Performance Analysis of Color Channel for DCT Based Image Watermarking Scheme

Vikas Saxena
Jaypee Institute of Information Technology University, Noida, India
vikas.saxena@jiit.ac.in

Paridhi Khemka
Jaypee Institute of Information Technology University, Noida, India
paridhi.khemka@gmail.com

Aditi Harsulkar
Jaypee Institute of Information Technology University, Noida, India
aditi8486@yahoo.co.in

JP Gupta
Jaypee Institute of Information Technology University, Noida, India
jp.gupta@jiit.ac.in

Abstract

Due to improvements in imaging technologies and the ease of digital contents creation and manipulation, today there is a pressing need for the copyright protection of digital contents. It is also essential to have techniques for authentication of the content as well as the owner. This paper examines the suitability of color channel to be used for hiding a monochromatic watermark in a 24 bit colored BMP image. This paper uses the scheme which is based on comparison of middle band DCT coefficients exchange scheme [13]-[14]. This paper also proposes a way to improve the robustness against JPEG attack. Experimental results show that proposed scheme is very robust against JPEG compression along various kinds of image processing attacks.

1. Introduction

In recent years the phenomenal growth of the Internet has highlighted the need for mechanisms to protect ownership of digital media. Exactly identical copies of digital information, be it images, text or audio, can be produced and distributed easily. Therefore to validate the claim of ownership, a proof is required which is provided by the recovery of watermark. A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity. Digital watermarking [3] is an extension of this concept in the digital world. It is a technique that provides a solution to the longstanding problems faced with copyrighting digital data. Digital watermarks are pieces of information added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data[3,4]. This information can be textual data about the author, its copyright, etc; or it can be an image itself.

There are two domains for digital image watermarking: Spatial Domain and Transform Domain. Spatial domain watermarking is a technique in which the watermark is embedded by directly modifying the pixel values. Least Significant Bit Substitution is a spatial domain technique. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. Extraction of the watermark is performed by extracting the least significant bit of each of the selected image pixels. If the extracted bits match the inserted bits, then the watermark is detected. This technique is not popular in digital world because it is not robust enough to resist some common attacks.

Transform domain watermarking is a technique in which the watermark is embedded in the transform domain e.g., DCT, DFT, DWT [6]. Watermarking Based on DCT Coefficient Modulation technique[5] embeds the watermark in the DCT domain to increase the robustness of the watermarking scheme against JPEG compression. The watermark bits are embedded in each 8x8 DCT block of the image. It is not wise to embed the watermark bits in the low frequency components of the DCT block, because these coefficients are subject to heavy quantization during JPEG compression [11]. Hence, it is better to embed the watermark in mid or high-frequency DCT components.

2. Preliminaries

Middle-band Coefficient Exchange algorithm [13]-[14]: This technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. FL is used to denote the lowest frequency components of the block; FH is used to denote the higher frequency components while FM is used to denote the middle frequency components. FM is chosen as the embedding region as to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image. Two locations $P_k(i1, j1)$ and $P_k(i2, j2)$ are chosen from the FM region for comparison. We choose the two locations such that they have identical JPEG quantization values as shown in Table 1. Due to this any scaling of one coefficient will scale the other by the same factor preserving their relative size.

Table 1. Quantization table

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

We observe that the locations (4, 1) and (3, 2) or (1, 2) and (2, 0) have identical values, therefore we choose them for comparison. The DCT block will encode a "1" if $P_k(i1, j1) > P_k(i2, j2)$; otherwise it will encode a "0". The coefficients are then swapped if the relative size of each coefficient does not agree with the bit that is to be encoded.

3. Proposed Scheme

We take four well known 24 bit colored test images of size 512*512 pixels. Test images used are lena.bmp, mandrill.bmp, monarch.bmp and pepper.bmp as shown in Fig (1). The watermark logo used is shown in Fig (2). We embedded the watermark in these images using the middle band coefficient exchange algorithm. To analyze the performance of RGB channels [8], we embedded the watermark separately in R, G and B channels.

Figure 1. Test Cover Images: Lena, Mandrill, Monarch and Pepper (Courtesy: Eric Van Bilson Audiovisuality: http://www.bilsen.com/)

Figure 2. Watermark Logo (80*40 bitmap image)

After watermark the images in all three color channels, we compress the watermarked images using JPEG compression at various JPEG quality factors. Our results indicate that if watermark is embedded in GREEN channel, recovery is better than other channels. This can be seen in Table 2. The recovered watermarks are shown in Figure 3.

It is clear from Table 2 and Figure 3 that for watermark embedding purpose, Green channel outperforms the Red and Blue color channel.

Now to further improve the quality of extracted watermark logo we are proposing the following steps:
We applied three "preprocessing" steps on the images as follows:

1. Take the 24-bit color image of size 512*512 pixels.
2. Equalize the histogram of Green channel of the image. [1, 2].
3. Embed the watermark in green channel using Middle-band coefficient exchange algorithm [1, 2].

To test our proposed scheme, we equalized the histogram of all three channels (R, G, B) and then watermark the image. Then we performed the following attacks on the watermarked images:

1. **JPEG Attack**: An image is compressed into a stream of bytes and decompressed back into an image. The compression method[12]is usually lossy compression, meaning that some visual quality is lost in the process.After this attack a 769 KB bitmap images is compressed to 27 KB(at low quality: Q=20). This shows that around 95% of data (including the watermark) is lost.
2. **Noise Attack**: Image noise is a random, usually unwanted, fluctuation of pixel values in an image.
3. **Histogram Equalization Attack** [1, 2]: This method usually increases the local contrast of many images, especially when the usable data of the image is represented by close contrast values. Through this adjustment, the intensities can be better distributed on the histogram.

Table-2 shows the results. It is found that if a colored image is HISTOGRAM EQUALIZED before embedding the watermark, recovery of watermark is better i.e. PSNR values are higher. Result also supports our schemes as performance of Green channel is again obvious. Increase in PSNR value of watermarking histogram equalized image is maximized if we equalized green channel.

Table 2. PSNR of Extracted watermark from JPEG compressed watermark test images

.	LENA.BMP				PEPPER.BMP			
JPEG Compression	**Q=20**	**Q=40**	**Q=60**	**Q=80**	**Q=20**	**Q=40**	**Q=60**	**Q=80**
RED	3.8138	5.86586	9.38713	13.737	4.44446	6.12934	11.3841	14.9055
GREEN	6.2285	10.8642	14.1634	17.8173	6.48408	10.3018	13.9941	15.7327
BLUE	3.78458	4.45904	7.00983	14.0586	4.0144	4.59762	7.27842	13.686
		MANDRILL.BMP				**MONARCH.BMP**		
JPEG Compression	**Q=20**	**Q=40**	**Q=60**	**Q=80**	**Q=20**	**Q=40**	**Q=60**	**Q=80**
RED	4.58561	6.09133	13.5342	17.9727	4.18767	6.06572	10.7443	15.4762
GREEN	7.3024	14.3188	18.4186	20.1702	4.88113	10.393	13.274	16.1883
BLUE	4.00899	4.72608	11.0469	17.8341	3.78916	4.38603	7.24002	13.9242

Red(psnr-5.86) **green(psnr-10.86)** **blue(psnr-4.45)**

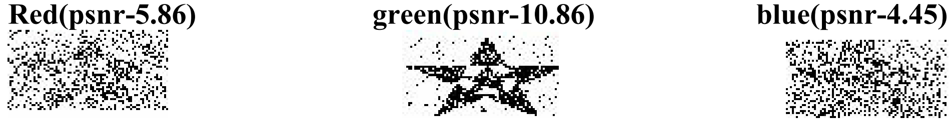


Figure 3. Recovered watermarks for lena.bmp after jpeg attack at Q=40.

Table 3. PSNR of extracted watermark from attacked watermarked test images.

		LENA.BMP			PEPPER.BMP		
Color Channel ↓	**Attack** →	**Jpeg Q20**	**Hist. Equ.**	**Noise (12.5%)**	**Jpeg Q20**	**Hist. Equ.**	**Noise (12.5%)**
RED	**original**	3.85853	15.5867	4.9277	3.89485	17.4944	6.87319
	equalized	4.7334	15.6074	5.13784	4.706	19.4657	7.05068
GREEN	**original**	6.2285	15.7285	5.25512	4.50915	14.7932	6.72312
	equalized	6.8358	18.7032	5.37656	6.9542	16.9559	7.69791
BLUE	**original**	3.78205	16.8769	4.96932	3.70676	15.503	6.7605
	equalized	4.1447	23.0387	5.41004	4.1985	18.6343	8.12838
		MANDRILL.BMP			**MONARCH.BMP**		
Color Channel ↓	**Attack** →	**Jpeg Q20**	**Hist. Equ.**	**Noise (12.5%)**	**Jpeg Q20**	**Hist. Equ.**	**Noise (12.5%)**

RED	**original**	4.58561	17.1942	8.9886		4.18767	16.9726	7.712
	equalized	5.2266	16.7228	9.36638		4.7169	18.1131	7.86498
GREEN	**original**	7.3024	17.4885	9.2963		4.88113	16.3554	7.65961
	equalized	11.1118	21.6698	9.81065		6.9542	21.0406	8.14772
BLUE	**original**	4.00899	16.7143	8.75787		3.78916	14.483	7.48674
	equalized	4.3586	18.3073	8.86063		4.3045	20.213	8.39899

4. Conclusion

This paper presents a study to analyze the suitability of color channel used to hide the watermark using the classical middle band coefficient exchange scheme for 24 bit color images. This paper also proposes a simple preprocessing for images so that watermarking scheme becomes more robust against JPEG compression and other common image manipulations. Further studies can be conducted to find out the suitability of color channel and preprocessing steps based on watermarking scheme and image characteristics.

5. References

[1] Vikas Saxena, J.P. Gupta, "Towards Increasing the Robustness of Image Watermarking Scheme Against Histogram Equalization Attack" (To be appear in the *Proceedings of IEEE 15th Signal Processing and Communication Applications Conference, 11-13 June 2007, Turkey)*

[2] Vikas Saxena, J.P. Gupta, "Collusion Attack Resistant Watermarking Scheme for Images Using DCT" (To be appear in the *Proceedings of IEEE 15th Signal Processing and Communication Applications Conference, 11-13 June 2007, Turkey)*

[3] N. Nikolaidis, I. Pitas," Digital Image Watermarking: an Overview", Department of informatics, University of Thessaloniki, Greece. http://poseidon.csd.auth.gr/signatures

[4] Adrian Perrig, Andrew Willmott, "Digital Image Watermarking in the Real World" Computer Science Department, Carnegie Mellon University. http://citeseer.ist.psu.edu/289264.html

[5] A. Piva M. Barni, F. Bartolini, V. Cappellini "DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image**".** Proceedings of the 1997 International Conference on Image Processing (ICIP '97) 3-Volume, Vol-1, http//portal.acm.org/citation.cfm?id=841631&dl=ACM&coll=portal

[6] H. I. Saleh, M. E. Elhadedy, M. A. Ashour, M. A. Aboelsaud, "Comparisons of dct based and dwt based watermarking schemes". http://icbmp.uaeu.ac.ae/Proceedings/PDFPAPERS/27_ICBMP.pdf

[7] Pei-Min Chen, Dept of Computer Science and IT, SooChow University, Taipei, Taiwan. "A Robust Digital Watermarking based on a statistic approach**"** Information Technology: Coding and Computing, 2000. Proceedings. International Conference on, pp 116-121,2000.

[8] Gael Chareyron and Alain Trémeau,”Watermarking of Color Images based on spectral modulation of viewing illuminant”, Laboratoire LIGIV EA 3070 - University Jean Monnet Site Carnot - 10, rue Barrouin 42000 Saint-Etienne – FRANCE.

[9] Narges Ahmidi, Reza Safabakhsh, “A Novel DCT-based Approach for Secure Color Image Watermarking”, *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on* **,** pp709- 713, Vol.2,April 2004.

[10] M. Arnold, M. Schmucker, and S. D. Wolthusen, “Techniques and application of Digital Watermarking and Content Protection”, Eds. Northwood, Artech House, 2003.

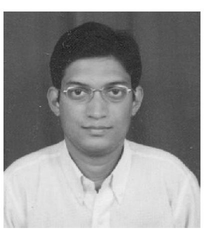
[11] Wenbin Luo, Gregory L. Heileman, Carlos E. Pizano, “Fast and Robust Watermarking of JPEG Files**”,** Image Analysis and Interpretation, 2002. Proceedings. Fifth IEEE Southwest Symposium on**,**pp 158-162, 2002.

[12] C.Y. Lin and S.F. Chang, “A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation”, IEEE Trans. on circuits and systems for video technology, vol. 11, no. 2, Feb. 2001, pp. 153-168.

[13] Z. Zhao, and E. koch, “Embedding Robust Labels Into Images For Copyright Protection*”, Proc. of International Congress on Intellectual Property Rights for Specialised Information, Knowledge and New Technologies*", Vienna, Austria, August 21-25,1995, pp. 242-251.

[14]N. Johnson, ,and S. Katezenbeisser, *“A Survey of Steganographic Techniques”*, Eds.Northwood, MA:ArtecHouse,43, 1999.

Authors



Vikas Saxena is a Ph.D. scholar in Jaypee Institute of Information Technology University, Noida, India. He received ME from VJTI Mumbai in 2001. He has more then 12 research publications in various international journals and reputed conferences. His area of interest is Computer Graphics, Image Processing and Software Engineering.

Aditi Harsulkar is a Final year graduate student in the department of Computer Science & Engineering in Jaypee Institute of Information Technology University, Noida, India. Her area of interest includes image processing and digital content security.

Paridhi Khemka is a Final year graduate student in the department of Computer Science & Engineering in Jaypee Institute of Information Technology University, Noida, India. Her area of interest includes image processing and digital content security.

Prof. J.P. Gupta is the Vice-Chancellor of Jaypee Institute of Information Technology University, Noida, India. Prof. Gupta obtained Master’s Degree in Electronics & Communication Engineering with the Gold Medal in 1973 from the University of Roorkee. He obtained his Doctorate Degree in Computer Engineering from the University of Westminster, London. He has held many coveted teaching and important administrative assignments. He held a position of Professor serving the University of Roorkee (now IIT, Roorkee) for over 25 years.