Multiple Binary Images Watermarking in Spatial and Frequency Domains

K.Ganesan[1] and Tarun Kumar Guptha[2]

[1]Director, TIFAC-CORE in Automotive Infotronics and
Senior Professor, School of Information Technology and Engineering, VIT University, Vellore, India
kganesan@vit.ac.in
[2]M.S.Software Engineering, School of Information Technology and Engineering, VIT University, Vellore, India.
tarunguptha@yahoo.com

Abstract

Editing, reproduction and distribution of the digital multimedia are becoming extremely easier and faster with the existence of the internet and the availability of pervasive and powerful multimedia tools. Digital watermarking has emerged as a possible method to tackle these issues. This paper proposes a scheme using which more data can be inserted into an image in different domains using different techniques. This increases the embedding capacity. Using the proposed scheme 24 binary images can be embedded in the DCT domain and 12 binary images can be embedded in the spatial domain using LSB substitution technique in a single RGB image. The proposed scheme also provides an extra level of security to the watermark image by scrambling the image before embedding it into the host image. Experimental results show that the proposed watermarking method results in almost invisible difference between the watermarked image and the original image and is also robust against various image processing attacks.

Key Words

Discrete Cosine Transform, Spatial Transform, LSB Technique, Watermarking, Scrambling, Cat Map

1. Introduction

A large number of Digital Watermarking schemes have been studied to protect the intellectual property rights of the owner. All these schemes implement either visible or invisible watermarks. An example of visible watermarking is seen in television channels when their logo is visibly superimposed in the corner of the screen. Streaming audio, video and still images are the best hosts for invisible watermarks to embed the copyright data. One of the types of media is digital imagery, which can be copied and widely distributed without any significant loss of quality. Protecting the property rights of the owners of these images is therefore important. Also, it is necessary to secure the images in security related areas so that the images are not tampered with. A means to protect this data is to apply a digital watermark.

Digital watermarking is the process by which an image is coded with an owner's watermark and can be done using either of two general approaches. One approach is to transform the host

DOI : 10.5121/sipij.2010.1213

image into its frequency domain representation [1, 2] and embed the watermark data therein. The second is to directly treat the spatial domain data of the host image to embed the watermark [3]. Regardless of the embedding method, the embedding technique must satisfy several requirements such as the watermarked image should retain as closely as possible the quality of the original image. The watermark should be robust to various types of image processing techniques such as JPEG compression, noise, etc [4, 5]. This requirement is due to the common application of techniques such as compression, as well as the possibility that these techniques may be applied with the intent to destroy the watermark in the image.

Capacity [6, 7] is also one of the important aspects that are to be noticed in the watermarking design along with the security and robustness. The main objective of our paper is to embed more watermark data using different transform domains and techniques and to minimize the distortion of the watermarked image.

This paper is organized in the following way. Section 2 deals with the related work. Section 3 describes the proposed scheme and the associated embedding and extracting methodologies in different domains. Section 4 deals with testing and results obtained. Section 5 deals with the conclusions based on the obtained results.

2. Related work

In the literature, many watermarking techniques using spatial [3, 4] and frequency domains [5, 8] are available. In [9] a novel technique using the combinational spatial and frequency domains is proposed. The splitting of the watermark image into two parts, respectively, for spatial and frequency insertion relies on the user's preference and data importance.

In [1] an Adaptive Frequency domain watermarking approach in real time is proposed, demonstrating robustness against intentional or unintentional attacks on the watermarked image. This is achieved by modifying the middle frequency coefficients. Since the image is analyzed and modified in the frequency domain the changes made are difficult to perceive.

In [10] a modified digital image watermarking scheme based on the combination of spatial and transform domains is proposed. The aim is to achieve robustness for the vital part of the watermark image without sacrificing the embedding capacity of the watermark image. The watermark image is split into two parts depending on the vital information. The perceptibility of the watermarked image is improved by hiding the vital part of the watermark image in the blocks of the host image having highest variance in transform domain. The remaining part of the watermark image is watermarked in the spatial domain.

In [11] a semi-blind reversible pixel-wise image authentication framework is proposed. The scheme allows one to authenticate and locate tampered pixels. Also exact recovery of the original image is possible.

In [12] a modified digital image watermarking scheme based on the combination of spatial and transform domains is proposed. The watermark image is split into two parts depending on the vital information. The perceptibility of the watermarked image is improved by hiding the vital part of the watermark image in the blocks of the host image having highest variance in

transform domain. The remaining part of the watermark image is watermarked in the spatial domain.

In [13] a heuristic method to enhance the quality of the extracted watermark is proposed. The image is divided into non overlapping blocks, and the reference coefficient data are used to modify the pixel values.

3. Proposed Watermarking Scheme

In order to embed more data into the host image, the watermark image which is an RGB image can be formed using multiple binary images. Let H be the colour host image of size NxN and W be the colour watermark image of size MxM which is formed by combining the multiple binary images. Each component of the watermark image is formed by 8 different binary watermark images. Hence, the RGB watermark image is formed by using 24 binary images. This colour watermark image is embedded into the colour host image in frequency domain using Discrete Cosine Transform (DCT). The obtained marked image must be less distorted when compared to the original image.

Watermark can be embedded in spatial domain also. The LSB substitution technique can be used to embed the data. The watermark image, which is an RGB image, has three components. Hence, three binary images can be embedded. In each component four LSB s can be replaced i.e., totally 12 binary images can be embedded in Spatial domain. If more number of images are embedded, then more is the distortion. Therefore, using the proposed combinational scheme totally 36 images can be embedded in a single RGB image.

3.1 Discrete Cosine Transform

A Discrete Cosine Transform can be interpreted as decomposition into a set of frequency coefficients having the same bandwidth on a logarithmic scale. The obtained coefficients are real number values. The coefficients can be split using the zigzag ordering into low frequency coefficients, mid-frequency coefficients, and high frequency coefficients as shown in Fig 3.1. The mid frequency coefficients are considered to be appropriate for embedding the watermark data. In the proposed method 50% of the total coefficients lying in the middle frequency region are used for embedding. The 25% coefficients belonging to the low frequency region affect visibility of the image and the 25% coefficients belonging to the high frequency coefficients are sensitive to the attacks.

The two-dimensional DCT of an M-by-N matrix A is defined as follows

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \qquad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases} \qquad \text{-----(1)}$$

The DCT is an invertible transform, and its inverse is given by

$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le m \le M-1 \\ 0 \le n \le N-1 \end{matrix}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \qquad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases} \qquad \text{-----(2)}$$

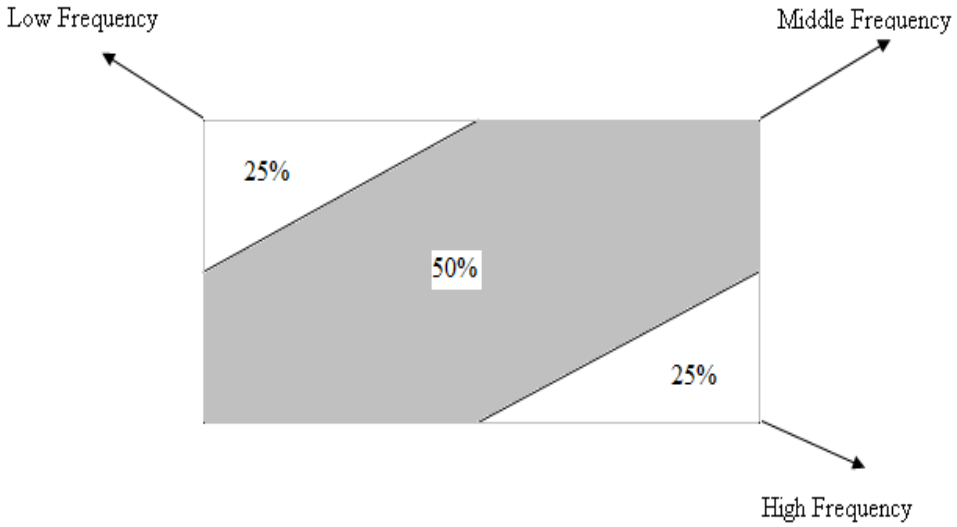


Fig 3.1: DCT decomposition of an image

3.2 Watermarking in the Frequency Domain

There are several transforms in frequency domain using which watermark can be embedded into the host image. Generally, we can insert data into the coefficients of a transformed image. The important consideration is, what locations are best for embedding watermarking in the frequency domain to avoid distortion. It is considered to be better to insert the data in the middle frequency coefficients of the host image.

The 24 binary images that are to be embedded into the host image Fig 3.2.1 are divided into three groups of 8 images. The size of each binary image is half of the size of the host image. The pixel values of the 8 binary images as shown in Fig 3.2.2 are combined to form a grey scale image as shown in Fig 3.2.3a. Each pixel bits of all the binary images are combined respectively to form the 8 bit intensity pixel value of the grey scale image. Similarly two more grey scale images are generated by combining 16 different binary images as shown in Fig 3.2.3b and Fig 3.2.3c. Each generated grey scale image is considered as a component of an RGB image and hence the three grey scale images are combined to form the RGB image as shown in Fig 3.2.4. This new RGB image is the watermark image that is to be embedded, whose size is half of the size of the host image.

The DCT is applied to each component of the host image and the watermark image in order to obtain the coefficients. The middle frequency coefficients of the host image are identified using the zigzag ordering. The watermark image component is embedded into the host image component with a proper embedding factor to minimize the distortion. The inverse DCT is applied to each embedded component and the components are combined to form the marked RGB image as shown in Fig 3.2.5.

Embedding is done by multiplying the watermark bit with an appropriate scaling factor.

$$I^{w}_{ij} = I_{ij} + \alpha * W_{ij} \qquad i,j=1,2,.....n \qquad \text{-----(3)}$$

where,

W=watermark image

I = Host image

α = Scaling factor

I^{w} = marked image

Fig 3.2.1: Host image

Fig 3.2.2: 8 binary images

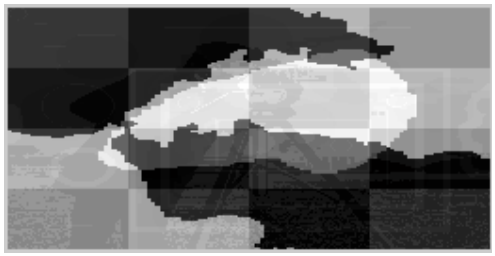


Fig 3.2.3a: Grey scale image1 formed by the binary images

Similarly, two more grey scale images are formed that are embedded in the host image components.

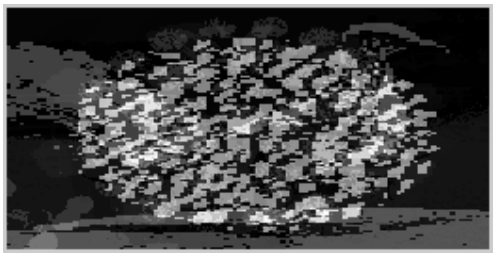


Fig 3.2.3b: Grey scale Image2

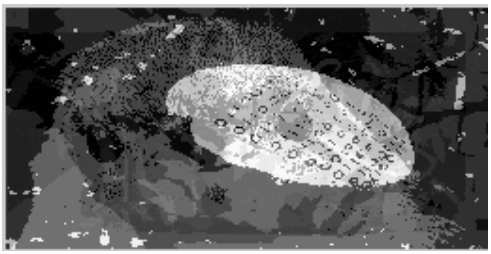


Fig 3.2.3c: Grey scale Image3

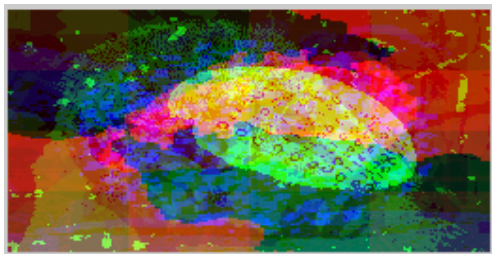


Fig 3.2.4: Generated RGB Watermark image

The RGB watermark image is obtained by combining the three grey scale images.

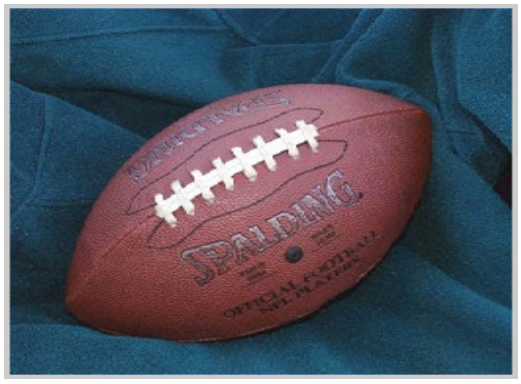


Fig 3.2.5: Marked image

The Marked image is obtained by embedding the watermark image into the host image.

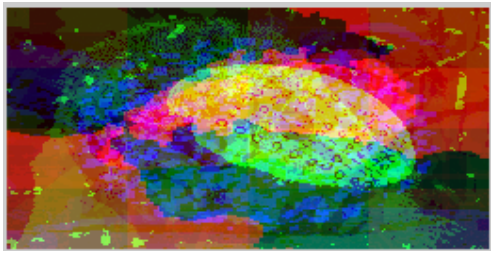
3.3 Extraction in the Frequency Domain:

The extraction process is the reverse process of embedding. The marked RGB image is obtained and is divided into individual components. The middle frequency coefficients of the original image component and the marked image component are subtracted and divided by the embedding factor to obtain the watermark image components which are grey-scale images as shown in Fig 3.3.1. Each bit of the pixel of the grey scale image is used to form different binary images. These images are compared with the original binary images using the similarity ratio which is defined in the later section.

$$W_{ij} = (I^{w}_{ij} - I_{ij}) / \alpha \qquad i,j=1,2,.....n \qquad \text{-------- (4)}$$

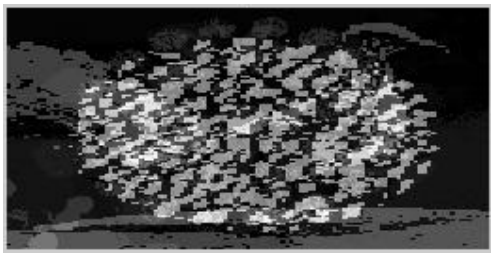
where,

W=extracted watermark image
I = original image
α = Scaling factor
I^{w} = marked image

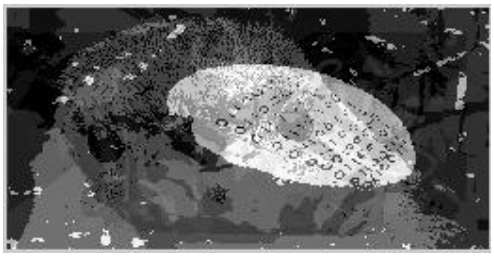


RGB Image

Grey scale Image1



Grey scale Image2



Grey scale Image3

Fig 3.3.1: Extracted images

3.4 Watermarking in the Spatial Domain

One of easiest way of embedding a watermark is to replace the LSB bit of the pixels of the host image. The components of RGB host image are obtained and the LSB bits of the pixel values of each component are replaced by the pixel values of the binary watermark image.

The 4 LSB bits of a pixel of a grey scale image can be replaced, with less distortion in the marked image. Hence, totally 12 binary images can be embedded in the RGB host image with different levels of distortion. The RGB components of the host image are obtained and depending upon the size of the watermark image, it is embedded into the host image by replacing the LSB bits of the corresponding pixels in the host component.

3.5 Extraction in Spatial Domain

Extraction in the spatial domain is the reverse process of the embedding. The RGB marked image is split into its components. Depending upon the size of the watermark image, the LSB bits of the corresponding pixels are extracted to form the binary image. The obtained binary image is compared to the original image using the similarity ratio (SR).

$$SR = S/(S+D) \quad \text{--- (5)}$$

where S denotes the number of matching pixel values in compared images, and D denotes the number of different pixel values in compared images. Here the compared images are the original and extracted watermarks. The acceptable range of the similarity ratio is 0.85 to 1.

3.6 Security Enhancement using Scrambling

Image scrambling transforms a meaningful image into a random or meaningless image using some of the mathematical equations. Before embedding the watermark image into the host image, it can be scrambled such that during the extraction the scrambled image is obtained and only the authorised person with the appropriate descrambling algorithm can descramble it to obtain the original image. Scrambling of an image can be performed using different techniques. Here in this paper, when embedding in the frequency domain, the simple sign changing technique is used and in spatial domain a cat map is used to scramble the image.

3.6.1 Image scrambling in frequency domain

The sign changing technique is used to scramble the watermark image. The Discrete Cosine Transform is applied to the image to obtain the DCT coefficients which are real numbers. The sign of few coefficients are reversed and then the inverse transform is applied to obtain the scrambled image as shown in Fig 3.6.1, which is then embedded into the host image.

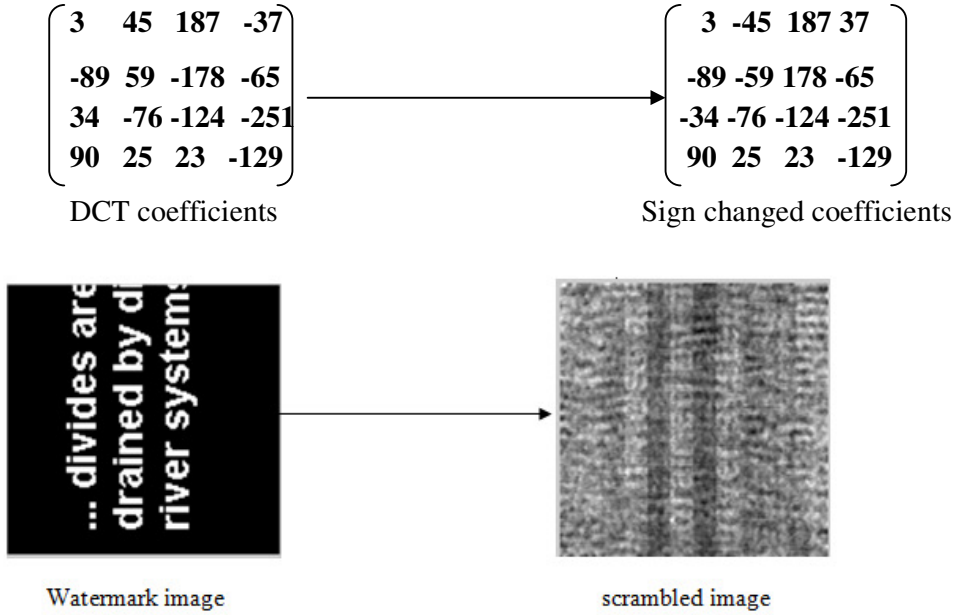


Fig. 3.6.1: Frequency domain scrambling

3.6.2 Image Scrambling in Spatial Domain

The watermark image is scrambled using the following cat map.

$$\begin{pmatrix} X1 \\ Y1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} * \begin{pmatrix} x \\ y \end{pmatrix} * \mathrm{mod}(N)$$

------(6)

The cat map provides the new position of the pixel using the above equation for the given pixel with its position which gives the scrambled image as shown in Fig 3.6.2, which is then embedded into the host image.

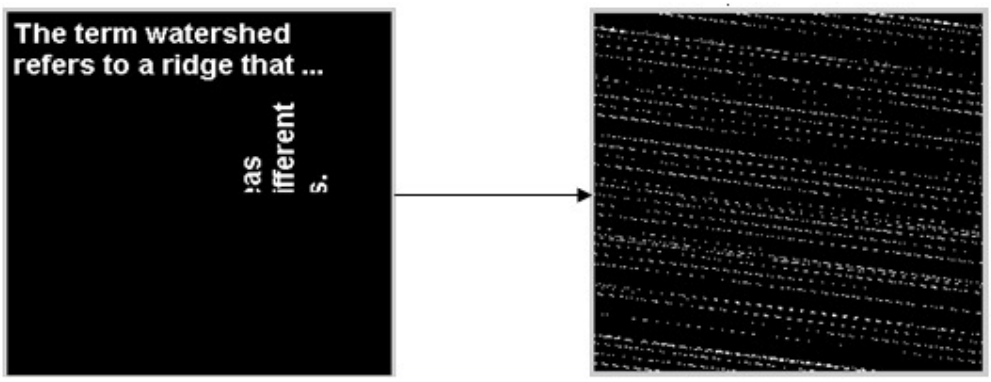


Fig 3.6.2: Spatial domain scrambling

4. Testing and Results

Various Image processing attacks can be applied to the marked image and the change in its quality can be tested using the PSNR (Peak Signal to Noise Ratio) values, which is defined by the equation

$$PSNR = 20\log_{10}(255/RMSE) \quad \text{-----(7)}$$

where 255 represents the maximum value of each pixel and RMSE is the square root of Mean Squared Error (MSE) between the original and marked images. The mean square error is calculated using

$$MSE=(1/H*W)\ {}_i\sum^{H}\ {}_j\sum^{W}(X_{ij}-X'_{ij}) \quad \text{-----(8)}$$

Here the notations H and W are the height and width of an image, X_{ij} is the pixel value of the coordinate(x, y) in an original image and $X'_{i,j}$ the pixel value of the watermarked image.

The image shown in the Fig4.1 is the extracted RGB image after applying the Gaussian noise of mean '0' and variance of '0.0001' to the marked image and the images in Fig 4.1a, Fig 4.1b and

Fig 4.1c are the corresponding grey scale images which corresponds to the R, G and B components.

Extracted Images after attack

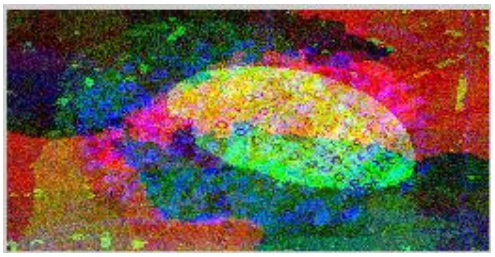


Fig 4.1: RGB image

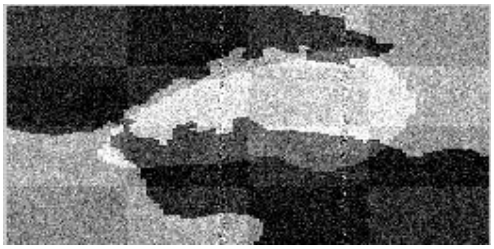


Fig 4.1a : Grey scale image(Rcomponent)

Fig 4.1b: Grey scale image(G component)

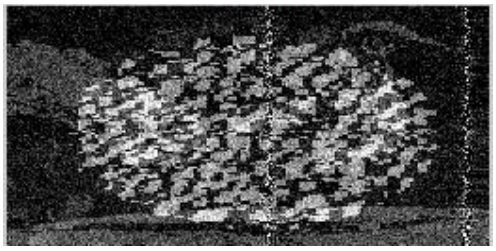


Fig 4.1c: Grey scale image(B component)

Different image processing attacks such as noise, JPEG compression, blur are applied to the marked image and is tested. The following table shows the PSNR values in the DCT domain for each component after applying the corresponding attack on the marked image. As the PSNR values ranging between 35 and 70 are acceptable, the values in the Table 4.1 show that the proposed scheme is robust against Gaussian noise and JPEG compression up to 90%.

Table 4.1: DCT Domain Embedding PSNR Values

Type of Attack	PSNR of R component	PSNR of G component	PSNR of B component
No attack	48.5890	49.9766	51.2626
Noise	48.5890	49.7847	45.6693
JPEG Compression (90%)	36.6431	37.8777	37.1655
JPEG Compression (99%)	44.1319	46.8349	45.1860
Blur	31.4040	31.3221	31.2598

The following table shows the PSNR values in the spatial domain after substituting in the first, second, third and fourth LSB bits. The values in the table show that, for better results embedding in the first two bits i.e., embedding 6 images is more preferable than embedding in the four bits i.e., 12 images. The proposed scheme is robust against noise and JPEG compression but not against blur.

Table 4.2: Spatial Domain Embedding PSNR Values

Bit of Insertion	PSNR of R component	PSNR of G component	PSNR of B component
First LSB	51.1336	51.1374	51.1283
Second LSB	45.7090	43.9684	43.2657
Third LSB	39.1514	37.4085	37.7457
Fourth LSB	31.8759	30.7681	31.7532

5. Conclusions

The proposed watermarking scheme provides 24 binary images to be embedded in the frequency domain and also 12 more binary images in the spatial domain. Hence, the capacity of the watermark to be embedded in the host image is much greater. Therefore, we not only increase the size of watermark, but also ensure acceptable level of security and imperceptibility. Hence, by using the combinational scheme totally 36 images can be embedded in a single RGB image.

The experimental results show that embedding of 6 binary images in spatial domain will give better results when compared to 9 or 12 binary images. Therefore, to obtain better results maximum of 30 binary images can be embedded in a single RGB host image. An increase in the level of security can be achieved by using different scrambling techniques before embedding in the host image in different domains. The major advantage of this scheme is the increase in the capacity with less distortion. We used different scrambling techniques in different domains to enhance the security.

Acknowledgements

This work forms the part of the R & D activities of TIFAC-CORE in “Automotive Infotronics” at VIT University, Vellore, India. The authors would like to thank TIFAC for providing necessary infrastructure needed for carrying out this work successfully.

References

[1] Ravi Shah, Abhinav Agarwal and Subramaniam Ganesan, “Frequency Domain Real Time Digital Image Watermarking”, Oakland university, MI-48309, 1998.

[2] Ing.Petr Cika, “The Improvement of the Method for Digital Image Watermarking in Frequency Domain”, IJCSNS international Journal of Computer Science ad Network Security, VOL.7 No.3, March -2007.

[3] O. Bruyndonckx, J.-J. Quisquater, B. Macq, “Spatial method for copyright labeling of digital images”, Proceeding of IEEE Workshop on Nonlinear Signal and Image processing, Neos Marmaras, Greece, 20–22 June 1995, pp. 456–459.

[4] N. Nikolaidis, I. Pitas, “Robust image watermarking in the spatial domain, Signal Processing”, volume 66, issue 3, (may 1998), pages 385-403.

[5] Shinfeng D. Lin, Chin-Feng Chen, “A robust DCT-based watermarking for copyright protection”, IEEE Trans. Consumer Electron. 46 (3) (2000) 415–421.

[6] M. Barni, F. Bartolini, A. De Rosa, A. Piva, "Capacity of the watermarkchannel: how many bits can be hidden within a digital image?" Proc. SPIE 3657 (1999) 437–448.

[7] P. Moulin, M.K. Mihcak, "The data-hiding capacity of image sources", IEEE Trans. Image Process, 2002.

[8] Jiwu Huang, Yun Q. Shi, Yi Shi, "Embedding image watermarks in DC components", IEEE Trans. CSVT 10 (6) (2000) 974–979.

[9] Frank Y.Shih, Scott Y.Y.Wu, "Combinational Image watermarking in the Spatial and Frequency domain", Pattern Recognition, volume 36,Number 4,April 2003,pages 969-975.

[10] Ken Cabeen and Peter Gent, "Image Compression and the Discrete Cosine Transform" (Private Communication)

[11] Romualdas Bausys,Arturas Kriukovas , "Reversible Watermarking Scheme for Image Authentication in Frequency domain", 48th International Symposium ELMAR -2006,07-09 June,Zadar,Croatia

[12] B. Chandra Mohan, S. SrinivasKumar t, B.N.Chatterjee, "DIGITAL IMAGE WATERMARKING IN DUAL DOMAINS" (Private Communication).

[13] Chin-Chen Chang, Yung-Chen Chang and Jau-Ji Shen , "A Heuristic Method for Extracting Enhanced Watermarks from Digital Images", IIH-MSP, International conference on Intelligent Information hiding and Multimedia, pages 453-456,2006.

Authors

K. Ganesan obtained his Ph.D from Bharathidasan University, Tiruchirapalli, India in 1993. Then he worked as a Post Doctoral Fellow at Queen's University of Belfast, United Kingdom for 3.25 years. He was heading the Computer Science and Engineering Department at Vellore Institute of Technology, Vellore, India during 2002-2005. Currently he is the Director of TIFAC Centre of Relevance and Excellence in Automotive Infotronics located at VIT University, Vellorte, India. He is guiding 5 Ph.Ds. He has visited more than 15 countries abroad. He has got more than 50 journal and International conference publications. He has recently filed a patent. His areas of interest include Image and Video processing, Data security, Wireless and embedded systems, Mobile computing. His profile has been included in the 9th and 10th anniversary edition of Marquis Who's Who in Science and Engineering. He has been identified as one of the Top 100 Scientists 2008 by International Biographical Centre, Cambridge, England.

Tarun Kumar Guptha is a student of VIT University, Vellore. He is currently pursuing his final year in M.S.Software Engineering .His area of interests are Image Processing , Embedded Systems and Software Engineering .