International Journal of IT & Knowledge Management (ISSN: 0973-4414)
Volume 12 • Issue 1 pp. 82-87 June 2018 - Dec 2018 www.csjournals.com

Watermark based Image Authentication Based On DCT

Navpreet Kaur
Research Scholar, Department of Computer Science
JJT University, Jhunjhunu, Rajasthan, INDIA

Abstract: A watermark is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light (or when viewed by reflected light, atop a dark background), caused by thickness or density variations in the paper. Watermarking is a method to hide some information that is integrated with a multimedia object. The object may be any form of multimedia, such as image, audio, video, or text. Watermarking has many different applications, such as ownership evidence, fingerprinting, authentication and integrity verification, content labelling and protection, and usage control. The success of any watermarking scheme is determined by its performance against intentional and unintentional attacks. This paper presents a new scheme for embedding and authentication of a watermark in colored image based on averaging of middle frequency coefficients of block Discrete Cosine Transform (DCT) 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 attacks like Additive White Gaussian Noise (AWGN), Gain attack and Filtering Attack etc.
Keywords: Collusion attack, Discrete Cosine Transform (DCT).

1. INTRODUCTION

With the rapid development of information technology, security for the confidential information has become challenging issue today. 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.

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 [1] which is additive embedding a pseudo noise watermark pattern and watermark recovery by correlation [2]. Cox suggested using the DCT domain [2], 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.

One of the common attacks that we encounter is gain attack. The first solution against the gain attack decreases the security of the algorithm, since the malicious attacker can change either the watermark or the pilot signals. Besides, pilots are deterministic objects in the main signal and can be easily detected. Although the second and third approach keeps the security of the QIM algorithm, they cause high computational cost. Besides, the low robustness of AQIM against additive white Gaussian noise (AWGN) and the high peak to average power ratio (PAPR) of RDM algorithm which happens due to its momentarily large quantization step size are the main drawbacks that should be addressed. Thus, no approach has been presented so far that both proposes an optimal decoder and remains invariant to the gain attack.

This paper proposes an efficient use of middle-band coefficients exchange to embed the watermark data. This paper uses the idea of Middle Band Coefficient Exchange which was discussed by Koch and Zhao [3] and further explained by Johnson and Katezenbeisser [4]. Later Hsu and Wu also used the DCT based algorithm to implement the middle band embedding [5]. Further one more efficient collusion attack resistant scheme has been presented based on middle-band coefficients exchange [6]. 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. 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.

International Journal of IT & Knowledge Management (ISSN: 0973-4414)
Volume 12 • Issue 1 pp. 82-87 June 2018 - Dec 2018 www.csjournals.com

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.

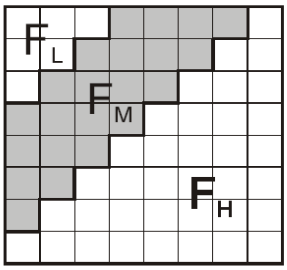

Figure 1: Frequency regions in 8x8 DCT

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 8 x 8 DCT of original image. Then two locations DCT (u1, v1) and DCT (u2, v2) 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 (u1, v1) > DCT (u2, v2); otherwise it will encode a "0".

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

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 FM region. The coefficients are swapped if the relative size of each coefficient does not agree with the bit that is to be encoded [3] [4].

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 (u1, v1) – DCT (u2, v2) > *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. 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 (u1, v1) > DCT (u2, v2); otherwise it will decode a "0" to form the watermark.

B. Why Collusion Attack should be considered

If attacker has access to more than 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". 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".

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.).

C. Collusion attack resistant Scheme.

So many 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.

D. Limitation of Middle-Band Coefficient Exchange Scheme

Previous Experimental results show that Middle-Band Coefficient Exchange is quite efficient against JPEG compression, Cropping, Noising and other common image manipulation operations. 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.

2. LITERATURE SERVEY

Digital watermarking embeds information within a digital work as a part of the media. Watermarking techniques falls into three categories of Robust, Semi fragile and fragile methods according to their specific applications. Robust watermarking mainly serves for identification purposes while the fragile and semi fragile watermarking are usually employed in authentication applications.

Since a good watermarking scheme should always be able to deal with some kinds of attacks, studies in the watermarking research area mostly target robust watermarking problems. Several robust watermarking techniques have been proposed so far. Cox [2] has proposed an additive watermarking approach based on Spread Spectrum concept which remains highly robust against Noise and Cropping attacks. Several other studies have improved this approach further [7]-[10]. Based on the observation that boosting the water marking power increases the barrier against attacks, most of the effective watermarking schemes tries to match the characteristics of the watermark to those of the image asset.

Multiplicative watermarking has been widely studied later on using local optimum decoders in Multi-resolution Transform domains such as Wavelet and Contourlet domains [11]–[16]. Besides, a universal optimal detector for scaling based watermarking schemes is presented in [17]. These schemes are highly robust against Noise and Compression attacks. To satisfy robustness against Geometric attacks and reduce the watermark synchronization problem, Tang and Hang [18] proposed a watermarking scheme which employs a feature extraction and image normalization approach.

Based on Log Polar Mapping (LPM) and phase correlation, Zheng et al. [19] proposed an image watermarking technique which embeds the watermark into the LPMs of the image Fourier magnitude spectrum. This scheme is invariant to rotation and remains comparatively robust to scaling attack.

One of the common but effective attacks in watermarking systems is Volumetric Distortions (i.e., any kind of amplitude scaling or Gamma Compensation). For image signals, it may happen due to the scanning process where light is not distributed uniformly over the paper.

This simple attack is the main drawback of most recent studies and even the quantization index modulation (QIM) algorithm [20] which has attained great popularity due to its lossless performance with lattice-based codebooks. Three types of solutions can tackle this problem, especially for the QIM method:

1) adopting auxiliary pilots through the watermarked signal known at both the encoder and decoder [21];
2) using spherical codewords [22] with correlator decoders [23] or using angle QIM (AQIM) [24-25];
3) introducing a domain in which the embedding process is invariant to the gain attack [26].

Some improvement/generalization on this scheme which is referred to as rational dither modulation (RDM) are proposed in [27– 28].

IJITKM 0973-4414
International Journal of IT & Knowledge Management (ISSN: 0973-4414)
Volume 12 • Issue 1 pp. 82-87 June 2018 - Dec 2018 www.csjournals.com

3. PROPOSED SCHEME

The proposed Scheme is based on the following modules;

A. Image as input :

We give image as input; process an image in 2x2 pixel blocks. This allows flexibility in tracking the edges and also achieves high computational complexity.

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

1. X denotes the set of instances of an 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 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 FM 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.

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 embed 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 simply select 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. 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.

B. *Watermark Embedding*:

Each 8x8 block of image is used to embed 1 bit of watermark logo. We take an 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 than one pair but if attacker is ready to lose 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 propose that attacker cannot 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 the 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.);
6) a)Hide "0": For all 4 chosen coefficients in step 3, assign the value of coefficients which is 'T' less than the average

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

C. *Watermarked Image*

After embedding the Watermark, we can have the Watermarked Image. The image will be stored in the desired folder.

D. *Authenticated Watermark*

After successful embedding the watermark to the image, we can authenticate it by providing password protection and we can save the file for our security purpose.

4. EXPERIMENTAL RESULTS

The original images have been taken within a folder. We embed the watermark to the images using our proposed scheme. First we have to browse the required image to insert a

watermark into it. After identifying the image, we have to embed the text watermark on to the image and the image must be saved in the folder in which the original image has been stored. To restrict attacks from the attackers, we simply provide password protection for authentication purpose.

For this, we have to simply select the image to be authenticated and provide a password to encrypt the file. Authentication plays a tremendous role in watermarking to restrict the usage of the watermarked image by unauthorized users or attackers.

The following figures show that the original images and the watermarked images respectively.

Figure 1: a) b)

a) represents College Logo, Taj Mahal and Red Fort Images respectively (top to bottom)

b) represents the watermarked Images (top to bottom).

After successfully embedding the watermark to the images, we can authenticate the images.

5. CONCLUSION

This paper presents a scheme for embedding watermark in an image, 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.

REFERENCES

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

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

[3] Z. Zhao, and E. koch, "Embedding Robust Labels Into Images For Copyright Protection", Proc. of Int. Cong. on Intellectual Property Rights for Specialised Information, Knowledge and New Technologies, Austria, 1995, pp. 242-251.

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

[5] 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.

[6] Vikas Saxena, J.P.Gupta, "Collusion Attack Resistant Watermarking Scheme for Images Using DCT" , IEEE 15th SPCA Conference, 11-13 June 2007, Turkey

[7] J.Hernandez, M.Amado, and F.Perez-Gonzalez, "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure," IEEE Trans. Image Process., vol. 9, no. 1, pp. 55 –68, Jan. 2000.

[8] Q. Cheng and T. Huang, "An additive approach to transform- domain information hiding and optimum detection structure," IEEE Trans. Mult., vol. 3- 3, pp. 273 – 284, Sep. 01.

[9] M. Kutter and S. Winkler, "A vision-based masking model for spread spectrum image watermarking," IEEE Trans. Image Process., vol. 11, no. 1, pp. 16 –25, Jan.2002.

[10] P. Moulin and A. Ivanovic, "The zero-rate spread-spectrum watermarking game," IEEE Trans. Signal Process., vol. 51, no. 4, pp. 1098 – 1117, Apr. 03.

[11] H. Altun, A. Orsdemir, G. Sharma, and M. Bocko, "Optimal spread spectrum watermark embedding via a multistep feasibility formulation," IEEE Trans. Image Process., vol. 18, no. 2, pp. 371 –387, Feb. 2009.

[12] S. Maity and S. Maity, "Multistage spread spectrum watermar detection technique using fuzzy logic," IEEE Signal Process Lett., vol. 16, no. 4, pp. 245 –248, Apr. 2009.

[13] "Optimum decoding and detection of multiplicative watermarks," IEEE Trans. Signal Process., vol. 51, no. 4, pp. 1118 – 1123, Apr. 2003.

[14] Q. Cheng and T. Huang, "Robust optimum detection of transform domain multiplicative watermarks," IEEE Trans.Signal Process., vol. 51, no. 4, pp. 906 – 924, Apr. 2003.

[15] J. Wang, G. Liu, Y. Dai, J. Sun, Z. Wang, and S. Lian "Locally optimum detection for barni's multiplicative watermarking in dwt domain," Signal Process., vol. 88, no. 1, pp. 117–130, 2008.

[16] M. A. Akhaee, S. M. E. Sahraeian, and F. Marvasti, "Contourlet-based image watermarking using optimum detector in a noisy environment," IEEE Trans. Image Process., vol. 19, no. 4, pp. 967 –980, Apr. 2010.

[17] M. A. Akhaee, S. M. E. Sahraeian, B. Sankur, and F. Marvasti, "Robust scaling-based image watermarking using maximum-likelihood decoder with optimum strength

factor," IEEE Trans. Multimedia, vol. 11- 5,pp. 822 –833, Aug. 2009.

[18] C.W.Tang and H.M.Hang, "A feature-based robust digital image watermarking scheme," IEEE Trans. Signal Process., vol. 51, no. 4, pp. 950 – 959, Apr. 2003.

[19] D.Zheng, J.Zhao, and A.El Saddik, "Rst-invariant digital image watermarking based on log-polar mapping and phase correlation," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 753 – 765, Aug., 2003.

[20] B.Chen and G.Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1423 –1443, May. 2001.

[21] J.Eggers, R.Buml, and B.Girod, "Estimation of amplitude modifications before scs watermark detection," in Proc.SPIE: Security Watermarking Multimedia Contents , vol. 46, San Jose, Ca, USA, Jan. 2002, pp. 387–398.

[22] J.H.Conway, N.J.A. Sloane, and E. Bannai, Sphere-packings, lattices, and groups. New York, NY, USA: Springer-Verlag New York, Inc., 1998.

[23] M.Miller, G.Doerr, and I.Cox, "Applying informed coding and embedding to design a robust high-capacity watermark," IEEE Trans. Image Process., vol. 13, no. 6, pp. 792 –807, Jun. 2004.

[24] C.Chen and X.Wu, "An angle qim watermarking algorithm based on watson perceptual model," in Proc. of ICIG07 ,Chengdu, Sichuan, China, 22-24 2007, pp. 324–328.

[25] F.Ourique, V.Licks, R.Jordan, and F.Perez-Gonzalez, "Angle qim: a novel watermark embedding scheme robust against amplitude scaling distortions," in Proc.IEEE Int. Conf. Acoustics, Speech, and Signal Processing, vol. 2, USA, Mar.05, pp. 797 – 800.

[26] F. Perez-Gonzalez, C. Mosquera, M. Barni, and A. Abrardo, "Rational dither modulation: a high-rate data-hiding method invariant to gain attacks," IEEE Trans.Signal Process., vol. 53, no. 10, pp. 3960 – 3975, Oct. 2005.

[27] P.Guccione and M.Scagliola, "Hyperbolic RDM for nonlinear volumetric distortions,"IEEE Trans. Inf. Forensics Security,Vol 4,no 1,pp 25 –35, Mar. 2009.

[28] M.A.Akhaee, A.Amini, G.Ghorbani, and F.Marvasti, "A solution to gain attack on watermarking systems: Logarithmic homogeneous rational dither modulation," in Proc. IEEE Int. Conf. Audio, Speech, and Signal Process., Dallas, TX, USA, May. 2010, pp. 1050 –1053.