Overview of Various Digital Image Watermarking Methods

Mr. S. G. Mujawar[1] Mr. A. A. Dum[2]
[1,2]Department of Technology
[1,2]Shivaji University, Kolhapur, Maharashtra, India

Abstract— Digital watermarking is the method which promises to tackle the piracy of multimedia. In digital watermarking, the watermark data (information related to publisher, file transaction/ downloading records, user identity, etc.) is embedded into the original multimedia object, in hidden format without affecting the normal usage of original file. Many algorithms are available for image watermarking based on histogram, spread spectrum, quantization, discrete cosine transform (DCT). From the previous research, it is clear that, there is a trade-off between the imperceptibility, embedding capacity and robustness. Different methods fulfill different extent of these parameters. Most of the methods do not improve the imperceptibility, embedding capacity, security and robustness satisfactorily. In applications such as, covert communication, embedding capacity must be high, while robustness against geometric attacks is not mainly concerned. The watermarking method based on DCT can normally achieve comparatively high embedding capacity than other methods under given imperceptibility and robustness. Hence, to further enhance the embedding capacity we can develop an algorithm based on discrete cosine transform.

Key words: Discrete cosine transform, High embedding capacity, Image watermarking

I. INTRODUCTION

It is easy and very economical to transmit images and video files using computer networks rather than to send hard copies by post. Hence, images are stored in databases in digital form. A major impediment to the use of electronic distribution and storage is the ease of intercepting, copying and redistributing electronic images and documents in their exact original form. As a result, publishers are extremely reluctant to use this means of disseminating material. As Communication networks growth is very fast and advances technologies in multimedia processing, piracy of multimedia has become a major problem. One can illegally redistribute the multimedia file, with his/her name, and make profit from it. Hence, there should be some promising technique to tackle the multimedia data piracy. The digital watermarking is the method which promises to tackle the piracy of multimedia. Digital watermark is a pattern of bits inserted into a digital multimedia (image, audio or video) that identifies the copyright and authenticates information.

The watermark data (publisher information, file transaction/ downloading records, user identity, etc.) is embedded into the original multimedia object, in hidden format without any disturbing the normal usage of original file.

According to human perception, watermarking is classified as visible and invisible watermarking. While according to working domain, watermarking is classified as spatial domain (watermark data is embedded into a carrier signal of image) and frequency domain (embed watermark data in the spectral coefficients of the image).

Imperceptibility, embedding capacity, security and robustness are primary concerns in the context of image watermarking. Until now, there are different algorithms used for watermarking based on histogram, spatial feature region, Spread Spectrum(SS), quantization method, discrete cosine transform, discrete wavelet transform are available.

The remainder of the paper is organized as follows. Section II describes available literature review. The comparison of previous methods is analyzed in Section III. Section IV concludes the paper.

II. LITERATURE SURVEY

T. Zong, Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou and G. Beliakov [1] presented a new image-watermarking method built upon histogram technique, to deal with Cropping and random bending attacks and other common attacks. Preprocessing of host image is done by Gaussian low-pass filter, such that watermarks will only be embedded into the low-frequency component of the host image, to deal with signal processing attacks. HFCM scheme is proposed to compensate the side effect of Gaussian filtering, which further enhances robustness.

X. Gao, C. Deng, X. Li and D. Tao [4], solved the problem of synchronization error in image watermarking by applying the affine invariant points of an image. They incorporate ACRs with normalization and orientation alignment steps; this improved the robustness of the proposed scheme, especially to non-isotropic scaling, RBAs, and other affine transformations.

J. Franco-Contreras, G. Coatrieux, F. Cuppens, N. Cuppens- Boulahia and C. Roux [6] presented a scheme which modulates the relative angular position of the circular histogram center of mass of one numerical attribute for embedding the message. Even if the database has been modified, this method can be used for verifying the integrity of the database and also for verifying its authenticity.

M. Andalibi and D. M. Chandler [7] presented a method, whose main idea is to recast the watermarking task into a texture similarity task by adaptively transforming the logo into a set of textures that visually match the textures of the host image. They transform the logo into a visually similar texture via the Arnold transform and one lossless rotation. And embedding of the transformed logo into that region via a standard wavelet based embedding scheme. Author also employs a multi-step extraction stage, in which affine parameter estimation is performed to compensate for possible geometrical transformations. This method is robust to a various attacks.

M. Li, M. K. Kulhandjian, D. A. Pados, S. N. Batalama and M. J. Medley[8] present a new type of watermarking detector to tackle the Host Signal Interference (HSI), which exploit multi-carrier concept. This method can

reduce HSI to certain extents. But, its performance deteriorates dramatically with the rise of embedding rate.

Shih-Hao Wang and Yuan-Pei Lin [9] proposed a method based on the uniform quantization of the direction of gradient vectors. This method embeds the watermark bits in the direction (angle) of significant gradient vectors, at multiple wavelet scales. To quantize the gradient direction, the DWT coefficients are updated based on the derived relationship between the changes in the coefficients and the change in the gradient direction. This method has these advantages- increased watermarking capacity, increased invisibility of the embedded watermark, and robustness to amplitude scaling attacks.

M. Zareian and H. R. Tohidypour [11] presented a novel quantization based watermarking approach, which is invariant to gain attack. In spatial domain, the host signal vector is considered. The host signal was divided into two parts and quantization was implemented in both parts, respectively. The decoding process is carried out by using Euclidean distance. The method is invariant to gain attack and also possess robustness to various attacks (scaling, salt & pepper attack, JPEG attack, etc.).

Q. Kang, K. Li and J. Yang [14] presented a robust watermarking method based on Discrete Cosine Transform (DCT) domain that combines Quick Response (QR) Code and chaotic system. In embedding process, the high error correction performance and the strong decoding capability of QR Code are utilized to decode the text watermark information which has a strong robustness and security.

T. Zong, Y. Xiang, P. Chen, S. Nahavandi and G. Beliakov [15] presented a novel rank based image watermarking, in which DCT and zigzag scanning is used to construct the coefficient sets with a secret key. Modify coefficient set to insert watermark bits. It can achieve high embedding capacity and robust to various common attacks. This method requires three coefficients are required to hide one watermark bit.

T. Zong, Y. Xiang, S. Guo and Y. Rong [16] presented a method, based on DCT. To hide one watermark bit require only two DCT coefficients, this leads to achieve high embedding capacity. Also, an error buffer is utilized to deal with error caused by different attacks. And, this method is free of HSI. These features make this method and possess robustness against various attacks.

III. Comparison of Previous Methods

Imperceptibility, embedding capacity, security and robustness are the major parameters in the context of image watermarking. Most of the watermarking methods developed promise to tackle the piracy problem but does not improve above parameters satisfactorily. Different methods fulfill different extent of these parameters. Table1. Show different watermarking methods with corresponding levels of parameters.

Overall, from previous research we can say that, the methods based on SS and quantization can normally achieve higher embedding capacity, compared to the Histogram and Spatial Feature Region watermarking methods. But, the SS-based watermarking approach suffers from the problem of host signal interference (HSI). It is known that HSI can greatly degrade the performance of watermark detection, especially in the presence of attacks, and thus lower robustness. However, similar to the SS-based watermarking methods, the quantization based watermarking methods do not perform well under high embedding rates.

Compared to all these methods, the rank based method built upon DCT, achieves high embedding capacity and under given imperceptibility and robustness.

Method	Parameter		
	Imperceptibility	Embedding capacity	Robustness
Histogram	High	Low	High
Spatial feature region	High	Low	High
Spread-spectrum	Medium	Medium	Medium
Quantization	Medium	Medium	High
DCT	Medium	High	High

Table 1: Different methods of watermarking with corresponding levels of parameters

IV. Conclusion

Rank based watermarking method based on discrete cosine transform achieves high embedding capacity compare to others. It possesses robustness against common attacks. Further enhancement can be done on this method by modifying the algorithm, to achieve high embedding capacity under given imperceptibility and robustness. In this rank based method, they require only two coefficients to hide one watermark bits. Future scope will be to use lesser ratio of the no. of coefficients required for hiding watermark data to the no. of watermark data.

References

[1] T. Zong, Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou and G. Beliakov, "Robust Histogram Shape-Based Method for Image Watermarking," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 25, no. 5, pp. 717-729, May 2015.

[2] S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain, " IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 6, pp. 777_790, Jun. 2008.

[3] P. Dong, J. G. Brankov, N. P. Galatsanos, Y. Yang, and F. Davoine, "Digital watermarking robust to geometric distortions, " IEEE Trans. Image Process., vol. 14, no. 12, pp. 2140_2150, Dec. 2005.

[4] X. Gao, C. Deng, X. Li and D. Tao, "Geometric Distortion Insensitive Image Watermarking in Affine Covariant Regions," in *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 40, no. 3, pp. 278-286, May 2010.

[5] L. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673_1687, Dec. 1997.

[6] J. Franco-Contreras, G. Coatrieux, F. Cuppens, N. Cuppens-Boulahia and C. Roux, "Robust Lossless Watermarking of Relational Databases Based on Circular Histogram Modulation," in *IEEE Transactions*

on Information Forensics and Security, vol. 9, no. 3, pp. 397-410, March 2014.
[7] M. Andalibi and D. M. Chandler, "Digital Image Watermarking via Adaptive Logo Texturization," in *IEEE Transactions on Image Processing*, vol. 24, no. 12, pp. 5060-5073, Dec. 2015.
[8] M. Li, M. K. Kulhandjian, D. A. Pados, S. N. Batalama and M. J. Medley, "Extracting Spread-Spectrum Hidden Data From Digital Media," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 7, pp. 1201-1210, July 2013.
[9] Shih-Hao Wang and Yuan-Pei Lin, "Wavelet tree quantization for copyright protection watermarking," in *IEEE Transactions on Image Processing*, vol. 13, no. 2, pp. 154-165, Feb. 2004.
[10] Q. Li and I. J. Cox, "Using perceptual models to improve fidelity and provide resistance to valumetric scaling for quantization index modulation watermarking," IEEE Trans. Inf. Forensics Security, vol. 2, no. 2, pp. 127_139, Jun. 2007.
[11] M. Zareian and H. R. Tohidypour, "A Novel Gain Invariant Quantization-Based Watermarking Approach," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1804-1813, Nov. 2014.
[12] E. Koch and J. Zhao, "Towards robust and hidden image copyright labeling," in Proc. IEEE Workshop Nonlinear Signal Image Process., Jun. 1995, pp. 452_455.
[13] P.-C. Su, Y.-C. Chang, and C.-Y. Wu, "Geometrically resilient digital image watermarking by using interest point extraction and extended pilot signals," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1897_1908, Dec. 2013.
[14] Q. Kang, K. Li and J. Yang, "A digital watermarking approach based on DCT domain combining QR code and chaotic theory," *2014 IEEE 10th International Conference on Intelligent Computer Communication and Processing (ICCP)*, Cluj Napoca, 2014, pp. 331-337.
[15] T. Zong, Y. Xiang, P. Chen, S. Nahavandi and G. Beliakov, "A high embedding capacity image watermarking method with rank-based embedder and decoder," *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)*, Hefei, 2016, pp. 1260-1264.
[16] T. Zong, Y. Xiang, S. Guo and Y. Rong, "Rank-Based Image Watermarking Method With High Embedding Capacity and Robustness," in *IEEE Access*, vol. 4, no. , pp. 1689-1699, 2016.

