ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Efficient and Robust Watermarking Technique against Jpeg Compression Attacks

Venkata Giridhar Madabhaktula*[1] and Tammineni Ravikumar[2]
*[1] Student, M.Tech(C.S.E), [2] Assistant professor, Department of C.S.E
Aditya Institute of Technology and Management,
Tekkali,A.P ,India
*giridharvenkata@yahoo.co.in

Abstract: Digital watermarking is an effective and popular technique for discouraging illegal copying and distribution of copyrighted digital image information. One of the important features of the watermarking technique is the robustness of the watermarked image, which will preserve the quality of the retrieved watermark. There are two parts about robust oblivious watermarking scheme based on the frequency domain and image authentication technique is presented in this paper. One is the region used to hide the information is located at the middle frequency portion of the host image so as to provide good quality for both the watermarked image and the retrieved watermark. Such a scheme can provide a high degree of robustness against JPEG compression attacks. The other is signature process i.e. the input is the extracted property from the edge of the image. The signature can be correctly verified when the image is incidentally damaged such as lossy compression. Experimental results are also presented to demonstrate the validity and robustness of the new approach.

Keywords: jpeg**,** DCT, Quantization, watermarking, data hiding, mean square error (mse) , blocking effect prediction (BEP).

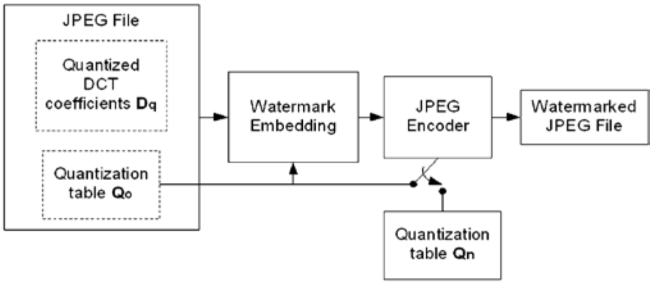
I. INTRODUCTION

Nowadays, most digital images are stored in JPEG format, in digital cameras and the World-Wide Web alike. People are gradually motivated to embed watermark or information bits such as owner information, date, time, camera settings, event/occasion of the image, image title, or even secret messages in the JPEG images for value-added functionalities and possibly secret communication. In these applications, the input to the watermarking scheme is a JPEG image file and the output is also a JPEG image file. We call this kind of watermarking (or data hiding) scheme JPEG-to-JPEG (J2J) watermarking schemes. This paper is about J2J watermarking schemes.

There are many papers investigating the robustness of watermarks against JPEG compression such as [9]–[11]. Eggers et al. [12] analyzed the quantization effect on the detection of watermarks by considering the additive watermark signal as a dithering signal. Although many watermarking (or data hiding) algorithms were proposed to embed digital watermarks in uncompressed images, those algorithms may not be suitable for embedding watermarks in JPEG-compressed images (.jpg files). This is because the DCT coefficients in JPEG-compressed images have special statistical characteristics—they must be multiples of the corresponding quantization factors. These special characteristics reduce the degree of freedom for watermarking. If the output images are not JPEG compatible, the existence of the watermark may be detectable using steganalysis techniques [13]. If the output images are JPEG-compatible which is the J2J framework, all DCT coefficients must be re-quantized after the watermark insertion, which further reduces the degree of freedom for watermarking.

There are a few existing schemes for J2J watermarking [2], [14]–[18]. Choi et al. [14] and Luo et al. [15] used inter-block correlation of selected DCT coefficients to embed the watermark bits, adding or subtracting an offset to the mean value of the neighboring DCT coefficients. Wong and Au proposed to hide bits by modifying the DC [16] and AC coefficients [17] in the block-based DCT domain. Hartung [2] used the spread spectrum technique (SST) [3] to embed watermarks in I-frames, P-frames or B-frames of MPEG-2 compressed video. Compression of I-frames is effectively the same as JPEG. Wong and Au proposed a robust watermark scheme using iterative SST [18]. These methods embedded different amount of watermark bits into JPEG images while maintaining good visual quality of the watermarked JPEG images. However, no one estimated the J2J data-hiding capacity, or the maximum amount of bits that can be embedded in JPEG image files.

There are some existing methods to estimate the data hiding capacity of digital images [19]–[28], though they are not JPEG images. Most of these methods apply the work of Shannon [7] and Costa [8]. Servetto et al. [19] used statistical models to analyze the robustness of the SST and estimated the watermarking capacity against the jamming noise. Barni et al. [20], [21] modeled each watermark channel by using Generalized Gaussian density to model the full frame DCT coefficients. Moulin et al. [22] modeled coefficients in different domains and estimated the data hiding capacity under mean square error (mse) constraints. Lin [37] estimated the zero-error capacity of images against JPEG attacks with largest applicable quantization step. Some papers combined the Information-Theoretic model [1] and perceptual models to estimate the capacity [23], [24]. Some [25], [26] focused on comparing the capacity among different transforms such as the identity transform (IT), discrete cosine transform (DCT), Karhunen–Loeve transform (KLT), and the Hadamard transform. Fei et al. [25] suggested that the coefficients in the Slant transform had the highest capacity while Ramkumar et al., [26] indicated that transforms with poor energy compaction property such as Hadamard transform tended to have higher capacity than those with higher energy compaction property such as DCT. Sugihara [27] estimated the capacity by taking robustness of the hidden data into account. Voloshynovskiy et al. [33] analyzed the security of the hidden data and suggested different modulation schemes for different purposes of data hiding. Kalker et al. [31] estimated the capacity of a particular data hiding area—lossless data embedding, first proposed by Fridrich et al. [32]. For lossless data embedding, the original cover work can be restored at the decoder. This is particularly useful for many digital media such as medical images. Cohen *et al.* [30] analyzed the capacity for private and public (or blind) data hiding schemes [6] and the capacity under additive attacks. Instead of estimating the capacity, some proposed realizations to approach the theoretical limit of capacity such as [29], [33], [34]. Perez Gonzalez *et al.* [29] suggested to use convolution and orthogonal codes. Eggers *et al.* [34] proposed the scalar costa scheme (SCS) by considering the data hiding as the communication-with-side-information problem which has good performance at high watermark- to-noise ratio (WNR).



Figur. 1. JPEG-to-JPEG watermarking (J2J).

In this paper, we attempt to estimate the data hiding capacity of JPEG images in J2J watermarking schemes. To embed watermarks in JPEG-compressed images, the JPEG file needs to be partially or fully decoded. The level of decoding depends on the domain the watermark will be embedded in. If the watermark is embedded in the bitstream domain, only variable-length decoding is needed. If the watermark is embedded in 8-by-8 block-based DCT domain, inverse zigzag scanning and inverse quantization are necessary. If the watermark is embedded in spatial domain or other frequency domains, inverse DCT would be needed. The J2J model is shown in Fig. 1. In this paper, we make two assumptions. The first assumption is that the watermarked images will be JPEG-compressed using either the original quantization table Q_o extracted from the input JPEG file or a new quantization table Q_n defined by the user. With this assumption, we have the J2J framework. The second assumption is that the dimensions of the images are not changed in the watermark embedding. The J2J model makes no assumption on the domain the watermark is embedded in. There are four J2J cases as follows and this paper addresses most of the cases.

a. The original quantization table Q_o is used to compress the watermarked image, i.e., $Q_n = Q_o$ and no other processing is applied to the image. An example is a watermarking command program.
b. The original quantization table Q_o may or may not be used to compress the watermarked image, i.e., $Q_n = Q_o$ or $Q_n \neq Q_o$ and no other processing is applied to the image. An example is a watermarking command program with an option to choose a different quality factor (QF) or Q
c. The original quantization table Q_o is used to compress the watermarked image, and the image may be altered by some kind of processing before or after the watermarking insertion. An example is image processing software such as Adobe Photoshop with watermarking functionality, and the user performs red-eye reduction or other filtering before or after the watermark insertion and then chooses the 'Save' (instead of 'Save as') command to save the image.
d. The original quantization Q_o table may not be used to compress the watermarked image, and the image may be altered by some kind of processing before or after the watermarking insertion. An example is the user performs red-eye reduction before or after the watermark insertion and then chooses the "Save As"' command (instead of "Save") to save the image. In the "Save As" command, the user may choose different QF in the JPEG compression.

For case 1, we propose a method in Section II to estimate the data-hiding capacity of the JPEG images. The estimated capacity is the upper bound of the amount of bits that can be embedded in JPEG image files without causing visible artifacts. The estimated capacity can be passed to the watermark embedding module as a reference. For case 2, since the new quantization table Q_n is unknown to the watermark embedding module, the problem is similar to embedding a watermark against JPEG attack. As most quantization tables in JPEG encoders are obtained by scaling a reference quantization table (most probably the default quantization table recommended in the JPEG standard) with a QF, the typical Q_n corresponding to different QFs and the reference quantization table can be derived in J2J. For case 2, our proposed algorithm in Section II can be used to estimate the data hiding capacity for a wide range of QF. The resulting capacity curve can be passed to the watermark embedding module as a reference. For cases 3 and 4, if the modification is done before watermarking insertion, our proposed algorithm in Section II can be used to estimate data hiding capacity. If the modification is done after the watermarking insertion, the modification should be treated as attacks leading to lower capacity.

II. WATERMARK CONCEPT

The block diagram of the digital watermark system is shown in Figure 1.

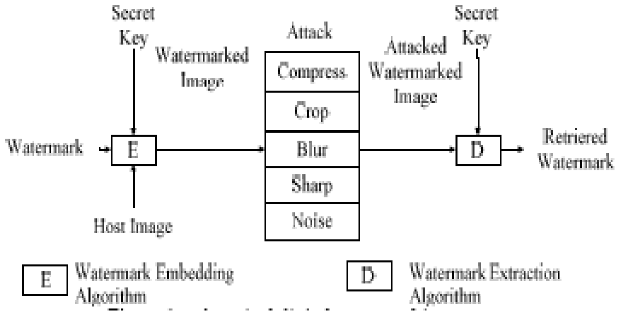


Figure 2. A typical digital watermarking system.

The methods for the imperceptible watermark technology can be broadly classified into two categories in the sense of embedding method: the spatial domain based and the transform domain based. Hiding the logo in the spatial domain is the simplest watermarking technique [36, 37] .The hidden information can be easily removed by users, or destroyed by JPEG compression. One robust way is to embed the logo into the middle frequency portion of the host image [35, 38].In those methods, some authors utilized the polarity information to modify the middle frequency coefficients [35] to achieve a robust approach. But the extraction procedure requires the watermark and the host image.

In this paper, a frequency domain scheme developed expressly for oblivious watermarking and signature process are presented. It uses the self-information of coefficients of the middle frequency in the host image, and explicitly takes in the cross-correlation between coefficients of the middle frequency and the watermark. and signature process that input is the edge properties extracted from the image. The signature can be correctly verified when the image is incidentally damaged such as lossy compression.

To achieve the robustness property, one will design the hiding mechanism according to the quantization algorithm of JPEG which is the most commonly used lossy compression standard. The overall block diagram of JPEG encoder and decoder is depicted in Figure 2

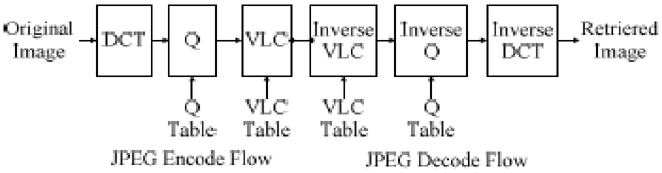


Figure 3. Block diagram of JPEG codec.

The DCT transforms image blocks from spatial domain to frequency domain. Let the block $b(u,v)$ denote the transformed coefficients. The quantization is performed by

$$b_q(u,v)=round(b(u,v)/Q(u,v))$$

The DCT transforms image blocks from spatial domain to frequency domain. Let the block $b(u,v)$ denote the transformed coefficients. The quantization is performed by

$$b_q(u,v)=round(b(u,v)/Q(u,v))$$

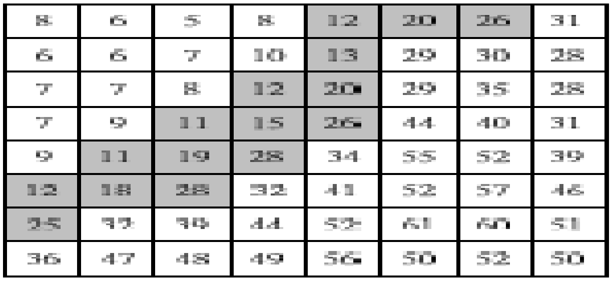
for $0 \le u,v < 8$ (1.1)

Where $Q(u,v)$ is the quantization table of size 8x8 . In the decoding process, the quantity $b^{\prime}(u,v)$ is retrieved from the de-quantization

$$b'(u,v)=b_q(u,v)\times Q(u,v)\ ,\ \text{for}\ \ 0\le u,v<8$$

(1.2)

The data loss of JPEG compression comes from the rounding operation in (1.1) and the retrieval in (1.2). There are two quantization tables for JPEG, one is the luminance table and the other is the chrominance table. An example of the luminance table is given in Figure 3.



8	6	5	8	12	20	26	31
6	6	7	10	13	29	30	28
7	7	8	12	20	29	35	28
7	9	11	15	26	44	40	31
9	11	19	28	34	55	52	39
12	18	28	32	41	52	57	46
25	35	38	44	52	61	60	51
36	47	48	49	56	50	52	50

Figure 4. Mid-frequency region chosen from JPEG quantization table for luminance.

It can be easily found from the quantization and de-quantization formula (1.1) and (1.2) that higher values of $Q(u,v)$ will produce more loss of $F(u,v)$ at the position (u,v) . Therefore if the information is hidden in high frequency region which divide higher quantization values, it will be easily erased by JPEG attack and if it is hidden in the low frequency region, the host image will be seriously damaged. Thus, in the proposed scheme, the information is hidden in the middle frequency region which is selected according to the values of $Q(u,v)$ as shown is Figure 3.

III. DIGITAL WATERMARKING IN JPEG

The main steps for JPEG are color space conversion and sampling, OCT and its inverse (IDCT), quantization, zigzag scanning, motion estimation, and entropy coding. A simpler approach is a single watermarking step in the compression framework because the computation requirements of watermarking are comparable to these steps. 3.1 Color Space Conversion

The color space conversion equations are as follows

$$\left.\begin{array}{rcl} Y & = & 0.299R+0.587G+0.114B, \\ C_b & = & 0.564(B-Y)+128, \\ C_r & = & 0.731(R-Y)+128. \end{array}\right\} \quad (3)$$

A. DCT or IDCT:

For ease of hardware implementation, we selected the fast DCT algorithm and its inverse [8]. The fast DCT algorithm reduces the number of adders and multipliers so that the evaluation of the DCT or IDCT coefficients is accelerated.

B. Quantization:

In the MPEG-4, a uniform scalar quantization is adopted. The feature of the scalar quantization scheme is an adaptive quantized step size according to the DCT coefficients. For computational efficiency and hardware simplification, scalar quantization step size is chosen from pre-defined tables.

C. Motion Estimation:

The criterion of match for two macro blocks is the minimized difference between them. For computational simplification, the sum of absolute difference (SAD) criterion is given as shown in the below equation

$$SAD(x,y)=\begin{cases} \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}|c(i,j)-p(i,j)|, (x,y)=(0,0), \\ \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}|c(i,j)-p(i+x,j+y)|\,. \end{cases} \quad (2)$$

D. Entropy Coding:

The entropy coding efficiency depends on the precision of calculating the probability of occurrence of each coefficient. The approach we followed is to utilize pre-calculated Huffman code tables for generic images.

IV. RESULTS ANALYSIS

We have presented here the input and output images and analysis of the experiment carried out i.e. figure 4a-4e. Results obtained clearly depict that the algorithm using blocking effect prediction model (BEP) has bettered the results as compared to early method by a significant multiplying factor.

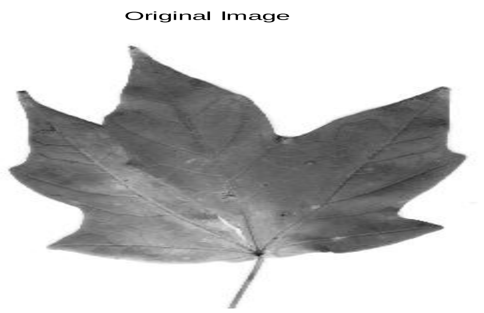


Figure 4a. Original Image

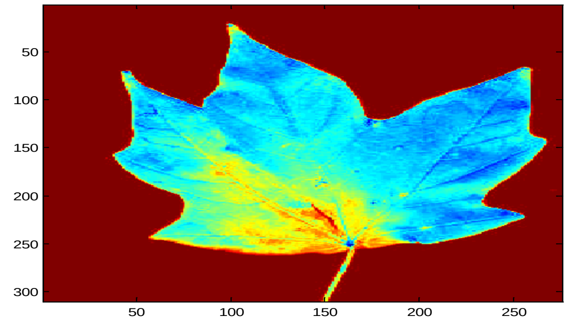


Figure 4b. Output Image

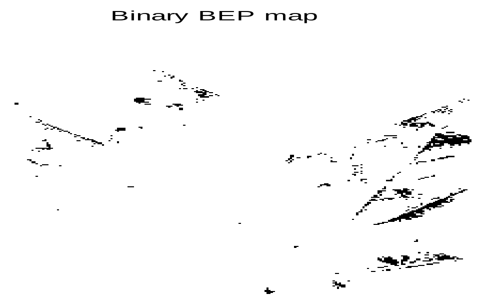


Figure 4c. Output Image

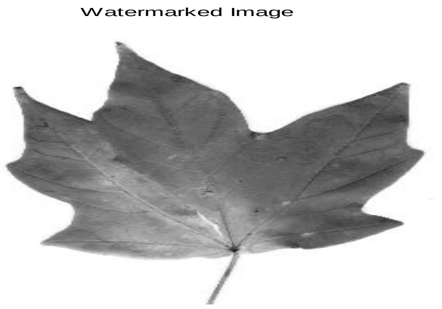


Figure 4d. Output Image

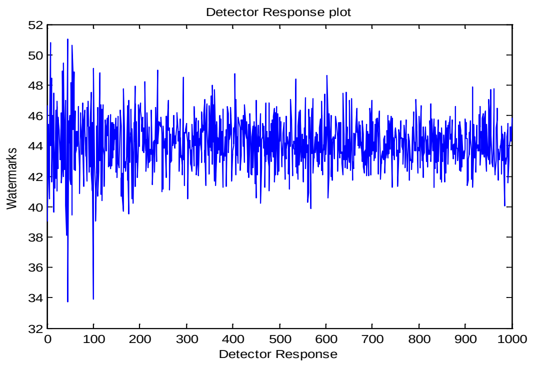


Figure 4e. Output Image

Table 1. Results of the experiment

Samples	Without BEP		With BEP	
	PSNR	SSIM	PSNR	SSIM
1	37.2	0.7	40.2	0.9
2	35.5	0.6	43.5	1
3	36.2	0.5	45.2	0.8
4	32.7	0.4	39.7	0.7

V. CONCLUSION

The paper presents a novel approach for robust watermarking to jpeg compression. The employed blocking effect prediction model (BEP) is simple and efficient by exploiting jpeg compression and learning process. The main idea of this article is to demonstrate the performance of a watermarking scheme when using BEP map to improve resistance against jpeg compression. The experimental results showed that the proposed method helps significantly to improve the watermark's transparency and it's robustness to jpeg compression. It is worth to notice that the proposed algorithm is quite flexible and can be exploited for other watermarking scheme resistant to block-based compression standards or for other block-based compression standards just by reloading the training phase when constructing the BEP map. As shown better perspective here using BEP model with a improved PSNR value as compared to conventional method.

VI. REFERENCES

[1]. T. Cover and J. Thomas, Elements of Information Theory. New York: Wiley, 1991.

[2]. F. Hartung, Digital Watermarking and Fingerprinting of Uncompressed and Compressed Video. Aachen, Germany: Shaker Verlag, 2000.

[3]. I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking. New York: Morgan Kaufmann, 2002.

[4]. A. B.Watson, “DCT quantization matrices optimized for individual images,” in Proc. SPIE Human Vision, Visual Processing, and Digital Display IV, 1993, pp. 202–216.

[5]. A. J. Ahumada and H. A. Peterson, “Luminance-model-based DCT quantization for color image compression,” in Proc. SPIE, vol. 1666, 1992, pp. 365–374.

[6]. M. Kutter and F. A. P. Petitcolas, “A fair benchmark for image watermarking systems,” in Proc. SPIE Security and Watermarking of Multimedia Contents, Jan. 1999, pp. 226–239.

[7]. C. E. Shannon, “A mathematical theory of communication,” Bell Syst. Tech. J., vol. 27, pp. 373–423 and 623–656, 1948.

[8]. M. Costa, “Writing on dirty paper,” IEEE Trans. Inform. Theory, vol. IT-29, pp. 439–441, May 1983.

[9]. I. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Trans. Image Processing, vol. 6, pp. 1673–1687, Dec. 1997.

[10]. M. Kutter, F. Jordan, and F. Bossen, “Digital signature of color images using amplitude modulation,” in Proc. SPIE Storage and Retrieval for Image and Video Databases, vol. 3022-5, Feb. 1997, pp. 518–552.

[11]. M. Kutter and F. A. P. Petitcolas, “A fair benchmark for image watermarking systems,” in Proc. SPIE Security and Watermarking of Multimedia Contents, vol. 3657, Jan. 1999, pp. 226–239.

[12]. J. J. Eggers and B. Girod, “Quantization effects on digital watermarks,” EURASIP Signal Processing, vol. 81, no. 2, pp. 239–263, 2001.

[13]. J. Fridrich, M. Goljan, and R. Du, “Steganalysis based on JPEG compatibility,” in Proc. SPIE Multimedia Systems and Applications IV, Aug. 2001, pp. 275–280.

[14]. Y. Choi and K. Aizawa, “Digital watermarking using inter-block correlation: extension to JPEG coded domain,” in Proc. IEEE Int. Conf. Information Technology: Coding and Computing, Mar. 2000, pp. 133–138.

[15]. W. Luo, G. L. Heileman, and C. E. Pizano, “Fast and robust watermarking of JPEG files,” in Proc. IEEE 5th Southwest Symp. Image Analysis and Interpretation, Apr. 2002, pp. 158–162.

[16]. P. H. W. Wong and O. C. Au, “Data hiding and watermarking in JPEG compressed domain by DC coefficient modification,” in Proc. SPIE Security and Watermarking of Multimedia Contents, vol. 3971, Jan. 2000, pp. 237–244.

[17]. “Data hiding technique in JPEG compressed domain,” in Proc. SPIE Security and Watermarking of Multimedia Contents, vol. 4314, Jan. 2001, pp. 309–320.

[18]. “A blind watermarking technique in JPEG compressed domain,” in Proc. IEEE Int. Conf. Image Processing, vol. 3, Sept. 2002, pp. 497–500.

[19]. S. D. Servetto, C. I. Podilchuk, and K. Ramchandran, “Capacity issues in digital image watermarking,” in Proc. IEEE Int. Conf. Image Processing, vol. 1, Oct. 1998, pp. 445–449.

[20]. M. Barni, F. Bartolini, A. D. Rosa, and A. Piva, “Capacity of the watermark channel: how many bits can be hidden within a digital images,” in Proc. SPIE Security and Watermarking of Multimedia Contents, vol. 3657, Jan. 1999, pp. 437–448.

[21]. “Capacity of full frame DCT image watermarks,” IEEE Trans. Image Processing, vol. 9, pp. 1450–1455, Aug. 2000.

[22]. P. Moulin and M. K. Mihçak, “A framework for evaluating the datahiding capacity of image sources,” IEEE Trans. Image Processing, vol. 9, pp. 1450–1455, Aug. 2000.

[23]. D. Kundur, “Implication for high capacity data hiding in the presence of lossy compression,” in Proc. IEEE Int. Conf. Information Technology: Coding and Computing, Mar. 2000, pp. 16–22.

[24]. C. Y. Lin and S. F. Chang, “Watermarking capacity of digital images based on domain-specific masking effects,” in Proc. IEEE Int. Conf. Information Technology: Coding and Computing, Apr. 2001, pp. 90–94.

[25]. C. Fei, D. Kundur, and R. Kwong, “The choice of watermark domain in the presence of compression,” in Proc. IEEE Int. Conf. Information Technology: Coding and Computing, Apr. 2001, pp. 79–84.

[26]. M. Ramkumar and A. N. Akansu, “Capacity estimates for data hiding in compressed images,” IEEE Trans. Image Processing, vol. 10, pp. 1252–1263, Aug. 2001.

[27]. R. Sugihara, “Practical capacity of digital watermark as constrained by reliability,” in Proc. IEEE Int. Conf. Information Technology: Coding and Computing, Apr. 2001, pp. 85–89.

[28]. Ç. Candan and N. Jayant, “A new interpretation of data hiding capacity,” in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, vol. 3, May 2001, pp. 1993–1996.

[29]. F. Pérez-González, J. R. Hernández, and F. Balado, “Approaching the capacity limit in image watermarking: a perspective on coding techniques for data hiding applications,” Elsevier Signal Processing, vol. 81, no. 6, pp. 1215–1238, June 2001.

[30]. A. S. Cohen and A. Lapidoth, “The gaussian watermarking game,” IEEE Trans. Inform. Theory, vol. 48, pp. 1639–1667, June 2002.

[31]. T. Kalker and F. M. J. Willems, “Capacity bounds and constructions for reversible data-hiding,” in Proc. IEEE Int. Conf. Digital Signal Processing, vol. 1, Jul. 2002, pp. 71–76.

[32]. J. Fridrich, M. Coljan, and R. Du, “Lossless data embedding—new paradigm in digital watermarking,” EURASIP J. Appl. Signal Processing— Special Issue on Emerging Applications of Multimedia Data Hiding, vol. 2002, no. 2, pp. 185–196, Feb. 2002.

[33]. S. Voloshynovskiy and T. Pun, “Capacity-security analysis of data hiding technologies,” in Proc. IEEE Int. Conf. Multimedia and Expo, vol. 2, Aug. 2002, pp. 477–480.

[34]. J. J. Eggers, R. Bäuml, R. Tzschoppe, and B. Girod. Scalar costa scheme for information embedding. IEEE Trans. Signal Processing [35] C. T. Hsu and J. L. Wu, “Hidden digital watermarks in images,” IEEE Trans. on Images Processing, 1999,pp. 58-68.

[35]. G. Voyatzis and I. Pitas, “Embedding robust watermarks by chaotic mixing,” in Proceedings of 13th International Conference on Digital Signal Processing (DSP'97), 1997, pp.213-216 .

[36]. M. Kutter, F. Jordan and F. Bossen, “Digital watermarking of color images using amplitude modulation,” Journal of Electronic Imaging, 1998,pp. 326 - 332.

[37]. A. Sinha, A. Das, and S. Pandith, “Pattern based robust digital watermarking scheme for images,” Acoustics, Speech, and Signal Processing, 2002 IEEE International Conference on, 2002, pp.3481-3484.

AUTHOR’S PROFILE

Venkata Giridhar Madabhaktula is pursuing M.Tech in Computer science and engineering from Jawaharlal Nehru Technological University, Kakinada, A.P., India. And B.Tech in computer Science and Engineering from Jawaharlal Nehru Technological university, kakinada A.P, India. He is a certified CCNA professional. His areas of research includes Image Processing and Data Mining.

Tammineni Ravikumar is M.Tech in Computer Science from Jawaharlal Nehru Technological University kakinada, A.P., India. And B.Tech in computer Science and Engineering from Jawaharlal Nehru Technological University Hyderabad, A.P. India. He is having 5 years of experience in teaching and presently working as Assistant Professor in the Department of Computer Science and Engineering at Aditya Institute of Technology and Management, Tekkali [AITAM], A.P, India**.** and His areas of research includes Image Processing, Data Mining, Web Technologies and Emerging Technologies.