Collusion Attack Resistant Watermarking Scheme for Colored Images using DCT

Vikas Saxena, J.P Gupta

***Abstract*- Image watermarking with both insensible detection and high robustness capabilities is still a challenging problem for copyright protection up to now. This paper presents a new scheme for hiding a logo-based watermark in colored still image which is inherently collusion attack resistant. This scheme is based on averaging of middle frequency coefficients of block Discrete Cosine Transform (DCT) coefficients of an image. It is different from earlier schemes based on middle frequency coefficient by mean of high redundancy, to sustain malicious attacks. Experimental results show the robustness of the proposed scheme against the JPEG compression and other common image manipulations**.

***Index Terms*- Collusion attack, Discrete Cosine Transform (DCT), Image watermarking, JPEG compression.**

I. INTRODUCTION

With digital multimedia distribution over World Wide Web, authentications are more threatened than ever due to the possibility of unlimited copying. So, watermarking techniques are proposed for copyright protection or authentication of digital media.

Many watermarking methods for images have been proposed [1]- [4].

More and more researchers are joining this area and number of publications is increasing exponentially. Most of the work is based on ideas known from spread spectrum communication [5] which is additive embedding a pseudo-noise watermark pattern and watermark recovery by correlation [6]. Cox et al suggested using the DCT domain [6], which has been extensively studied because this is the transform used in JPEG compression. Further advantage of using DCT domain includes the fact that frequency transform is widely used in image and video compression and DCT coefficients affected by compression are well known.

This paper proposes an efficient use of middle-band coefficients exchange to hide the watermark data. This paper uses the idea of Middle Band Coefficient Exchange which was discussed by Koch and Zhao [8] and further explained by Johnson and Katezenbeisser [9]. Later Hsu and Wu also used the DCT based algorithm to implement the middle band embedding [10]. Further one more efficient collusion attack resistant scheme has been presented based on middle-band coefficients exchange [42].

Collusion attack is the severe problem for some applications of watermarking like fingerprinting which involve high financial implications. So while designing a watermark scheme we are taking this attack as a prime. [43]-[45]

Our main motivation behind selecting middle-band coefficients exchange scheme as a base is that this scheme has proven its robustness against those attacks which any how do not affect the perceptual quality of an image such as JPEG compression.

Section 2 discusses the background studies. Section 3 describes the proposed method and section 4 discusses the results.

II. PRELEMINARIES

Classical Middle-band based algorithm interchanges only one pair of coefficients and is quite robust against JPEG compression and common image manipulation operations but vulnerable to collusion attack.

A. Middle-band Coefficient Exchange Scheme

The middle-band frequencies coefficients (F_M) of an 8x8 DCT block are shown in Figure 1.

F_L is used to denote the lower frequency coefficients of the block, while F_H is used to denote the higher frequency coefficients. F_M is chosen as embedding region to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image. First we take 8x8 DCT of original image. Then two locations DCT (u_1, v_1) and DCT (u_2, v_2) are chosen from the F_M region for comparison of each 8x8 block. We should select the coefficients based on the recommended JPEG quantization table shown as Table-I. If two locations are chosen such that they have identical quantization values in JPEG quantization table, then any scaling of one coefficient will scale the other by the same factor to preserve their relative strength. Based on Table-I, we observe those coefficients at location (4, 1) and (3, 2) or (1, 2) and (3, 0) are more suitable candidates for comparison because their quantization values are equal. The DCT block will encode a "1" if DCT (u_1, v1) > DCT (u_2, v2); otherwise it will encode a "0".

Manuscript received February 15, 2007. This work is a part of a doctoral degree under the Jaypee Institute of Information Technology University, Noida, India

Vikas Saxena is Senior Lecturer in CSE & IT Department Jaypee Institute of Information Technology University, Noida, India (phone: +91-120-2400974-326; fax: +91-120-2400976; e-mail: vikas. saxena@jiit. ac. in)

J. P. Gupta is vice chancellor of Jaypee Institute of Information Technology University, Noida, India (e-mail: jp. gupta@jiit. ac. in)

So, instead of embedding any data, this scheme is hiding watermark data by means of interpreting "0" or "1" with relative values of 2 fixed locations in F_M region.

The coefficients are swapped if the relative size of each coefficient does not agree with the bit that is to be encoded [8] [9].

Swapping of such coefficients will not alter the watermarked image significantly, as it is generally believed that DCT coefficients of middle frequencies have similar magnitudes. Further, we can improve the robustness of the watermark by introducing a watermark "strength" constant *k*, such that DCT (u_1, v_1) − DCT $(u_2, v_2) > k$. If coefficients do not meet these criteria, we modify by the use of random noise to then satisfy the relation. Increasing *k* thus reduces the chance of detection errors at the expense of additional image degradation [8] [9]. Purpose is that larger coefficients should remain larger even after lot of compression because their relative values decide the decoding of the watermark data.

While extracting the watermark, we again take the 8x8 DCT of image, decode a "1" if DCT $(u_1, v1)$ > DCT $(u_2, v2)$; otherwise it will decode a "0" to form the watermark.

B. Limitation of Middle-Band Coefficient Exchange Scheme

Experimental results show that Middle-Band Coefficient Exchange is quite efficient against JPEG compression, Cropping, Noising and other common image manipulation operations. But above scheme has one serious drawback. If only one pair of coefficient is used (say (4, 1) and (3, 2)) to hide the watermark data then it is vulnerable to collusion attack. By analyzing 4 -5 watermarked copies of image, one can easily find out that these coefficients always have a certain pattern and attacker can predict the watermark as well as destroy it.

C. Why Collusion Attack should be Considered

If attacker has access to more then one copy of watermarked image, he/she can predict/ remove the watermark data by colluding them.

Fingerprinting is the well known watermarking application area. Researchers working on this particular area should primarily focus on the "collusion attack". Even Network Technology research Center claims on their website that they pay at least equal attention to watermark attacks/counter-attacks as watermark designs[43]. To facilitate pirate tracing in video distribution applications, different watermarks carrying distinguishing client information are embedded at source. If a few clients requesting for the same source data get their differently marked versions together, they may collude to remove or weaken the watermark leading to what is commonly called "collusion attack".

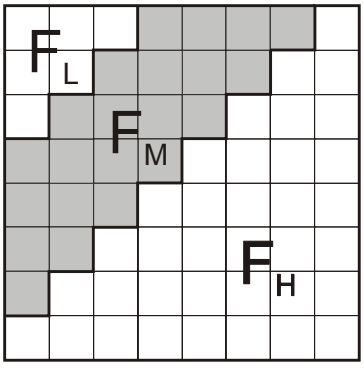

Figure 1: Frequency regions in 8x8 DCT

Table-I: JPEG 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

Collusion attacks are powerful attacks because they are capable of achieving their objective without causing much degradation in visual quality of the attacked data (sometimes, visual quality may even improve after attack.).

In their paper "Multi-bits Fingerprinting for Image", authors focused on collusion attack for fingerprinting application [44]. They states that the main difference between watermarking and fingerprinting is that different copies for each customer can be produced. This point is very helpful for attackers. Attackers compare several fingerprinting copies and find the location of the embedded information and destroy it by altering the values in those places where a difference was detected.

One more work, specially conducted against collusion attack can be found as "Collusion-resistant watermarking and fingerprinting (US Patent Issued on June 13, 2006)" [45].

D. Collusion attack resistant Scheme.

In [42], authors have presented one simple extension of classical middle band coefficient exchange scheme to make it collusion attack resistant by swapping 4 pairs of middle band coefficients instead of one pair along with correlation with low frequency coefficients. Results are promising. But this scheme covers only gray level images and if we compress the watermarked image using JPEG compression with quality factor less then 20, then watermark data starts disappearing.

III. Proposed Scheme

Proposed watermarking scheme is defined as 6-tuple (X, W, P, G, E, D):

1. X denotes the set of instances of a single colored image (Xi, $0 \le i \le N$ of size M1xM2 which has to be protected), as we will

watermark the image every time differently to sustain collusion attack.
2. W denotes the monochrome watermark logo of size L1xL2;
3. P denotes the set of policies Pi , $0 \le i \le N$; where each Pi is the set of 4 coefficients from F_M region of any of R,G or B color channel. (each Xi will have a unique Pi associated with it)
4. G denotes policy generator algorithm
G: DCT (Xi) →Pi;
5. E denotes the watermark embedding algorithm
E: Xi x W x Pi →Xi';
where Xi' is watermarked image.
6. D denotes the watermark detection algorithm
D: Xi' x Pi→ W';
Where W' represents extracted watermark.

While watermarking, we watermark each copy of image differently. There are 22 middle band coefficients in 8x8 DCT. By saying "Policy" we mean that for every copy of image, along with the average of middle band coefficients, there will be 4 unique middle band coefficients as well as color channel used to hide the watermark. So for every copy of image, those 4 coefficients will vary. This is what we call Pi for each Xi.. To generate Pi, we are simply selecting 4 coefficients randomly out of 22 coefficients lying in middle frequency band of 8x8 DCT and taking the average of rest 18 coefficients. **Then we hide the watermark data by using the relative value between this 'average' and chosen 4 coefficients**. So, we can watermark $^{22}C_4$=7315 copies of a single image such that no two watermark images have same policy of watermark (even if we use the same color channel to hide the watermark for every copy of the image). One such policy, which we are using in our experiments, is

P i={(5,1), (4,2), (6,3) and (5,4)} in Blue channel.

While embedding, we convert W into a string of "1"s and "0"s. Each 8x8 DCT block of Xi will hide one bit of W four times.

A. Policy Generator(G):

First we take 8x8 DCT of the input image. Then we randomly select any 4 coefficients out of 22 coefficients for each copy of image to be watermarked from one of the R, G or B color channel.

B. Embedding algorithm(E):

Each 8x8 block of image is used to hide 1 bit of watermark logo. We take a monochrome image as a logo which can be interpreted as a 1D-array of "1" and "0".

Our embedding algorithm is based on averaging the coefficients of F_M region. We can fight against collusion attack by swapping more then one pair as discussed in [42] but if attacker is ready to loose some quality, he/she can disturb all the coefficients in F_M region. Therefore, even if we introduce redundancy with randomness, our watermark data may still be attacked. So we are proposing that attacker can not alter the "average" of coefficients of F_M region badly as it will heavily impact the quality of image. So, we are hiding "1" or "0" by the relative values of 4 coefficients with the average of coefficients of F_M region and along with this we are introducing randomness and redundancy so that our scheme can guarantees the robustness against collusion attack.

Embedding algorithm steps are:

1) Convert monochromatic watermark W into a string of "1"s and "0"s;
2) Take 8x8 DCT of cover image Xi;
3) Generate Pi (i.e. choose one color channel and then randomly select any 4 coefficients from F_M region of its block DCT);
4) For each block repeat step 5 to 7;
5) Calculate the average "Av" of remaining 18 middle band coefficients (Unlike classical scheme which swap one pair of middle band coefficient, we are taking 4 coefficients and each is compared with the average.);

//Now like classical middle band scheme, relative size between average Av and chosen 4 coefficients in step 3 will interpret "0" or "1" of watermark data.//

6) *a)Hide "0"*: For all 4 chosen coefficients in step 3, assign the value of coefficients which is 'T' less then the average

b) *Hide "1":* For all 4 chosen coefficients in step 3, assign the value of coefficients which is 'T' greater then the average; and

//Here 'T' indicates the strength of watermark analogous to 'k' discussed in section 2.1//

7) Take IDCT to reconstruct the watermarked image Xi'.

C: Watermark detection algorithm (D):

Watermark extraction is reverse procedure of watermark embedding. To extract the watermark from the watermarked image, we calculate average "Av" in same way as in embedding algorithm. Owner should have a record of all policies used to watermark the image. Based on "policies"; owner of the image can recover watermark using following rule:

1) If at least 1 out of 4 chosen coefficients are less then average, *Interpret "0"and;*
2) If at least 1 out of 4 chosen coefficients are greater then average, *interpret "1".*

So, even if values of few coefficient of F_M region alter because of DCT and IDCT, we can decode "1" or "0" based on single coefficient.

IV. Results

We have tested our scheme on 3 test images lena, mandrill and pepper of size 512x512 in Windows 24 bit BMP format.

Figure 2: Test images of lena, mandrill & pepper.
(Courtesy: Eric Van Bilson Audiovisuality, http://www.bilsen.com/)

As discussed in Section 3.2 we can decide the watermark strength by setting a parameter 'T'. By increasing the value of 'T' we can make our watermark more detectible but in that case original image will degrade more. Our experiments suggest that T=150 is the optimum value for 'T' in image imperceptibility versus robustness tradeoff.

We are using "Blue" color channel to hide the watermark data. Bossen et al.[46] have stated that the watermarks should he embedded mainly in the blue color channel of an image. The human eye is least sensitive to change in blue channel. But it is found that suitability of color channel to be used is dependent on the image itself. Here we suggest that the color channel which should be used can be found on the basis of the amount of the color present in the image or on the basis of histogram of each color channel (i.e. color with spreader histogram should be given priority).

When we are hiding the watermark in the test images using T=150, there is no loss in the perceptual quality of the images. Figure 4 shows the extracted watermark from watermarked copy of lena, mandrill and pepper at T = 150 which is not attacked or manipulated at all.

All results are found using MATLAB and all image manipulation are done using Adobe Photoshop. To measure the quality, we are using Peak Signal to Noise Ration (PSNR).

A. Robustness against Collusion attack

We design a scheme which is inherently collusion attack resistant. As every watermark copy will have the different "policy", attacker can not predict the watermark location and watermark data by colluding many copies of watermark image. Owner (watermark embedder) always has a record of different policies used to embed the watermark and can always extract the watermark data by supplying different policies while extracting a watermark from attacked watermark image.

So after ensuring that our scheme is collusion attack resistant, we now need to check that our proposed scheme is robust against known attacks and common image manipulations as follows:

B. Performance against JPEG Compression

We applied JPEG compression on watermarked image (generated by keeping T=150) with different quality parameters.

Table-II summarizes the PSNR of extracted watermark after JPEG compression. It is clear from Table-II that even if at Q=20, quality of extracted watermark is very fine and logo is quite detectible.

C. Performance against common image manipulations

We have conducted following image manipulations to watermarked test images and extract the watermark:
Attack-1: Equalize the Histogram.
Attack-2: Apply uniform scaling (Zoom).
.

Figure 3. Watermark logo used

Table-II:PSNR of extracted watermark after JPEG compression

Quality factor	PSNR(DB)		
	Lena Watermarked with T=150	Mandrill Watermarked with T=150	Pepper Watermarked with T=150
Q=80	39.9987	37.0185	39.9987
Q=60	39.9987	34.98135	39.9987
Q=40	24.57225	14.51025	25.20285
Q=20	21.92385	12.26715	21.3678

Table -III: PSNR of extracted watermark logo from watermarked test images after attacks

	PSNR (DB)					
	Histogram Equalization	Zoom	Brightness-Contrast Adjustment	Hue-Saturation	Gaussian Noise	Gaussian Blur
Lena	34.67	34.67	34.67	34.67	34.67	34.67
Mandrill	28.06	28.04	28.04	28.04	28.04	28.04
Pepper	32.25	32.07	30.78	32.48	31.78	31.10

Figure 4: Extracted watermark from watermarked lena, mandrill and pepper images respectively at T=150.

Attack-3: Adjust the brightness to +40 and contrast to +25
Attack-4: Adjust the hue and saturation to +10 each.
Attack-5: Add 10 % Gaussian noise.
Attack-6: Blur the image using Gaussian blur with 1 pixel radius.

Our proposed scheme sustained all the attacks and quality of extracted watermark logos is very fine. Table-III summarizes the PSNR of extracted logo from all test images. We are also showing the recovered logos. It is clear that recovered logos are quite detectible. Figure 5 shows the recovered logos from attacked images.

V. COMPARATIVE STUDY

We have compared our scheme against JPEG compression with other similar methodologies which are well known for their robustness against JPEG compressions. We are giving a brief description of those methodologies. We have purposely selected these methodologies for comparison because all these

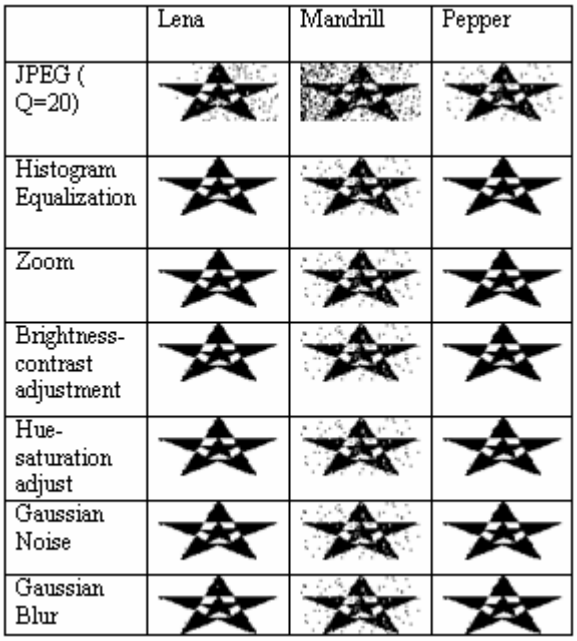

Figure 5: Recovered logos from attacked images

schemes and our proposed one are similar in nature. We re-implemented the following schemes as they were not originally for colored images. We have made the following scheme for watermarking the colored images and hide the data in BLUE channel.

A. Scheme-A (Correlation based Techniques)

The most straightforward way to add a watermark to an image is to add a pseudorandom noise pattern to the luminance values of its pixels. Many methods based on this principle have been suggested by researchers [11-27]. A pseudo-random noise (PN) pattern W(x, y) is added to the cover image I(x, y), according to the equation shown below in Equation 1.

$$I_w(x,y) = I(x,y) + k * W(x,y) \qquad (1)$$

In Equation 1, k denotes a gain factor, and I_W the resulting watermarked image. Increasing k increases the robustness of the watermark at the expense of the quality of the watermarked image.

To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and possibly watermarked image computed. If the correlation exceeds a certain threshold T, the watermark is detected, and a single bit is set. This method can easily be extended to a multiple-bit watermark by dividing the image up into blocks, and performing the above procedure independently on each block. For comparison purpose, we name this scheme as Scheme-A.

B. Scheme-B (The Classical Middle Band coefficient exchange schema)

As original scheme is for gray level image, we have converted it to watermark the colored image in blue channel

Table-IV : PSNR of extracted logo from highly compressed watermark test images using various schemes.

Schemes	JPEG Quality Factors	PSNR (DB)		
		Lena	Mandrill	Pepper
Scheme-A	Q=15	8.723	7.89	8.12
	Q=10	7.67	7.12	7.988
	Q=05	4.5	4.324	4.657
Scheme-B	Q=15	4.222	4.587	3.987
	Q=10	3.45	3.87	3.95
	Q=05	2.32	2.2	1.97
Scheme-C	Q=15	4.323	4.565	4.33
	Q=10	4.11	4.249	4.12
	Q=05	2.234	2.229	2.1
Scheme-D	Q=15	16.305	10.845	13.335
	Q=10	15.585	10.62	12.885
	Q=05	14.13	10.29	11.4

by keeping the main idea of this scheme intact. We are naming this scheme as Scheme-B

C. Scheme-C

Scheme proposed in [42] is also based on middle band coefficient exchange scheme and collusion attack resistant. This scheme swaps 4 pairs of coefficients in FM region in correlation with low band coefficients. We are naming this scheme as Scheme-C

We are naming our proposed scheme as **Scheme-D**

D. Comparative study results

We found that all the above schemes are robust against JPEG compression attack but if we compress the watermark images by low quality factors (less then Q=20), our proposed scheme outperforms the other schemes discussed above. We compressed the watermarked test images by keeping JPEG compression quality factor Q=15, 10, and 5. No scheme other than the proposed one was able to extract the watermark logo which is detectible.

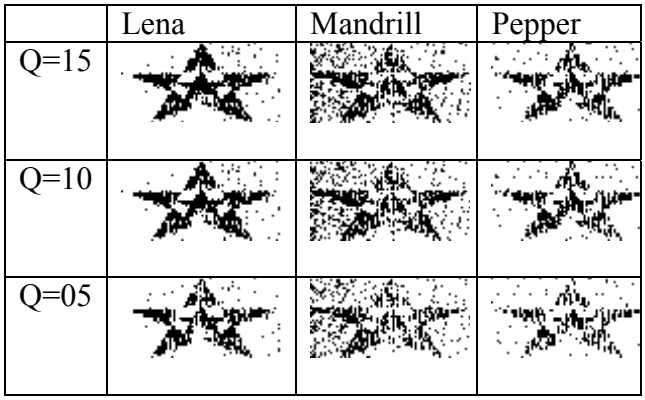

Figure 6: Extracted logo using proposed scheme from high JPEG compressed watermarked test images.

Table-IV summarizes the PSNR of extracted logo from highly compressed watermark test images using various schemes. Figure 6 shows the recovered watermark logos using our proposed scheme from highly compressed watermarked images.

Therefore, our scheme is not only inherently collusion attack resistant but also enhances the performance. Results indicate that proposed scheme recovers the watermark even from an attacked image which is compressed up to Q=5 quality factor of JPEG (i.e. after 95-99% size reduction). In addition to this, the proposed scheme is resisting common image manipulations like cropping, scaling, flipping, histogram equalization, brightness- contrast adjustment, Hue-saturation alteration, Gaussian noise and Gaussian blur

V. Conclusion

This paper presents a scheme for image watermarking based on average of middle-band coefficients of DCT domain. Experimental results prove that proposed scheme is robust against collusion attack as well as outperforms other schemes against JPEG compression. It also sustains the common image manipulations. Further research may be conducted on the suitability of color channel based on image characteristics itself.

Acknowledgment

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views if the Jaypee Institute of Information Technology University. We would like to thank the Jaypee Institute of Information Technology University to provide the opportunity to do research. In particular, Vikas Saxena would like to thank Dr. Y. Medury , Prof Ashok Subramanyam, Prof S.L. Maskara, and Prof. Sanjay Goel for providing the valuable guidelines.

References

[1 F.Hartung, and M. Kutter, "Multimedia Watermarking techniques", *Proceddings of IEEE,* Vol. 87, No 7, July 1999, pp. 1079-1107.

[2] M. Arnold, M. Schmucker, and S.D. Wolthusen, "*Techniques and application of Digital Watermarking and Content Protection*", Eds.Northwood ,Artech House, 2003.

[3] Saraju P. Mohanty , "*Digital Watermarking: A Tutorial Review"*, URL: http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999 Mohanty.pdf http://citeseer.ist.psu.edu/mohanty99digital.htm

[4] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. "Techniques for data hiding". *IBM Systems Journal*, Vol. 35.(3/4), 1996, pp. 313-336.

[5] P.G.Flikkema, "Spread Spectrum techniques for wireless communication*", IEEE Signal Processing 14*, pp. 26-36, May 1997.

[6] I.J. Cox, J.Kilian, T.Leighton and T. Shamoon, *"Secure Spread Spectrum watermarking for Multimedia," IEEE Tras. on Image Processing ,* Vol. 6,No12, 1997, pp. 1673-1687.

[7] P. Meerwald, and A.Uhl, "A Survey of Wavelet-Domain Watermarking Algorithm," in P.W. Wong and E.J.Delp,(eds.), *Proceedings of Electronic Imaging 2001,Securityand Watermarking of Multimedia Contents III*, San Jose, CA, January 2001, pp. 505-515.

[8] 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.

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

[10] C.T.Hsu, and J.L.Wu*.,* "Hidden Singatures in Images", *Proc. IEEE International Conf. on Image Processing, ICIP-96*, Vol.3, pp.223-226.

[11] G Langelaar et.al. "Watermarking Digital Image and Video Data: A State-of-art Overview",IEEE Signal Processing Magzine, September 2000, pp 20-46

[12] W. Bender, D. Gruhl, and N. Morimoto, Techniques for data hiding," in *Proc. SPIE, Storage and Retrieval or Image and Video Databases III*, vol.2420, San Jose, CA, Feb. 9-10, 1995, pp. 165-173.

[13] G. Caronni, "Assuring ownership rights for digital images," in *Proc. Reliable IT Systems, VIS '95,* ermany, 1995, pp. 251-263.

[14] J. Fridrich, "Robust bit extraction from images," in *Proc. IEEE ICMCS'99 Conf.*, Florence, Italy, June 7-11, 1999.

[15] A. Hanjalic, G.C. Langelaar, P.M.B. van Roosmalen, J. Biemond, and R.L. Lagendijk, *Image and Video Databases: Restoration, Watermarking and Retrieval* (Advances in Image Communications, vol. 8). New York: Elsevier Science, 2000.

[16] F. Hartung and B. Girod, "Digital watermarking of raw and compressed video," in *Proc. SPIE 2952: Digital Compression Technologies and Systems for Video Communication*, Oct. 1996, pp. 205-213.

[17] T. Kalker, G. Depovere, J. Haitsma, and M. Maes, "A video watermarking system for broadcast monitoring," in *Proc. SPIE Electronic Imaging '99, Security and Watermarking of Multimedia Contents,* San Jose, CA, Jan. 1999, pp. 103-112.

[18] G.C. Langelaar, J.C.A. van der Lubbe, and R.L. Lagendijk, "Robust labeling methods for copy protection of images," in *Proc. SPIE Electronic Imaging '97, Storage and Retrieval for Image and Video Databases V*, San Jose, CA, Feb. 1997, pp. 298-309.

[19] I. Pitas and T.H. Kaskalis, "Applying signatures on digital images," in *Proc. IEEE Workshop on Nonlinear Signal and Image Processing*, Neos Marmaras, Thessaloniki, Greece, June 20-22, 1995, pp. 460-463.

[20] I. Pitas, "A method for signature casting on digital images," in *Proc. ICIP-96*, *IEEE Int. Conf. Image Processing*, vol. III, Lausanne, Switzerland, Sept. 15-17, 1996, pp. 215-218.

[21] R.G. van Schyndel, A.Z. Tirkel, and C.F. Osborne, "A digital watermark," in *Proc. IEEE Int. Conf. Image Processing*, vol. 2, Austin, TX, Nov. 1994, pp. 86-90.

[22] J.R. Smith and B.O. Comiskey, "Modulation and information hiding in images," in *Preproc. Information Hiding*, University of Cambridge, U.K., May 1996.

[23] R.B. Wolfgang and E.J. Delp, "A watermark for digital images," in *Proc.IEEE Int. Conf. Image Processing*, vol. III, Sept. 16-19, 1996, Lausanne, Switzerland, pp. 219-222.

[24] R.B. Wolfgang and E.J. Delp, "A watermarking technique for digital imagery: Further studies," in *Proc. Int. Conf. Imaging Science, Systems, and Technology,* Las Vegas, NV, June 30-July 3, 1997.

[25] R.B. Wolfgang and E.J. Delp, "Overview of image security techniques with applications in multimedia systems," in *Proc. SPIE Conf. Multimedia Networks: Security, Displays, Terminals, and Gateways,* vol. 3228, Dallas, TX, Nov. 2-5, 1997, pp. 297-308.

[26] R.B. Wolfgang and E.J. Delp, "Fragile watermarking using the VW2D watermark" in *Proc. Electronic Imaging '99*, vol. 3657, San Jose, CA, Jan. 25-27, 1999, pp. 204-213.

[27] W. Zeng and B. Liu, "On resolving rightful ownerships of digital images by invisible watermarks," in *Proc. ICIP 97*, *IEEE Int. Conf. Image Processing*, Santa Barbara, CA, Oct. 1997, pp. 552-555.

[28] F.M. Boland, J.J.K. Ó Ruanaidh, and C. Dautzenberg, "Watermarking digital images for copyright protection," in *Proc. IEE Int. Conf. on Image Processing and Its Applications*, Edinburgh, U.K., July 1995, pp. 326-330.

[29] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," NEC Res. Insti., Princeton, NJ, Tech. Rep. 95-10, 1995.

[30] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "A secure, robust watermark for multimedia," in *Preproc. Information Hiding*, Univ. of Cambridge, U.K., May 1996.

[31] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," in *Proc. 1996 Int. Conf. Image Processing*, vol. 3, Lausanne, Switzerland, Sept. 16-19, 1996, pp. 243-246.

[32] C.-T. Hsu and J.-L. Wu, "Hidden signatures in images," in *Proc. ICIP-96*, *IEEE Int. Conf. Image Processing*, vol. III, Lausanne, Switzerland, Sept. 16-19, 1996, pp. 223-226.

[33] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "DCT-based watermark recovering without resorting to the uncorrupted original image," in *Proc. ICIP 97, IEEE Int. Conf. Image Processing,*, Santa Barbara, CA, Oct. 1997, pp. 520-527.

[34] C. Podilchuk and W. Zeng, "Perceptual watermarking of still images," in *Proc. 1997 IEEE 1st Workshop Multimedia Signal Processing*, Princeton, NJ, June 23-25, 1997, pp. 363-368.

[35] J.J.K. Ó Ruanaidh, W.J. Dowling, and F.M. Boland, "Watermarking digital images for copyright protection," *Proc. Inst. Elec. Eng. Vision, Image, and Signal Processing*, vol. 143, no. 4, pp. 250-256, Aug. 1996.

[36] S. Rupley, "What's holding up DVD?" *PC Mag.*, vol. 15, no. 20, pp. 34, Nov. 19, 1996.

[37] R.B. Wolfgang, C.I. Podilchuk, and E.J. Delp, "Perceptual watermarks for digital images and video," *Proc. IEEE*, vol. 87, pp. 1108-1126, July 1999.

[38] M. Barni, F. Bartolini, V. Cappellini, A. Lippi, and A. Piva, "A DWT-based technique for spatio-frequency masking of digital signatures," in *Proc. SPIE/IS&T Int. Conf. Security and Watermarking of Multimedia Contents*, vol. 3657, San Jose, CA, Jan. 25-27, 1999, pp. 31-39.

[39] F.M. Boland, J.J.K. Ó Ruanaidh, and C. Dautzenberg "Watermarking digital images for copyright protection," in *Proc. IEE Int. Conf. on Image Processing and Its Applications*, Edinburgh, U.K., July 1995, pp. 326-330.

[40] D. Kundur and D. Hatzinakos, "A robust digital image watermarking scheme using wavelet-based fusion," in *Proc. ICIP 97*, *IEEE Int. Conf. Image Processing*, Santa Barbara, CA, Oct. 1997, pp. 544-547.

[41] X.-G. Xia, C.G. Boncelet, and G.R. Arce, "A multiresolution watermark for digital images," in *Proc. ICIP 97*, *IEEE Int. Conf. Image Processing*, Santa Barbara, CA, Oct. 1997, pp. 548-551.

[42] 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)***

[43] Network Technology research Center, Nanyang Technological University, Singapore, http://www.ntu.edu.sg/ntrc/research.htm

[44] W. Kim, S.H. Lee, H.-W. Jang, and J. Kim, "Multi-bits Fingerprinting for Image" http://www.actapress.com/PaperInfo.aspx?PaperID=15683

[45] Collusion-resistant watermarking and fingerprinting,
US Patent Issued on June 13, 2006
http://www.patentstorm.us/patents/7062653.html

[46] F. Bossen M. Kutter, F. Jordan, "Digital signature of color images using amplihlde modulation," in Proc. *of SPlE storage and retrieval for image and video databases,* San lose, USA, vol. 3022-5, February *1997,* pp. 518-526.