# Watermarking for digital Images

**Ms. Priyanka Nandal**
Maharaja Surajmal Institute of Technology, GGSIPU, Delhi, India

***Abstract***-*With the expansion of internet the need for copyright of digital images has cropped up. The objective of this work is to describe watermarking techniques. Watermarking using text, image or key for the digital image has been described in the current work. Use of multiple watermarking techniques has also been illustrated*

***Keywords***-Digital watermarking; Copyright protection

## I. INTRODUCTION

Digital technology has grown explosively in the recent years. Digital images can be forged without any difficulty. Watermarking is needed for tracing copyright infringements. A signal which can be embedded into a digital image is known as a digital watermark. Digital watermarking is used for image authentication and forgery prevention. Digital watermark helps one to identify a buyer, establish ownership, to provide extra information about digital content, etc. A digital watermark is either visible or invisible. However in both the cases it serves its purpose. For the protection of digital images many approaches are available. The traditional approaches include methods like encryption, time stamping or image authentication.

Digital water marking for text documents have been performed by Brassil et al. [1]. A unique binary codeword is embedded into the document which serves to identify legitimate users. Modifications like changing the interword spacing and line width are used to embed codeword into the document. The watermark is not removed by the standard operations for document handling like scanning, photocopying. It was further proposed that the same idea may be used for image protection. The redundant features of digital images were applied to the transmission in the least significant bits of data by Kurak and McHugh [2]. They also proposed that the presence of corruption cannot be detected by only seeing the image. Checksums were introduced in the least significant bits of an image to restrict unauthorized tampering and implementing a watermark [3]. Least significant bits were also used as a possibility for watermark introduction but the results were not promising in some cases [4]. JPEG image compression algorithm has also served as a watermarking approach for digital images [5]. Using this approach the image was segmented into 8x8 blocks. Marking was done only for eight DCT coefficients in the block. The blocks were placed at random positions to minimize the attacks on the image. Information is conveyed using the remaining DCT coefficients. It is also mentioned in the literature that this technique resembles to the frequency hop spread spectrum communications. Watermarks were produced using m-sequences having properties such as defiant to image cropping, filtering and cryptographic attack [6]-[9]. More robust watermarks are produced as indicated by the recent research [10]. For the watermarking of video and images linear predictive coding has also been used [11]. Their approach was robust as the quantization noise was concentrated over textured features and edges. But this theory was contradicted [12, 13]. Adaptive transform domain methods were developed by them for watermarking. The watermark was embedded in most significant components of image in contrast to all the above listed approaches. They used general methods for division of image into blocks. Mapping of each block into the transform domain was done using the Hadamard transform [14] or DCT transform [15]-[17]. A number of advantageous features are exhibited by the transform domain modulation schemes. First, watermarks can be placed at least noticeable place like texture of the image, as a result of which the original image and the transform domain watermark look same. The irregular distribution of watermark over the image makes it difficult to decode and read the mark.

The algorithms proposed by O' Ruanaidh et al. [13] and Cox et al. [12] also differs from each other in many ways. The significant difference is in the detection and decoding of the mark. A unique Gaussian distribution sequence is embedded into the coefficients by Cox et al. whereas O' Ruanaidh et al. embeds a binary code directly into the image. The purpose of using Gaussian distribution is that it prevents attacks. The need to maintain large database of watermarks is avoided in the latter method. The demerit is that the discrete valued sequences are produced and hence the watermark is less resistant.

Discrete Fourier transform (DFT) has also been used for watermarking [13, 18]. Magnitude and phase of image is represented using DFT, given that DFT of a real image is mainly complex valued. DFT phase was also used for information transmission [13] because human visual system is hypersensitive to phase distortions than magnitude disorders. The relative significance of phase and magnitude components

of the DFT of an image was investigated and it was found that phase is more important [19].

A survey on the existing digital image watermarking techniques is presented by Parasher and Singh [20]. The results of various techniques used for digital image watermarking based on transform domain, spatial domain or wavelets were compared on the basis of their outputs for the watermarking techniques. In their survey, the significant methods of transform domain and spatial domain were elaborated with the advantages and disadvantages of these techniques. An algorithm for color images was proposed by Han et al. [21]. The watermark was processed based on visual cryptography to generate two shares. One share is protected by the copyright and the other share is embedded into the image. The embedding capacity of watermark and robustness are improved to a great extent in their algorithm.

**Plan of paper:**

This paper is organized as follows: Section II describes watermarking methods for images. This section also includes the screen shots of the proposed work. Section III describes results and discussions. Section IV consists of conclusion and future work.

## II. WATERMARKING METHODS FOR IMAGES

In this section the techniques used in the current work for digital watermarking of images are presented. A novel watermarking scheme is presented. Using this technique multiple watermarks are embedded sequentially into a digital image. The proposed method is asymmetric, secure under projection attack and robust against distortion owing to basic operations like format conversion and transmission. This method is based on elementary linear algebra.

The method is accomplished by applying the affine transform to the small blocks. The method interpolates the image samples computed from the affine transform to compute image sample values at discrete sample locations within the transformed block. These interpolated sample values form a block of image data approximating a block in the watermarked image at the time of embedding. However, errors due to estimation and non-linear distortion remain.

**Key Watermarking**

The image to be watermarked is presented in Fig.1.

Fig. 1 Image to be watermarked

Choose the watermarking image as input. Next, select the type of watermarking as text. In the next step, select the text to be embedded as watermark and the font settings of the selected text for the watermarking purpose. The text watermarked image is shown in Fig. 2.

**Image watermarking**

Choose the watermarking image as input. Next, select the image type of watermarking. Select the second image. In the next step, append the selected image onto the original image. The selected second image is shown in Fig. 3 and the appended images are shown in Fig. 4.

Fig. 2 Text Watermark Displayed

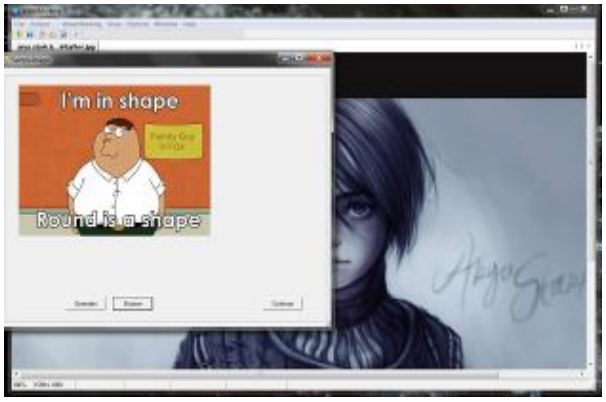


Fig. 3 Select the second image

Fig. 4 Append selected image onto original image

**Multiple Image watermarking**

In multiple image watermarking one image is append onto the other, then the third image is appended onto the previous obtained image. The screenshots of the process followed are illustrated in the Figs. 5 to 7 respectively. Fig. 5 shows the watermarked image using one image as shown in the previous section. Fig. 6 shows the watermarked image with more than one image.

Fig. 5 Watermarked image with one image

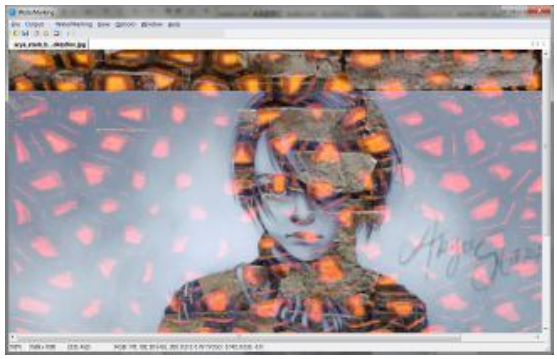

Fig. 6 Watermarked image with more than 1 image

**Key watermarking**

The last module of this work is key based watermarking. The image chosen by the user is encrypted at the sender's end using a randomly generated or user specified 8 digit key. Fig. 6 shown above is used as the input image for key watermarking. Fig. 7 shows the encrypted image.

Fig. 7 Eccryption successful

At the receiver's end, the original image sent by the user can be extracted only after entering the correct key. The decrypted image is obtained and the reverse process is followed to obtain the original image. Fig. 8 shows the original image received on entering correct key and decoding.

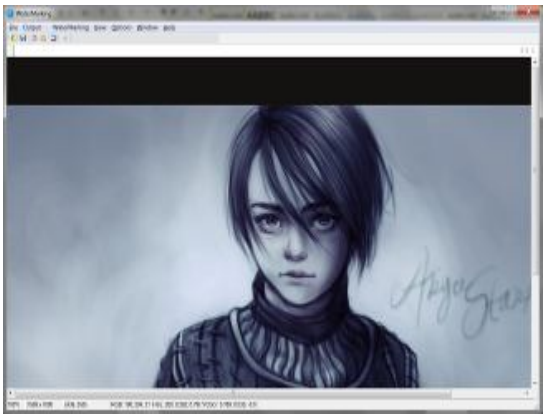

Fig. 8 Original Image received on entering correct key and decoding.

## III. RESULTS AND DISCUSSION

In this work we have presented a technique for watermarking of digital images. This technique can be used to protect the authenticity of the images. The author has also proposed a method to encrypt the watermark in the image.

## IV. CONCLUSION AND FUTURE WORK

The current work proposed in this paper outlines methods for embedding robust watermarks in digital images. The watermark embedded using encryption is invisible to the naked eye. The algorithm proposed can work for color images as well as black and white images. Work can be continued to devise watermarks which are more robust and invisible even

to the careful observer. The watermark image is also prone to geometrical attacks. The geometrical attacks coupled with other attacks are the most severe type of attacks. A template can also be embedded to rectify the geometrical attacks in the future.

## REFERENCES


[1] J. Brassil, S. Low, N. Maxemchuk and L. O'Gorman, Electronic marking and identification techniques to discourage document copying, Proceedings of INFOCOM 94, 1994, pp. 1278-1287.

[2] C. Kurak and J. Mchugh, A cautionary note on image downgrading, Proceedings 8th Annual Computer Security Applications Conference, San Antonio, 1992, pp. 153-159.

[3] S. Walton, Image authentication for a slippery new age, Dr Dobb's J., 1995, pp. 18-26.

[4] C. Dautzenberg and F. M. Boland, Watermarking images, Technical report, Department of Electronic and Electrical Engineering, Trinity College Dublin, 1994.

[5] W. B. Pennebaker and J. L. Mitchell, JPEG still image compression standard, Van Nostrand Reinhold, New York, 1993.

[6] J. Zhao and E. Koch, Embedding Robust Labels into Images for Copyright Protection, In KnowRight, 1995, pp. 242-251.

[7] A. Z. Tirkel, G. A. Rankin, R. M. Van Schyndel, W. J. Ho, N. R. A. Mee and C. F. Osborne, Electronic water mark, Proceedings of Digital Image Computing, Technology and Applications (DICTA'93), 1993, pp. 666-672.

[8] A. Z. Tirkel, R. G. Van Schyndel and C. F Osborne, A two-dimensional digital watermark, Proceedings of DICTA, Dec. 1995, pp. 5-8.

[9] R. G. Van Schyndel, A. Z. Tirkel and C. F. Osborne, A digital watermark, IEEE International Conference on Image Processing (ICIP-94), 1994, pp. 86-90.

[10] R. G. Van Schyndel, A. Z. Tirkel, and C. F. Osborne, Towards a robust digital watermark, Dicta, 1995, pp. 504-508.

[11] K. Matsui, Video steganography:-how to secretly embed a signature in a picture, IMA Intellectual Property Project Proc., 1994, pp. 187-206.

[12] I. Cox, J. Killian, T. Leighton and T. Shamoon, Secure spread spectrum communication for multimedia, Technical Report 95–10, NEC Research Institute, 1995.

[13] J. J. Ruanaidh, W. J. Dowling and F. M. Boland, Phase watermarking of digital images, IEEE International Conference on Image Processing, 1996, pp. 239-242.

[14] R. J. Clarke, Transform coding of images, Astrophysics, 1985.

[15] W. B. Pennebaker and J. L. Mitchell, JPEG: Still image data compression standard, Springer Science and Business Media, 1992.

[16] W. H. Press, S. A. Teukolsky, W. T. Vetterling and B. P. Flannery, Numerical recipes in C, Cambridge: Cambridge university press, 1996.

[17] K. R. Rao, and P. YIP, The discrete cosine transform: algorithms, advantages, applications, New York: Academic, 1990.

[18] J. J. Ruanaidh, W. J. Dowling and F. M. Boland, Watermarking digital images for copyright protection, IEEE Proceedings- Vision, Image and Signal Processing, 1996, pp. 250-256.

[19] A. V. Oppenheim and J. S. Lim, The importance of phase in signals, Proceedings of the IEEE, 1981, pp. 529-541.

[20] P. Parashar and R. K. Singh, A survey: Digital image watermarking techniques, Int. J. Signal Process. Image Process. Pattern Recognit, 2014, pp. 111-124.

[21] Y. Han, W. He, S. Ji and Q. Luo, A digital watermarking algorithm of color image based on visual cryptography and discrete cosine transform, IEEE International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014, pp. 525-530.