Engineering Universe for scientific Research and management
ISSN (Online): 2319-3069
Vol. XIII Issue II
February 2021

A REVIEW ON DIGITAL IMAGE WATERMARKING TECHNIQUES

Ajeet Kumar Singh[1], Neetesh Raghuwanshi[2], Bharti Chourasia [3]
[1,2,3]ECE Department, SRK University, Bhopal, India.
ajeetsingh261@gmail.com[1], Neeteshrkdf2010@gmail.com[2], Bharti.chourasia27@gmail.com[3]

ABSTRACT: Digital image watermarking is a branch of information hiding in which the ownership information will be hidden in the cover image. Performing digital image watermarking, some important issues such as imperceptibility, robustness, capacity and security should be considered. The strength and weakness of each of these issues depends on the watermark algorithm and also the domain in which the watermark has been hidden. In this research we investigate the role of the different domains used in digital image watermarking and categorize them based on the power of the mentioned issues that each domain potentially and innately offers.

Keywords: DWT, DCT, Digital Image Watermarking, SVD

1. INTRODUCTION

The introduction of watermarking and the relevant publications goes back to 1979, but the main interest to this area commenced at 1990 with the growth of the multimedia systems and the necessity of transmitting data over the Internet. Although data digitization provide a lot of advantages for users in all over the world, it is highly and simply possible for the digital data to be manipulated and missing its originality. Digital image watermarking is introduced to care the digital data from illegitimate access and alteration. In this paper, at first the definition and the requirements of the digital image watermarking is described, then a classification of digital image watermarking in accordance with the implemented domain is explained. Afterwards, the advantages and the weak points of each domain is presented to identify the best potential domain for watermark implementation.

1.1 Digital Watermarking

The "watermark" word is taken from the dimly visible marks printed on organizational stationery. Dissimilar to visible watermarks in which the watermark is intended to be perceptible, digital watermarks are planned to be totally invisible. In general, invisible watermarking is designed in digital multimedia communication systems [1, 2]. Digital watermarking is essentially including secret symbols as watermarks embedding in video, image and audio data which is used later for the purposes on copyright detection and authentication verification [3-5]. Additionally, the bits including the watermark have to be spread in the whole of the file, so that they cannot be recognized and manipulated.

The embedding technique must not change the original information perceptually and an extraction algorithm needs the watermark data to be detected [6]. In fact it is a technique in which the original image will be changed in accordance with a watermark image. In order to conceal the data related to the identification of the owner of the original content certain characteristics of the cover image must be altered. Both cover and watermark image have to pass through each one of the watermarking techniques and the watermarked image is obtained as a result [7].

1.2 Watermarking Requirements

The most important requirements for digital watermarking are summarized as below. However, the relative importance of these properties might be changed depends on the application.

1.2.1 Imperceptibility

The perceptual similarity between the watermarked image and the original image is reffered to imperceptibility. It means that no visual or audio effect should be perceived by the end user. The quality of the content should not be degraded by the watermark, although in some applications a little degradation will be acceptable in order to achieve higher robustness or lower expenditure. [8, 9].

1.2.2 Robustness

Even if the algorithmic principle of the watermarking method is public, eliminating the watermark should be impossible. Obviously, the watermark can be removed with adequate knowledge of specific embedding process but it should be robust against a wide range of attacks [10-12].

1.2.3 Capacity

In a watermarking system, a suitable amount of information must be embedded into an image. This embedded amount of information in a watermarked image is called data payload. It means the number of bits encoded with the image and the amount of it must be adequate to make possible the envisioned application [9, 13].

1.2.4 Security

The watermark must resist against attacks which aimed directly to eliminate the embedded information. For an attacker it must not be possible to remove, retrieve or alter the watermark especially without the knowledge of the secret key [14].

2 WATERMARKING CLASSIFICATION ACCORDING TO DOMAIN

Watermarking techniques can be classified into various categories based on different criteria. One of them is the domain in which the watermark is inserted. Generally they are categorized to spatial and transform domain techniques.

2.1 Spatial Domain Techniques

In spatial domain techniques, the pixel values of the cover image will be changed directly by embedding the watermark bits [15, 16]. These techniques are computationally simple, straightforward and fast [17, 18], they are also less complex and can be easily implemented with low cost of operation [19] while there is no need for cover image to be transformed. However, they cannot resist on image processing or other geometric attacks [20].

Table1 indicates a comparison between spatial domains and transform domain watermarking.

Table 1: Comparison of spatial and transform domains

Characteristics	Spatial domain	Transform domain
Capacity	Low	High
Imperceptibility	Yes	Yes
Robustness	No	Yes
Speed	Fast	Slow
Time spending	No	Yes
Cost of operation	Low	High
Simplicity	Yes	No
Security	No	Yes
Computational load	No	Yes

2.2 Transform Domain Techniques

Instead of embedding the watermark to the cover image directly, in transform domain techniques, at first the cover image will be transformed and then the watermark will be embedded to the coefficients of the transformed image [15, 21]. In order to retrieve the original signal, an inverse transform of the modified coefficients needs to be taken. Embedding the watermark in transformed domain proves to be more robust against attacks like JPEG compression [19, 21]. Transform domain based algorithms are usually used in robust watermarking to ensure flexibility of the watermark to common signal processing attacks. The most important reason for using transform domain based embedding is the possibility of choosing only samples of the transform domain watermarked having desired specifications in terms of fidelity and robustness [22].

There are many transform domain watermarking techniques such as discrete cosine transforms (DCT), singular value decomposition (SVD), discrete Fourier transforms (DFT), and discrete wavelet transforms (DWT). The distinction of these methods is to provide

higher imperceptibility and more robustness to image manipulations and common signal processing attacks, but the cost of computation is higher than spatial domain watermarking methods. The mentioned techniques have advantages such as computing speed for watermarking, but they cannot make a balance between imperceptibility and robustness automatically in watermarking [23].

2.2.1 Discrete Fourier Transform (DFT)

Fourier transform is one of the finest and broadly used techniques in image processing. It provides a pure frequency domain analysis but, there is no positioning ability in the space-time domain. So that in any partial time quantum, Fourier transform is unable to offer frequency information. To overcome these deficiencies, DCT and DWT are planned to be replaced with fourier transform; these techniques have a variety of superior characteristics of fourier transform exclusive of its limitations [24].

2.2.2 Discrete Cosine Transform (DCT)

Discrete Cosine Transform converts the time domain signal into the frequency domain signal. The 2-dimensional DCT of a matrix gives the frequency coefficients in form of another matrix. Left top most corner of the matrix represents the lowest frequency coefficients while the right bottom most corner represents the highest frequency coefficients. Using the DCT, an image is divided into pseudo frequency bands, and usually the watermark is inserted into the middle frequency sub bands. Conversely, if the watermark inserted in high frequencies; the watermark is easy to be hidden but, the scheme is less resistant to attacks [19, 21, 25].

2.2.3 Discrete Wavelet Transform (DWT)

Wavelets offer a very good recognition in discontinuity and abrupt transmission on signals. Wavelet transforms is a multipurpose mathematical transform having various applications in different areas. It has become a significant technique in image processing and watermarking thanks to its excellent energy compaction properties. [23, 26, 27].

Since after processing an image by the wavelet transform, most of the information contained in the original image is concentrated into the LL sub band, it is called approximate image. On the other hand the other sub bands contain some details like the edge and textures which will be represented by large coefficients in the high frequency sub-bands. The most vertical detail information corresponding to horizontal edges will be shown in LH. While the horizontal detail information from the vertical edges will be represented by HL. The LL (low pass) sub-band can be further decomposed to another level of decomposition and this process can be continued until the desired level of decomposition determined by the application [26, 28, 32].

In watermark embedding, wavelet domain is a promising domain. Discrete Wavelet Transform is based on small waves of limited duration and various frequencies. The coefficients show the amount of similarity between the signals of the image and the selected wavelet. Big coefficients show the most signal similarities. In this technique at first, cover image is transformed into frequency domain and then its frequency coefficients are modified according to transformed coefficients of the watermark and then a robust watermarked image is obtained. The reconstructed image will be achieved by the inverse discrete wavelet transform (IDWT) [7].

Mathematically points of view, discrete wavelet transform (DWT) of a function f(x) is given by the DWT transform pair:

$$W_{\varphi}(j_0,k) = \frac{1}{\sqrt{M}} \sum_{X} f(x)\varphi_{j0,k}(x). \quad (1)$$

$$W\psi(j,k) = \frac{1}{\sqrt{M}} \sum_{X} f(x)\psi_{j,k}(x) \quad (2)$$
$$\forall j \geq j_0$$

And f(x) is shown as:

$$f(x) = \frac{1}{\sqrt{M}} \sum_{k} W_{\varphi}(j_0,k)\varphi_{j0,k}(x) + \frac{1}{\sqrt{M}} \sum_{j=j0}^{\infty} \sum_{k} W\psi(j,k)\psi_{j,k}(x) \quad (3)$$

Where, f(x), φj0, k(x), and **ψ** j, k(x) are functions of the discrete variable x=0, 1, …, M−1. Normally j0=0 and M is selected as a power of 2 (i.e., M=2j) so the summations are done over x=0, 1, …, M−1, j=0, 1, …, j−1, and k=0, 1, …, 2j−1.

The coefficients defined in Eqs. (1) called as approximation coefficient and the coefficients defined in Eqs. (2) Known as detail coefficients. The one dimensional transform can be easily extended to two dimensional transform. In two dimensions, a two dimensional scaling function, φ(x, y), and two dimensional wavelets, ψH(x,y), ψV(x, y) and ψD(x,y), are necessary. Where each of them is the product of a one dimensional scaling function φ and the consequents wavelet ψ.They measure gray level variations for images along vertical, horizontal and diagonal directions: ψH measures variations along columns, ψV measures variations along rows and ψD measures variations along diagonals. Given two separate dimensional scaling and wavelet functions, the discrete wavelet transform of function f(x, y) of size M×N is defined as:

$$W\varphi(j_0,m,n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y)\varphi_{j0,m,n}(x,y) \quad (4)$$

$$W^{i}_{\psi}(j,m,n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y)\psi^{i}_{j,m,n}(x,y) \quad (5)$$

Where j0 is an arbitrary initial scale and the Wφ (j0, m, n) coefficients identify an approximation of f(x, y) at scale j0. The Wψi (j,m,n) coefficients include horizontal, vertical and diagonal details for scales j≥j0 and i={H,V,D} [33, 34].

2.2.4 Singular Value Decomposition (SVD)

The singular value decomposition, or SVD, is derived from a theorem of linear algebra in which a rectangular matrix A can be analyzed into three matrices of an orthogonal matrix U, a diagonal matrix S and the transpose of an orthogonal matrix V. in this method correlated variables transform into a set of uncorrelated ones in order to expose the various relationships among the original data clearly. A digital image also can be viewed as a matrix of nonnegative scalar entries. Let A be a rectangular image of m x n (m ≥n), then mathematically, according to SVD it can be shown as:

$$A=USV^{T} \quad (6)$$

Where *UUT=Im* and *VVT=In*; the columns of U are ortho-normal eigenvectors of AAT, the columns of V are ortho-normal vectors of ATA and S is a diagonal matrix including the square roots of the eigen values from U or V in descending order. Considering r (r ≤n) is the rank of the matrix A then the elements of the diagonal matrix S can be satisfied with the relation (7) and the matrix A can be written as (8):

$$\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r \geq \sigma_{r+1} = \sigma_{r+2} \ldots = \sigma_n = 0 \quad (7)$$

$$A = \sum_{k=1}^{r} \sigma_k u_k v_k^{T} \quad (8)$$

Where uk and vk are the kth eigenvector of U and V and sk is the kth singular value. The reason that these schemes have high robustness is due to the fact that in the SVD subspace, the singular values can preserve the significant amount of the watermark which is provided by the owner and from the protected image it can not be extracted [26].

Using singular value decomposition, some advantages will bring to digital image watermarking techniques. Firstly, SVD transformation can be shown by a rectangle or a square because in which the size of memory is not fixed. Secondly, SVD helps to increase accuracy and decrease the memory constraints. Thirdly, the bigger singular values in SVD keep most energy of an image and also resist against attacks. Therefore if general image watermark is executed, singular values are less affected and this property reinforces the robustness of the inserted watermark. Finally, singular value decomposition follows by algebraic properties and the small changes in the singular values would not perceptually influence on an image, so the image would approximately remain the same even after inserting the watermark. Each singular value in a SVD matrix specifies the luminance of an image layer while the subsequent pair of singular vectors identifies the geometry of the image layer [27-28].
Table 2 refers to the pros and cons of each transform technique mentioned above.

Table 2: Comparison of transform domain techniques.

Technique	Advantages	Disadvantages

DWT	• Excellent spatial localization • Frequency spread (multi resolution) • Excellent time frequency analysis (DWT captures both frequency & location information) • Good energy compaction • Good for signal processing attacks • Compatible with jpeg 2000 for compaction	• Computation complexity • Less robustness against geometric attacks
DFT	• Good resistant against scaling and rotation attacks	• Not robust to some geometric attacks like cropping &shearing • Loss of time frequency analysis tends to difficulty in processing (just frequency information) • Not compatible with standard image compression techniques (jpeg, jpeg2000)
DCT	• Good imperceptibility • Compatible with jpeg compression standard (fast &suitable) • Easier computation compared with DFT (regarding the real numbers instead of complex part) • Reasonable complexity (execution time)	• Block effect (higher compression ratio makes the blocks visible) • Effect of picture cropping
SVD	• Good resistance against geometric and signal processing attacks (high robustness) • High energy compaction • Low computation cost	• False positive problem • Rising computation expenses in case of using lonely

3 CONCLUSION AND FUTURE WORKS

In this paper, the most prevalent watermarking techniques have been described. DWT can be regarded as a high-quality technique among the other techniques because of offering multi resolution characteristics and excellent time frequency analysis. However, the performance of each technique is different according to the usage and robustness of watermark against particular groups of attacks. On the other hand, combination of the mentioned techniques can compensate the drawbacks of each of them lonely. Future work is to combine the mentioned techniques in order to investigate the performance of the characteristics that each combination offers to increase robustness of watermark.

REFERENCES

[1] S. Rohith and K. Bhat, "A Simple Robust Digital Image Watermarking against Salt and Pepper Noise using EURASIP Journal on Advances in Signal Processing, vol. 2012, pp. 1-17, 2012.

[2] S. Deng, et al., "A Robust Triple Digital Watermarking Algorithm Based on Image Blocking," International Journal of Nonlinear Sciences and Numerical Simulation, vol. 10, pp. 727-733, Jun 2009.

[3] H. Shojanazeri, et al., "Video Watermarking Techniques for Copyright protection and Content Authentication," International Journal of Computer Information Systems and Industrial Management Applications, vol. 5, pp. 652-660, 2013.

[4] N. Chandrakar and J. Bagga, "Performance Comparison of Digital Image Watermarking Techniques: A Survey," International Journal of Computer Applications Technology and Research, vol. 2, pp. 126- 130, 2013.

[5] N. Rawat and R. Manchanda, "Review of Methodologies and Techniques for Digital Watermarking," 2014.

[6] M. Abbasfard, "Digital image watermarking robustness: A comparative study," Delft University of Technologyrertre, 2009: 74 pages, 2009.

[7] N. Bisla and P. Chaudhary, "Comparative Study of DWT and DWT-SVD Image Watermarking Techniques," International Journal, vol. 3, 2013.

[8] E. Hussein and M. A. Belal, "Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey," International Journal of Engineering, vol. 1, 2012.

[9] M. A. Akhaee and F. Marvasti, "A Survey on Digital Data Hiding Schemes: Principals, Algorithms, and Applications," The ISC International Journal of Information Security, vol. 5, p. 5, 2013.

[10] A. A. Hood and N. Janwe, "Robust Video Watermarking Techniques and Attacks on Watermark–A Review," International Journal of Computer Trends and Technology-volume4Issue1, 2013.

[11] Y. Liu, et al., "Novel robust multiple watermarking against regional attacks of digital images," Multimedia Tools and Applications, pp. 1-23, 2014.

[12] G. Gupta and J. Pieprzyk, "Database relation watermarking resilient against secondary watermarking attacks," in Information Systems Security, ed: Springer, 2009, pp. 222-236.

[13] N. M. Basheer and S. S. Abdulsalam, "Digital Image Watermarking Algorithm in Discrete Wavelet Transform Domain Using HVS Characteristics," in Proceedings of the IEEE International Conference on Information Technology: Coding and Computing, 2011, pp. 122-127.

[14] A. Nikolaidis, "Local distortion resistant image watermarking relying on salient feature extraction," Intelligent Control and Automation, 2006. WCICA 2006. The Sixth World Congress on, 2006, pp. 3024-3027.

[15] H.-H. Tsai, et al., "An SVD-based image watermarking in wavelet domain using SVR and PSO," Applied Soft Computing, vol. 12, pp. 2442-2453, 2012.

[16] A. Abbasi and C. Woo, "Robust Image Watermarking Using Genetic Programming," Journal of Software & Systems Development, 2012.

[17] Z. Wang, et al., "A novel blind watermarking scheme based on neural network in wavelet domain," in Repetition Codes," International Journal on Signal & Image Processing, vol. 3, 2012.

[18] D. Muselet and A. Trémeau, "Recent trends in color image watermarking," Journal of Imaging Science and Technology, vol. 53, pp. 10201-1, 2009.

[19] S. D. Lin, et al., "Improving the robustness of DCT-based image watermarking against JPEG compression," Computer Standards & Interfaces, vol. 32, pp. 54-60, 2010.

[20] A. K. Singh, et al., "A novel technique for digital image watermarking in spatial domain," in Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on, 2012, pp. 497-501.

[21] S. Bedi, et al., "Robust secure SVD based DCT–DWT oriented watermarking technique for image authentication," in International Conference on IT to celebrate S. Charmonman's 72nd birthday, 2009, pp. 46.1- 46.7.

[22] P. Lipinski, "On domain selection for additive, blind image watermarking," Bulletin of the Polish Academy of Sciences-Technical Sciences, vol. 60, pp. 317-321, Jun 2012.

[23] A. K. Singh, et al., "Wavelet Based Image Watermarking: Futuristic Concepts in Information Security," Proceedings of the National Academy of Sciences, India Section A: Physical Sciences, vol. 84, pp. 345-359, 2014.

[24] P. Wu, "Research on digital image watermark encryption based on hyperchaos," 2013.

[25] D. Arya, "A survey of frequency and wavelet domain digital watermarking techniques," International Journal of Scientific & Engineering Research, vol. 1, 2010.

[26] M. Ali and C. W. Ahn, "An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain," Signal Processing, vol. 94, pp. 545-556, 2014.

[27] H. A. Abdallah, et al., "Blind Wavelet-Based Image Watermarking," International Journal of Signal Processing, Image Processing & Pattern Recognition, vol. 4, 2011.

[28] Dolatabadi, Z.S.S., A.B.A. Manaf, and M. Zamani, Using Three Levels DWT to Increase Robustness against Geometrical Attacks. International Journal of Advancements in Computing Technology, 2013. 5(14): p. 86