CDMA Based Reversible and Blind Watermarking Scheme for Images

Muhammad Kashif Samee and Jürgen Götze

Abstract—**Digital watermarking is a well known technique used for copy rights protection of multimedia data. The biggest disadvantage of general watermarking schemes is that they permanently distort original data. Reversible watermarking techniques allow the restoration of original data, after watermark detection. A blind robust and reversible watermarking algorithm based on CDMA is proposed in this paper. Watermark is arithmetically added in CDMA based watermarking schemes. Therefore, it is not difficult to make CDMA based watermarking schemes reversible. In proposed algorithm, spreaded watermark is added to middle frequency coefficients in DCT domain in a specific way. Watermark is extracted by using spreading codes only. After extraction, the watermark can be removed from watermarked data only by using same spreading codes. Furthermore, the original watermark is not required during watermark removal process.**

Index Terms—**Reversible watermarking, DCT, CDMA**

I. Introduction

With the emergence of wide bandwidth wireless networks, mobile internet is set to provide a significant channel of multimedia content distribution. In the absence of proper digital rights management systems, there is a real risk of interception, manipulation, misuse and unauthorized distribution of information. Digital watermarking is one of those techniques used for copyrights protection of multimedia data. Digital watermarking has become a very active area of research in recent years.

Watermarking schemes are divided in two main categories: non-oblivious and oblivious watermarking schemes. In non-oblivious watermarking schemes original image is required during extraction process. It is not needed in oblivious, or blind, schemes. Generally a watermarking scheme should be unobtrusive, robust, universal and unambiguous. In [1] qualities of a good watermarking scheme are described in detail. Another property of a good watermarking scheme is security i.e. how robust a watermarking scheme against malicious attacks. Code Division Multiple Access (CDMA) systems are considered as one of the most secure communication systems. Proposed watermarking scheme is based on Direct Sequence Code Division Multiple Access (DS-CDMA). Every watermark bit is spread before insertion to an image and mistaken for noise, such that it goes undetected by an evedropper.

Manuscript received September 14, 2012; revised October 22, 2012.

Muhammad Kashif Samee is with Department of Electrical Engineering, CEET University of the Punjab Quaid e Azam Campus, and Lahore, Pakistan (e-mail: kashif.samee@tu-dortmund.de)

Jürgen Götz is with Information Processing Lab, Dortmund University of Technology Otto-Hahn-Str. 4, 44227, Dortmund, Germany

Biggest disadvantage of general watermarking algorithms in practice is that they permanently distort original image. In sensitive applications like military or medical imagery original image is required after watermark extraction. This requirement creates another category of watermarking schemes called reversible watermarking schemes. In these schemes, the watermark can be removed completely after watermark extraction (detection) to retrieve original image back.

Proposed watermarking algorithm is blind and based on CDMA. It is secure, reversible and can carry more payload than some other CDMA based schemes [2]. This algorithm is very flexible and watermark can be added at wide range of PSNR values. This scheme is very robust even if watermark is added at high PSNR value. So, it can be used as irreversible watermarking algorithm for normal distribution of images in less sensitive applications [3]. When a very strong watermark is needed, watermark is added at low PSNR value and visible on watermarked image, but it only looks like a noise. If a very noisy watermark is added, watermarked image become useless for unauthorized users. Authorized users can detect the watermark and later remove it to get noise free original image.

Compared to previous reversible watermarking schemes, proposed scheme has certain advantages. Visible watermarks are usually added to specific areas of image [4], but in proposed algorithm visible watermark is spread over whole image in the form of noise. Reversible watermarking schemes use properties of image [5], [6] and thus are image format dependent. Some of these schemes were not applicable to compressed images. Therefore, some more reversible watermarking schemes were presented for compressed images [7], [8]. Proposed algorithm is independent of image format. Watermark is arithmetically added in frequency domain. It does not matter whether DCT coefficients are quantized or not. Presented algorithm is very robust, unlike most of reversible watermarking scheme which are fragile [9], [10]. In proposed algorithm original watermark is not needed during watermark removal process. Therefore, this scheme is perfect for medical applications where patient name and date of birth are embedded as a watermark.

This paper is organized as follows: In Section 2 CDMA based reversible watermarking algorithm is described. Section 3 presents the experimental results and section 4 concludes this paper.

II. Reversible Watermarking Algorithm

Every watermark bit is spread using a zero mean spreading code before insertion. Original image is transformed to frequency domain (DCT). Spreaded

DOI: 10.7763/IJFCC.2013.V2.138

watermark is arithmetically added to selected frequency coefficients. Modified frequency coefficients are transformed back to get watermarked image. At receiver, watermarked (attacked) image is transformed to frequency domain and same coefficients are selected. Just by calculating cross correlation between selected coefficients and spreading codes watermark is extracted. So, watermark is extracted blindly only by using spreading codes (which can be provided in secret key). Extracted watermark is spread again using same spreading codes and subtracted from the selected frequency coefficients of watermarked image. After applying inverse transformation original image is obtained. So only by using spreading codes watermark can be removed, even original watermark is not required during watermark removal process.

TABLE I: LENA IMAGE

α	PSNR (db) Watermarked image	BER Extracted watermark	PSNR (db) After watermark Removal
0.005	42.9034	0.39%	60.3451
0.007	40.0435	0%	Infinite
0.01	36.9268	0%	Infinite
0.02	30.9708	0%	Infinite
0.03	27.4328	0%	70.3462

TABLE II: MILK DROP IMAGE

α	PSNR (db) Watermarked image	BER Extracted watermark	PSNR (db) After watermark Removal
0.005	42.9034	1.46%	55.0323
0.007	40.0435	0.29%	59.6756
0.01	36.9274	0%	87.1311
0.02	30.9974	0%	59.8520
0.03	27.5148	0%	50.4257

TABLE III: GOLD HILL IMAGE

α	PSNR (db) Watermarked Image	BER Extracted watermark	PSNR (db) After watermark removal
0.005	42.9034	2.44%	52.8087
0.007	40.0435	0.59%	56.0854
0.01	36.9268	0%	Infinite
0.02	30.9740	0%	73.5252
0.03	27.4588	0%	56.7638

TABLE V: 1024 BITS WATERMARK

Attacks (no. of attacks)	Lena	Milk Drop	Gold Hill	Average
resample(1)	100%	100%	100%	100%
ML(7)	43%	43%	29%	38%
MAP(6)	100%	100%	100%	100%
Filtering(3)	100%	100%	100%	100%
ColorReduce(2)	100%	100%	100%	100%
JPEG(12)	83%	83%	92%	86%
Wavelet(10)	90%	90%	80%	87%
Average(123)	88%	88%	86%	87%

TABLE VI: 4096 BITS WATERMARK

Attacks (no. of attacks)	Lena	Milk Drop	Gold Hill	Average
resample(1)	100%	100%	100%	100%
ML(7)	43%	43%	14%	33%
MAP(6)	100%	83%	67%	83%
Filtering(3)	100%	100%	100%	100%
ColorReduce(2)	50%	0%	0%	17%
JPEG(12)	67%	67%	75%	69%
Wavelet(10)	80%	90%	70%	80%
Average(123)	77%	69%	61%	69%

TABLE IV: 64 BITS WATERMARK

Attacks (no. of attacks)	Lena	Milk Drop	Gold Hill	Average
resample(1)	100%	100%	100%	100%
ML(7)	100%	100%	100%	100%
MAP(6)	100%	100%	100%	100%
Filtering(3)	100%	100%	100%	100%
ColorReduce(2)	100%	100%	100%	100%
JPEG(12)	100%	92%	100%	97%
Wavelet(10)	90%	90%	100%	93%
Average(123)	99%	97%	100%	99%

A. Watermark Insertion

Let $\boldsymbol{w_{in}}$ be a binary watermark which is changed to antipodal bits (simply replace zeros with minus ones) to form a watermark representation $\boldsymbol{w} = [b_1, b_2, \ldots, b_n]$, where, $b_i \in \{-1,1\}$. Select "k" mutually orthogonal spreading codes, $\boldsymbol{s_i} = [s_1, s_2, \ldots, s_l]$ each of length "l". These spreading codes should have zero mean and follow these necessary conditions:

$$s_i \in \{-1,1\}$$

$$\sum_{i=0}^{l} s_i = 0$$

$$< \boldsymbol{s_i}, \boldsymbol{s_j} > = \boldsymbol{s_i}.\boldsymbol{s_j}^T = 0 \; if \; i \neq j$$

Now $\boldsymbol{X}$ be an image of size $N \times N$ which is subject to watermark. Apply 8×8 Forward Discrete Cosine Transformation (FDCT) on $\mathbf{X}$.

$$\boldsymbol{Y} = FDCT(\boldsymbol{X})$$

Select frequency coefficients to form vectors $\boldsymbol{i_j} = [i_1, i_2, \ldots, i_l]$ (selection of frequency coefficients is discussed in Sec. *2.4*. Length of $\boldsymbol{i_j}$ must be equal to the length of spreading codes $\boldsymbol{s_i}$. Modify these $\boldsymbol{i_j}$ vectors according to:

$$\boldsymbol{i_j}' = \boldsymbol{i_j} + \alpha[b_1 \boldsymbol{s_1} + b_2 \boldsymbol{s_2} + \ldots + b_k \boldsymbol{s_k}]$$

In each $\boldsymbol{i_j}$ vector "k" bits are added, here "k" is the number of spreading codes used. α is the gain factor, which controls the intensity of watermark. Higher the value of α, stronger be the watermark and noisier be the watermarked image. Replace all $\boldsymbol{i_j}$ vectors by $\boldsymbol{i_j}'$ to form $\mathbf{Y}'$. By applying Inverse Discrete Cosine Transformation (IDCT) on $\mathbf{Y}'$ watermarked image $\mathbf{X}'$ is obtained.

$$\mathbf{X}' = IDCT(\mathbf{Y}')$$

B. Watermark Extraction

Let $\widehat{\boldsymbol{X}}$ be the received or attacked image. Apply FDCT on $\widehat{\boldsymbol{X}}$:

$$\widehat{\boldsymbol{Y}} = FDCT(\widehat{\boldsymbol{X}})$$

Select same $\boldsymbol{i_j}$ vectors as before, but are now $\hat{\boldsymbol{i}}_{\boldsymbol{j}}$. Every bit is extracted by calculating cross correlation between $\hat{\boldsymbol{i}}_{\boldsymbol{j}}$ and spreading codes $\boldsymbol{s_i}$.

$$< \hat{\boldsymbol{i}}_{\boldsymbol{j}}, \boldsymbol{s_i} > = \hat{\boldsymbol{i}}_{\boldsymbol{j}}.\boldsymbol{s_i}^T = \boldsymbol{i_j}.\boldsymbol{s_i}^T + \alpha[\hat{b}_1 \boldsymbol{s_1}.\boldsymbol{s_i}^T + \hat{b}_2 \boldsymbol{s_2}.\boldsymbol{s_i}^T + \ldots + \hat{b}_k \boldsymbol{s_k}.\boldsymbol{s_i}^T]$$

By using orthogonality of spreading codes the equation can be simplified as:

$$< \hat{\boldsymbol{i}}_{\boldsymbol{j}}, \boldsymbol{s}_{\boldsymbol{i}} >= \ \boldsymbol{i}_{\boldsymbol{j}}.\boldsymbol{s}_{\boldsymbol{i}}{}^{T} + \ \alpha \hat{b}_i \, \boldsymbol{s}_{\boldsymbol{i}}.\boldsymbol{s}_{\boldsymbol{i}}{}^{T}$$

Here α is a positive quantity and $\boldsymbol{s}_{\boldsymbol{i}}.\boldsymbol{s}_{\boldsymbol{i}}{}^{T}$ is always positive so sign of $(\alpha b_i \, \boldsymbol{s}_{\boldsymbol{i}}.\boldsymbol{s}_{\boldsymbol{i}}{}^{T})$ is determined by b_i . Therefore,

$$\hat{b}_i \ = sign < \hat{\boldsymbol{i}}_{\boldsymbol{j}}, \boldsymbol{s}_{\boldsymbol{i}} > \qquad if \ \ \left|\boldsymbol{i}_{\boldsymbol{j}}.\boldsymbol{s}_{\boldsymbol{i}}{}^{T}\right| < |\alpha \boldsymbol{s}_{\boldsymbol{i}}.\boldsymbol{s}_{\boldsymbol{i}}{}^{T}|$$

Here $\boldsymbol{s}_{\boldsymbol{i}}$ is zero mean spreading code and magnitude of $(\boldsymbol{i}_{\boldsymbol{j}}.\boldsymbol{s}_{\boldsymbol{i}}{}^{T})$ is not very large if the length of the spreading codes is long and the elements of $\boldsymbol{i}_{\boldsymbol{j}}$ vectors are mutually similar. So higher the value of α and longer the spreading codes larger be the magnitude of ($\alpha \boldsymbol{s}_{\boldsymbol{i}}.\boldsymbol{s}_{\boldsymbol{i}}{}^{T}$), hence more accurate is the watermark extraction. Every watermark bit is extracted to form extracted watermark $\hat{\boldsymbol{w}} = [\hat{b}_1, \hat{b}_2, \ldots, \hat{b}_n]$.

C. Removal of Watermark

The watermark can be removed after extraction using:

$$\boldsymbol{i}_{\boldsymbol{j2}} \ = \hat{\boldsymbol{i}}_{\boldsymbol{j}} - \ \alpha\left[\hat{b}_1 \, \boldsymbol{s}_{\boldsymbol{1}} + \ \hat{b}_2 \, \boldsymbol{s}_{\boldsymbol{2}} + \ \ldots + \hat{b}_k \boldsymbol{s}_{\boldsymbol{k}}\right]$$

Now all $\hat{\boldsymbol{i}}_{\boldsymbol{j}}$ are replaced by $\boldsymbol{i}_{\boldsymbol{j2}}$ again to get original image back. Another advantage of the proposed scheme is that original watermark is not needed during watermark removal process.

D. Formation of i_j Vectors

$\boldsymbol{i}_{\boldsymbol{j}}$ vectors should be formed in such a way that magnitude of $(\boldsymbol{i}_{\boldsymbol{j}}.\boldsymbol{s}_{\boldsymbol{i}}{}^{T})$ remains as small as possible. As number of ones and minus ones are equally distributed in spreading codes $\boldsymbol{s}_{\boldsymbol{i}}$, the magnitude of $(\boldsymbol{i}_{\boldsymbol{j}}.\boldsymbol{s}_{\boldsymbol{i}}{}^{T})$ will be small, if the elements of $\boldsymbol{i}_{\boldsymbol{j}}$ vectors are mutually similar. Mutually similar elements can be obtained if $\boldsymbol{i}_{\boldsymbol{j}}$ vectors are formed in same rows of every 8×8 DCT block. Variation in lower frequency rows are higher than middle or higher frequency rows of DCT blocks, so lower frequency coefficients are not used. As higher frequency coefficients are discarded during compression process only middle frequency rows are used to make $\boldsymbol{i}_{\boldsymbol{j}}$ vectors. Fig. 1 shows how row-wise $\boldsymbol{i}_{\boldsymbol{j}}$ vectors are formed over the whole image. Different formations presented in [3] can also be used.

III. Experimental Results

A. Reversible Watermarking

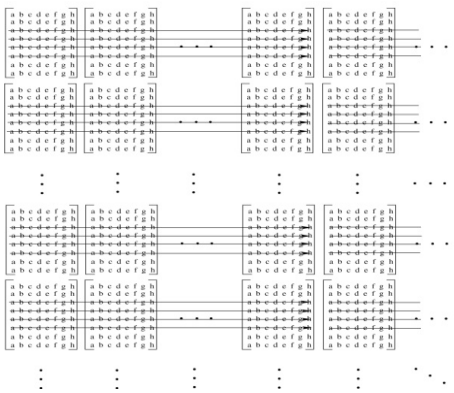

Fig. 1. Row-wise formation of $\boldsymbol{i}_{\boldsymbol{j}}$ vectors. every matrix represents 8 × 8 transformed DCT block.

In all the experiments 512×512 grayscale images (Lena, Milk drop and Gold hill (Fig. 2) are used. A binary watermark 32×32 (1024 bits long) is spread using four 512 bits long mutually orthogonal spreading codes. $\boldsymbol{i}_{\boldsymbol{j}}$ vectors are formed in 3rd, 4th, 5th and 6th rows of 8×8 DCT coefficients blocks (Fig. 1). Column 2 of tables I to III show the PSNR values of watermarked images at different α values. All PSNR values are with respect to original images, shown in Fig. 2. Column 3 presents BER in extracted watermarks. Column 4 shows PSNR values after watermark removal using respective extracted watermarks. Tables I to III show that the PSNR values of restored images are so high (in some cases infinite) that the distortions can be considered as perceptually transparent. Generally, for PSNR values, anything over 40db is not visible.

Fig. 2. (a) Lena image (b) Milk drop image (c) Gold hill image

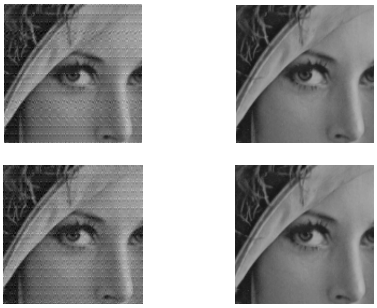

Fig. 3. (a)Watermarked lena image (PSNR=27.4328db). (b)Lena after watermark removal (PSNR=70.3462). (c)Watermarked lena image (PSNR=27.4433db). (d)Lena after watermark removal (PSNR=84.4629)

Fig. 3(a) presents a zoom in version of watermarked image which is very noisy (PSNR=27.4328db). This image is watermarked using a 32×32 (1024 bits long) binary watermark. This image is so noisy that it is useless for unauthorized users. Watermark is extracted with no bit errors from the this watermarked image. Fig. 3(b) shows image after watermark removal, which is identical to original image (PSNR=70.3462). Fig. 3(c) and 3(d) shows the same results with a 64×64 (4096 bits long) watermark. Now the spreading codes are 128 bits long.

B. Robustness where Reversibility is not Required

The watermarking scheme, presented in this paper, is tested against a variety of attacks by using checkmark 1.2 [11]. Checkmark 1.2 only tells whether the watermark is detected or not. So, the watermark detector is programmed at thresholds 70%. In case of 70% threshold, the watermark is considered as detected if BER ≤ 0.3. All images are tested

using three different binary watermarks 64×64 (4096 bits), 32×32 (1024 bits) and 8×8 (64 bits). Images are watermarked at PSNR value of 40db in the following experiments. Results show that this scheme is very robust against jpeg compression as well as wavelet compression. Checkmark 1.2 compresses the watermarked images with a quality factor as low as 10%. Table IV shows that, in average, 97% and 93% of the watermarks are detected against jpeg and wavelet compression respectively. Tables IV to VI show the percentage of correctly detected watermarks from different watermarked images against each attack. Last column in every table shows the average percentage of the detected watermarks against each attack on all the images. Last row shows the average percentage of the detected watermarks against all the attacks on each image.

IV. Conclusion

A blind and reversible watermarking algorithm is presented in this paper. Proposed algorithm is very flexible and watermark can be embedded at a wide range of PSNR values. This scheme can also be used as a normal watermarking application where reversibility is not required. Perceptually transparent watermark can be added at high PSNR values using proposed algorithm. Simulations have proved that this scheme is very robust against a variety of attacks. Reversible version of proposed algorithm can extract the watermark and later recover the original image back. Watermark can be extracted and removed only by using spreading codes. Original watermark is not required during extraction as well as removal process. Further research can be done to send some useful information beyond a simple security tag as a watermark. This information can be extracted after receiving watermarked data, processed and later removed to get original data back.

References

[1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687.

[2] B. Vassaux, P. Bas, and J. M. Chassery, "A New CDMA Technique for Digital Image Watermarking," *Enhancing Capacity of Insertion and Robustness International Conference on Image Processing*, vol. 3, 2001, pp. 983-986,.

[3] M. K. Samee and J. Götze, "Increased Robustness and Security of Digital Watermarking Using DS-CDMA," in *Proc. of 7th IEEE International Symposium on Signal Processing and Information Technology*, Dec. 2007, pp. 189-193,.

[4] Y. Hu and B. Jeon, "Reversible Visible Watermarking Technique for Image," in *Proc. of IEEE International Conference on Image Processing*, 2006, pp. 2577-2580.

[5] H. Golpîra and H. Danyali, "Reversible blind watermarking for medical images based on wavelet histogram shifting," in *Proc. of IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, Dec. 2007, pp. 31-36,.

[6] D. Coltuc, "Improved Capacity Reversible Watermarking," *IEEE International Conference on Image Processing (ICIP)*, vol. 3, 2007

[7] R. A. Farrugia, "A reversible visible watermarking scheme for compressed images," in *Proc. of 15th IEEE Mediterranean Electrotechnical Conference (MELECON)*, 2010, pp. 212-217,.

[8] S. Emmanuel, H. C. Kiang, and A. Das, "A Reversible Watermarking Scheme for JPEG-2000 Compressed Images," *IEEE International Conference on Image Processing*, 2006, pp. 69-72.

[9] Y. Du and T. Zhang, "A Reversible and Fragile Watermarking Algorithm Based on DCT," *International Conference on Artificial Intelligence and Computational Intelligence (AICI)*, 2009, pp. 301-304.

[10] R. Baušys and A. Kriukovas, "Reversible watermarking scheme for image authentication in frequency domain," in *Proc. of 48th International Symposium focused on Multimedia Signal Processing and Communications (ELMA*R), 2006, pp. 53-56,.

[11] S. Pereira, S. Voloshynovskiy, M. Manneño, S. M. Maillet, and T. Pun, "Second Generation Benchmarking and Application Evaluation Information Hiding Workshop III," *Pittsburgh*, PA, USA, April 2001.