digital watermark is a set of secondary information embedded into an original image [7]. This information is embedded in the image in such a way that it is hidden from everyone's view or visible to everyone. From this point of view, watermarking is divided into two types: visible and invisible [8].

Visible: the properties and requirements of a visible watermark can be stated as follows [7]:

- A visible watermark should be visible on both color and grayscale images. This requires that the watermarking technique be used only for the luminance of the pixels of the image. In addition, the watermark should cover a large area of the image and be visible in almost all parts of the covered area.
- The watermark should be visible, but the details of the image below it should not be too obscure.
- Removing the watermark should be difficult. As much as possible, removing the watermark should be more expensive than buying the image usage right.
- Embedding the watermark should be easy.

Figure (1) shows an example of visible watermarking.

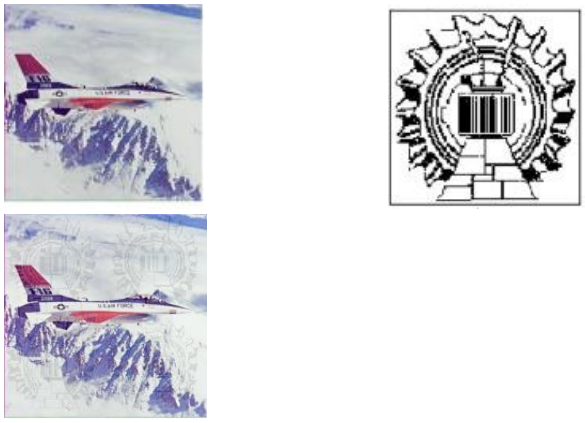

Fig.1.An example of visible watermarking [9]

Invisible: in contrast with visible watermarking, in invisible watermarking, information is embedded inside the original image without creating perceptible distortions [7]. Invisible watermarking itself is divided into three types: robust, fragile and semi-fragile.

Robust watermarking

In this type of watermarking, the watermark is robust to common image processing operations or attacks such as compression, filtering, analog to digital conversions and vice versa, cropping and etc. Most of these attacks, such as compression, often affect the less important parts of the image. So in order to be resistant to such attacks, the watermark must be embedded in the important parts of the image [6]. In general, in order to maintain the robustness of the watermark against various attacks, more information should be embedded in the image. On the other hand, as the amount of information embedded in the image increases, its quality decreases. In other words, the robustness and invisibility of the watermark act in conflict with each other [8]. One way to balance them is to use the Human Visual System (HVS) specification. In this method, the amount of embedded information depends on the characteristics of the original image; until the maximum-possible

imperceptibility of the watermark is guaranteed [1].

The properties and requirements of a robust invisible watermark are as follows:

- Robustness: A watermarking system should be resist to various attacks. Even after intentional or unintentional attacks on the watermarked image, the watermark should be detectable. In order to achieve high resistance of the image, the watermark should be embedded in the important parts of the image.
- Perceptible transparency: The watermarking algorithm should embed the watermark in the image in such a way that it does not cause a defect in the quality of the original image. In other words, the watermark must be hidden inside the image. But watermark invisibility may conflict with other requirements such as robustness. Sometimes it is necessary to use human vision system when embedding watermark. In this case, the amount of embedded information depends on the characteristics of the original image, so that the invisibility of the watermark is largely guaranteed. Also, the watermark should be statistically invisible. This means that an unauthorized person cannot obtain the watermark using statistical methods.
- Security: If an unauthorized person cannot reveal and remove the watermark using watermarking algorithms, this watermarking will be secure. In other words, the places where the watermark is embedded and the changes caused by embedding are unknown to people who do not know the secret key [1].

Fragile watermarking

Fragile watermarking is sensitive to changes. Any changes in the original image will change or lose the embedded watermark. Therefore, this method can be useful to prove the authenticity of an image. For example, if the watermark embedded in an image is altered, the image tampering is proven [7]. In fragile watermarking, more information can be embedded. In other words, this type of watermarking has a high embedding capacity. A fragile watermark should have the following properties [7]:

- The watermark should be easily modified by altering the pixel values of the image. In other words, the watermark extracted from the modified image is different from the original watermark, and the difference can be a proof of altering the pixels of the image.
- The watermark should be secure. This means that it is impossible to recover the changes or reproduce the watermark after the image has been altered, even when the watermarking procedure or the watermark itself is known.

Semi-fragile watermarking

Like fragile watermarking, semi-fragile watermarking is used to prove the authenticity of an image. The semi-fragile watermarking combine the advantages both the robust watermarking and fragile watermarking. A semi-fragile watermarking should have the following property [10]:

- The watermark should make a balance between robustness and fragility. On the one hand, after malicious tampering, such as collage attach, watermark should be modified to show its fragility; on the other hand, after reasonable image processing operations, such as JPEG compression, filtering, and so on, the watermark should be accept them to show its robustness.

In summary, different types of watermarking techniques from the point of perceptibility are shown in Fig. 2.

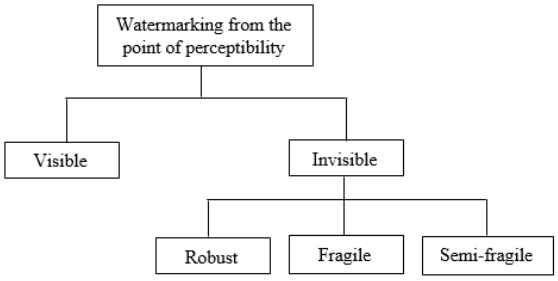

Fig.2.Types of watermarking according to perceptibility.

According to the domain in which the watermark will be embedded, the watermarking techniques are categorized into spatial and transform domain techniques.

Spatial domain watermarking

In these techniques, the watermark is embedded by directly changing the pixel values of the original image. These techniques often fail with signal processing attacks such as filtering and compression, yet their algorithms are easy to implement. Embedding the watermark in the least significant bit (LSB) of the original image is one of the spatial domain watermarking methods. In this method, the least significant bit of the image is replaced with the watermark information. The major disadvantage of spatial domain watermarking is the lack of robustness against the image cropping attack, which may result in the watermark removal [11].

Transform domain watermarking

In these techniques, in order to embed the watermark, the original image is first transferred into the transform domain, and then the transform coefficients are altered. The common transform domains are discrete wavelet transform (DWT), discrete cosine transform (DCT), discrete Fourier transform (DFT) and singular value decomposition (SVD). The transform domain watermarking is more robust than spatial domain watermarking against various attacks, because the watermark information can be spread over the entire image [12]. Among the transform domain methods, wavelet based methods are more popular and effective due to their excellent frequency localization properties.

In the transform domain watermarking, if the goal is robust embedding, embedding in high-frequency coefficients that have a small value and are affected by various processes such as compression should be omitted. On the other hand, the human eyes are more sensitive to changes in low frequencies, so less information should be embedded in these coefficients to prevent the image quality degradation. Therefore, these types of watermarking have a low embedding capacity.

Watermarking in DCT domain: In DCT domain, the coefficients for watermark embedding are selected in such a way that the two requirements of invisibility and robustness of the watermark are satisfied. The selected coefficients should have the following characteristics:

- They should have a high capacity so that the watermark can be embedded in them without visual distortion. This satisfies the requirement of watermark invisibility.
- They should alter less with the image processing and noise addition. As a result, the watermark embedded in these coefficients will be robust to various attacks.

As it was said, the human eyes are more sensitive to changes in low frequencies (smooth areas), so less information should be embedded in these coefficients so that the quality of the image does not degrade. On the other hand, the watermark embedded in higher frequency coefficients may be lost during quantization in lossy compression. Therefore, the watermark embedding is done in the middle frequency coefficients of the image so that the embedded watermark be invisible and can support lossy compression.

Watermarking in Wavelet Domain: The human eyes are not sensitive to the small changes in edges and textures of the image. On the other hand, it is very sensitive to small changes in the smooth parts of the image [4]. By using the discrete wavelet transform, the edge and texture parts of the image are well exploited in high frequency bands. The large coefficients in these bands define the edges of an image. As a result, adding a watermark to these large coefficients will not be visible to the viewer, even if it results in a loss of quality. This is one of the advantages of discrete wavelet transform. Another advantage of DWT is that it is compatible with image and video compression standards such as JPEG2000 and MPEG4 [4].

3. Image Watermarking Procedure

The image watermarking procedure is described as two main stages: watermark embedding and watermark extraction. Figures 3 and 4 show the embedding and extracting process of digital image watermarking.

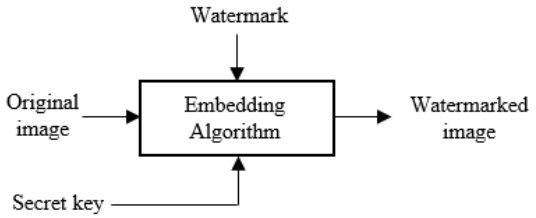

Figure 1. Embedding process of digital image watermarking.

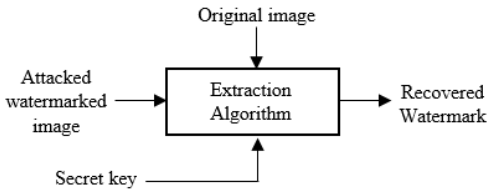

Fig.3. Extracting process of digital image watermarking.

3-1 Watermark Embedding

In the embedding stage, the watermark is imbedded into the original image by applying a certain algorithm, a secret key and spatial or transform domain techniques to generate the watermarked image. The secret key should be known at the watermark extraction process.

3-2 Watermark Extraction

The extraction process is the inverse of the embedding process in which the watermark can be extracted from the distorted watermarked image using a certain algorithm and the secret key. Watermark extraction methods can be divided into two categories: blind and non-blind. In blind watermarking, watermark extraction algorithms do not have access to the original image. This makes the watermark extraction difficult. While in non-blind watermarking, watermark extraction algorithms need the original image in order to extract the watermark. When the original image is available, the watermark extraction becomes easier. Because by subtracting the watermarked image from the original image,

changes can be made on the obtained distortion and so the embedded watermark can be extracted. According to the different applications, one of the two kinds of extraction method is used. For example, in data authentication, the original image is not used in the extraction process. In other applications such as copy protection, watermark extraction algorithms do not have access to the original image. In some cases, it is impossible to use the original image due to its large size. In applications such as copyright protection, watermark extraction algorithms can use the original image. Blind watermarking algorithms are often less resistant to various types of attacks than non-blind watermarking.

4. Related works

In this section, some robust image watermarking techniques for copyright protection are reviewed. Dote et al. [13] proposed a wavelet based watermarking scheme in which a visual watermark embedded into wavelet coefficients of the original image. In this method, 5-level DWT and 1-level DWT were applied to the host image and the watermark, respectively. Then, transformed watermark coefficients were embedded into those of the host image at each resolution level with a secret key. Kang et al. [14] proposed a blind DWT-DFT composite image watermarking scheme in which a key based sequence is embedded in the coefficients of the *LL* sub band in the DWT domain. Lin et al. [19] proposed a blind watermarking algorithm based on maximum wavelet coefficient quantization in which a binary watermark is embedded into DWT coefficients of host image. Although this scheme performs well against some attacks, it is not robust enough against geometric attacks such as cropping. Bhatnagar et al. [20] presented a semi-blind reference watermarking scheme based on DWT and singular value decomposition (SVD). In [21], Lai et al. proposed another hybrid DWT-SVD based watermarking scheme in which the watermark is directly embedded into the singular values of the host image's DWT sub bands. Huang et al. [23] proposed an adaptive watermarking scheme based on morphological Haar wavelet transform (MHWT). The gray watermark image is adaptively embedded into low frequency band of MHWT of host image, combining the characteristic of HVS. In our previous works [19, 20], wavelet domain watermarking algorithms based on region of interest (ROI) and are proposed. In these techniques, the ROI of host image is used as watermark to enhance robustness and imperceptibility. The proposed method in [20] takes advantage of Arnold transform for making the scheme more robust and secure. J. Abraham et al. [21] proposed a new spatial domain based color image watermarking. The watermark information are spread over a region of pixels as implemented by the transform domain techniques. For estimating the most appropriate region within an image block, simple image region detector (SIRD) method is used. This scheme is a non-blind technique and the original image is required at the watermark extraction process. Zhou et al. [22] proposed a secure and robust watermarking scheme based on lifting wavelet transform, discrete cosine transform, discrete fractional angular transform and singular value decomposition. The particle swarm optimization (PSO) algorithm is used to optimize the scaling factors and the parameter of the improved discrete fractional angular transform. In [23], Ernavan et al. proposed a

block-based image watermarking scheme using redundant wavelet transform and singular value decomposition considering human visual system (HVS) characteristics. The blocks which have the lower HVS entropies are selected for embedding the watermark. In order to provide additional security, a binary watermark is scrambled by Arnold transform before embedding the watermark into the host image. In [24], Hsu et al. proposed a blind color image watermarking scheme using extreme pixel adjustment (EPA), multi-bit partly sign-altered mean modulation (MPSAM), mixed modulation (MM). In this scheme, the PSO algorithm is used to optimize the parameters of the scheme. Khare et al. [25] proposed an image watermarking technique based on DWT, SVD and homomorphic transform (HT). In this scheme, first level DWT is performed on the host image and then the HL subband is chosen. The HL subband is decomposed in illumination and reflectance components by HT. The watermark is embedded into singular values of the reflectance component. Before embedding, the watermark is scrambled by Arnold transform to provide additional security.

5. Conclusions

Digital watermarking is a technique in which certain information called watermark is hidden inside the original data. At any time, the hidden information can be extracted and used to prove ownership, to authenticate data, or to obtain some information related to copyright. The original data can be an image, video, audio and text. In this paper, concepts, different types and methods of image watermarking technique are reviewed. According to perceptibility, image watermarking is categorized as visible and invisible. Invisible watermarking itself is categorized as robust, fragile and semi-fragile. Robust watermarking is used for copyright protection. Fragile and semi-fragile watermarking can be useful to prove the authenticity of an image. According to the domain in which the watermark will be embedded, the watermarking techniques are categorized into spatial and transform domain techniques. In this review, these techniques are compared and also some of the image watermarking schemes based on these techniques are studied.

References

[1] H. Qi, D. Zheng and J. Zhao, “Human Visual System Based Adaptive Digital Image Watermarking,” Signal Processing 88, pp. 174-188, July 2007.

[2] A. Kejariwal, “Watermarking,” IEEE Potentials, Oct. /Nov. 2003.

[3] J. Liu and X. He, “A Review Study on Digital Watermarking,” First International Conference on Information and Communication Technologies, (ICICT), pp.337- 341, Aug. 2005.

[4] X. G. Xia, C. G. Boncelet and G. R. Arce, “A Multiresolution Watermark for Digital Images,” ICIP, 1997 International Conference on Image Processing, (ICIP'97), vol. 1, pp. 548-551, 1997.

[5] L. W. Kang and J. J. Leo, “A Survey of Error Resilient Coding Schemes for Image and Video Transmission Based on Data Embedding,” The 2004 IEEE Asia-Pacific Conference on Circuits and Systems, Dec. 2004.

[6] A. K. Gangadaran, “Wavelet-Based Digital Image Watermarking,” M.S. Thesis, Submitted to the college of Graduate Studies, Texas A&M University-Kingsville, Dec. 2003.

[7] M. M. Yeung, F. C. Mintzer, G. W. Braudaway and A. R. Rao, “Digital Watermarking for High-quality Imaging,” IEEE First Workshop on Multimedia Signal Processing, 1997.

[8] M. A. Suhail and M. S. Obaidat, “Digital Watermarking-Based DCT and JPEG Model,”

IEEE Transaction on Instrumentation and Measurement, vol. 52, no. 5, Oct. 2003.

[9] E. F. Navaroo, and et al., "Seam Carving based visible watermarking robust to removal attacks," Journal of King Saud University - Computer and Information Sciences, vol. 34, pp. 4499-4513, 2022.

[10] M. M. Yeung, F. C. Mintzer, G. W. Braudaway and A. R. Rao, "Digital watermarking for high-quality imaging," Proceedings of First Signal Processing Society Workshop on Multimedia Signal Processing, pp. 357-362, 1997.

[11] C. T. Hsu and J. L. Wu, "Hidden Digital Watermarks in Images," IEEE Transaction on Image Processing, vol. 8, no. 1, Jan. 1999.

[12] S. Joo, Y. Suh, J. Shin, and H. Kikuchi, "A New Robust Watermark Embedding into Wavelet DC Components," ETRI Journal, vol. 24, no. 5, Oct. 2002.

[13] Y. Dote, and M.S. Shaikh, "A Robust Watermarking Method for Copyright Protection of Digital Images Using Wavelet Transform," IEEJ Trans. on Electronics, Information and Systems, vol. 122, no. 2, pp. 262-266, Jan. 2003.

[14] X. Kang, J. Huang, Y.Q. Shi, and Y. Lin, "A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression, " IEEE Trans. on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 776-786, 2003.

[15] W.H. Lin, Y.R. Wang, S. J. Horng, T. W. Kao, and Y. A. Pan, "Blind Watermarking Method Using Maximum Wavelet Coefficients Quantization, " Expert Systems with Applications, vol. 36, no. 9, pp. 11509-11516, 2009.

[16] G. Bhatnagar, B. A. Raman, "New Robust Reference Watermarking Scheme Based on DWT-SVD, ". Computer Standards & Interfaces, vol. 31, no. 5, pp. 1002-1013, 2009.

[17] C. C. Lai, and C. C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition, " IEEE Trans. on Instrumentation and Measurement, vol. 59, no. 11, pp. 3060-3063, 2010.

[18] X. Huang, and S. Zhao, "An Adaptive Digital Image Watermarking Algorithm Based on Morphological Haar Wavelet Transform, " In: Int. Conf. on Solid State Devices and Material Science, Physics Procedia, pp. 568-575, 2012.

[19] R. Keshavarzian, "A New ROI and Block Based Watermarking Scheme Using DWT, " In: 20th Iranian Conf. on Electrical Engineering, (ICEE2012), May 15-17, Tehran, Iran, 2012.

[20] R. Keshavarzian, and A. Aghagolzadeh, "ROI based robust and secure image watermarking using DWT and Arnold map, " AEU-International Journal of Electronics and Communications, vol. 70, no. 3, pp. 278–288, 2016.

[21] J. Abraham, V. Paul, "An imperceptible spatial domain color image watermarking scheme," Journal of King Saud University - Computer and Information Sciences, vo. 31, pp. 125-133, 2019.

[22] N.R. Zhou, A.W. Luo, and W.P. Zou, "Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm, " Multimed Tools Appl, vol. 78, pp. 2507–2523, 2019.

[23] F. Ernawan, and M.N. Kabir, "A block-based RDWT-SVD image watermarking method using human visual system characteristics, " Vis Comput, vol. 36, pp. 19–37, 2020.

[24] L.Y. Hsu, and H. T. Hu, "Blind watermarking for color images using EMMQ based on QDFT, " Expert Systems with Applications, vol. 149, 2020.

[25] P. Khare, and V.K. Srivastava, "A reliable and secure image watermarking algorithm using homomorphic transform in DWT domain, " Multidim Syst Sign Process, vol. 32, pp. 131–160, 2021.