Image Authentication Based on DCT with Recovery Capability

JOSE ANTONIO MENDOZA NORIEGA
BRIAN M. KURKOSKI
University of Electro-Communications UEC
Dept. of Inf. and Communication Eng.
1-5-1 Chofugaoka, Chofu-shi
Tokyo, 182-8585
JAPAN
kurkoski@ice.uec.jp

MARIKO NAKANO MIYATAKE
HECTOR PEREZ MEANA
National Polytechnic Institute IPN
SEPI, ESIME Culhuacan
Av. Santa Ana Num. 1000
Mexico City 04430
MEXICO
hmperezm@ipn.mx

Abstract: In this paper an image authentication algorithm is proposed where the modified areas in an image are detected, besides an aproximation of the original image, called digest image C_{dig}, is recovered (recovery capability). Two different watermarks are used. One semi-fragile watermark w_1 is used for authentication phase. The digest image C_{dig} is compressed using an arithmetic code, then redundancy is added by applying BCH error correcting code (ECC) resulting w_{dig}. Finally both watermarks are embedded in the integer wavelet transform (IWT) domain. The proposed scheme is evaluated from different points of view: watermark imperceptibly, payload, accuracy detection of tamper area and robustness against some non intentional attacks. Experimental results show the system detects accurately where the image has been modified and the recovered digest image has a good quality. The proposed system is robust to noise insertion.

Key–Words: Semi-fragile watermark, recovery capability, DCT, IWT, ECC.

1 Introduction

Currently digital images are used as legal evidence in situations such as: car crashes, political scandals and medicals images. Under these circumstances, image authentication has become an important issue in the digital world, because these images can be modified easily using image processing tools.

Conventionally, the methods used for image authentication can be classified into: digital signature-based methods [1], [2], and watermarking-based methods [3], [4], [5]. A digital signature is a set of features extracted from an image and these are stored in a separate file. Watermarking, on the other hand, is a technique that embeds imperceptible authentication information into an image. Most of the existing watermarking and digital signature-based image authentication systems can detect malicious tampering successfully; unfortunately there are few systems that have recovery capability of the tampered region without original image.

The proposed methods in [6],[7],[8] have recovery capability, but none of those is able to resist insertion of even a small amount of noise or large modification of the image.In [6] a watermarking scheme is proposed in which a highly compressed version of the original image is generated using integer wavelet transform (IWT) and discrete cosine transform. The compressed version is embedded in the middle frequency of wavelet. One disadvantage of this scheme is that it is not robust against attacks such as noise insertion and is not able to resist large modifications. In [7] the same authors proposed another authentication system where the original image is compressed using IWT and integer cosine transform (ICT), before embedding, and Huffman compression is applied. A problem with this method is if some bits in the Huffman code, are modified, for example due to a modification, it is impossible carry out reliable decoding. In [8] was proposed a scheme, in which the original image is divided into a region of Interest ROI and a region of Embedding ROE; due this separation the system is not able to protect the whole image, in addition it requires manual selection of the ROI and it is not robust against noise insertion.

In this paper an image authentication algorithm is proposed where the modified areas in an image are detected, and a digest image is recovered. Two different watermarks are used. One semi-fragile watermark (w_1) is used for the authentication phase and is generated as a random sequence.The digest image C_{dig} is compressed using an arithmetic code to reduce the payload and increse the quality of the watermarked image. Then redundancy is added by applying BCH error correcting code (ECC) in order to protect the watermark of against some attacks or modifications.

The compressed and ECC encoded digest image is the second watermark w_{dig}. Finally both watermarks are embedded in the integer wavelet transform (IWT) domain. The second watermark w_{dig} makes possible the recovery because it is embedded into the image.

In the authentication stage, the watermark (w_1') of the suspicious image is extracted and compared with (w_1). If the watermarks are different the second watermark w_{dig} is extracted to recover the digest image.

This paper is organized as follows: in section 2 the proposed authentication method is described. In section 3 the experimental results are provided. Finally conclusions of this paper are described in Section 4.

2 Proposed method

The proposed system uses input parameters: key k_1 for generating of watermark w_1, key k_2 for performing the permutation of w_{dig} before being embedded and ECC parameters(n, k)

2.1 Watermark generation

The first watermark w_1 is generated as a random sequence using a key k_1 similar to [3].

In addition the second watermark w_{dig} the digest image is generated as follows.

1. The original image is down-sampled by half to reduce the size; this is called I.
2. Subtract 127 from gray levels of I to force pixel values to be [-127,128]. This reduces the DCT coefficients values range.
3. I is divided in non-overlapping blocks of 8×8 pixels.
4. Compute the 2D-DCT of each block of 8×8.
5. The first sixteen DCT coefficients are retained from each block (1 DC coefficient and 15 AC coefficients) in zig-zag order.
6. The DCT coefficient are rounded to the nearest integer and represented by 7 bits, including sign.
7. Before being encoded, DCT coefficients are quantized using the JPEG quantization matrix with quality factor equal to 50.

The above steps, produce C_{dig} with length 112 bits per block.

Once that digest image C_{dig} has been generated it is encoded using arithmetic coding which offers a way to compress data and is especially useful for data sources with small alphabets such as binary sources.

After C_{dig} sequence has been compressed, a BCH error correcting code (ECC) is applied which adds redundancy to the original message resulting w_{dig} to detect and correct some errors produced by attacks or modifications. A BCH code is characterized using three parameters (n, k, t) where n represents codeword length, k represents message length and t represents error-correction capability of the ECC.

2.2 Watermark embedding

The proposed watermark embedding process can be summarized as follows. Embed the first watermark w_1 for the authentication process:

1. perform IWT on original image, and embedding is done in low frequency LL_4.
2. The wavelet coefficients are quantized using the following quantization function $f(c_{(i,j)})$ as follows:

$$f(c_{(i,j)}) = \begin{cases} 0, \text{if round}(c_{(i,j)}/\Delta) \text{ is even} \\ 1, \text{if round}(c_{(i,j)}/\Delta) \text{ is odd} \end{cases} \quad (1)$$

where $c_{(i,j)}$ is the (i, j)-th IWT coefficient and Δ represents the quantization step.

The following assignment rule is used to embed the watermark bit $w_{1(i,j)}$ into the selected coefficient $c_{(i,j)}$.

1. If $f(c_{(i,j)}) = w_{1(i,j)}$ then no change in the coefficient is necessary.
2. Otherwise, if $f(c_{(i,j)}) \neq w_{1(i,j)}$ change $c_{(i,j)}$ so that $f(c_{(i,j)}) = w_{1(i,j)}$ as follows:

$$f(c_{(i,j)}) = \begin{cases} c_{(i,j)} + \Delta = & \text{if } c_{(i,j)} \leq 0 \\ c_{(i,j)} - \Delta = & \text{if } c_{(i,j)} > 0 \end{cases} \quad (2)$$

Embed the second watermark w_{dig} for recovery of digest image:

1. Embedding is performed in the second decomposition level of IWT of middle and high frequency, where every wavelet coefficient of subband High-Low HL_2, Low-High LH_2 and High-High HH_2 is represented using eight bits.

   For an image with size $N \times N$ after applying second decomposition level an IWT is obtained with coefficients matrix M_C. The M_C is an $N/4 \times N/4$ matrix.For example, if N = 256, then M_C = 64×64

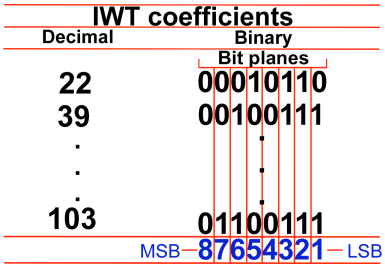

Figure 1: Binary representation of IWT coefficients

2. The M_C matrix is converted to a vector V_C and every IWT coefficient is represented using 8 bits. The payload is divided into 3 parts, one each for HL_2, LH_2 and HH_2.Because the payload is variable, bits are first inserted into bit plane 1, then 2, then 3, etc. until all information is embedded, as shown in Fig. 1.

3. Before being embedded w_{dig} is permuted using a key k_2. This permutation has two purposes: the first is to reduce errors caused by burst errors, produced by some attacks or modification and second is to give security to the watermark.

4. The inverse integer wavelet transform (IIWT) is applied in order to obtain watermarked image.

The output of our algorithm is the watermarked image I_w

2.3 Authentication and recovery

The authentication and recovery process is applied to suspicious image $\widehat{I}_w$ and is described as follows:

1. Watermark w_1 is generated as before using the same key k_1.

2. The IWT of fourth level is applied to suspicious image and using the equation (1) watermark sequence $\widehat{w}_1$ is extracted.

3. If $\widehat{w}_1$=w_1 then the suspicious image has not been modified, and authentication stops.

4. If $\widehat{w}_1 \neq w_1$ the digest image is extracted, immediately the inverse permutation is applied using the same key k_2; then BCH decoding and arithmetic decoding is carried out.

5. Finally the digest image is recovered by performing inverse discrete cosine transform IDCT on the watermark extracted sequence $\widehat{w}_{dig}$.

Table 1: Parameter's values used during embedding.

n	k	t	R=k/n	Bit planes	PSNR
127	120	1	0.945	5	42.01dB
1023	848	18	0.829	5	41.73dB
1023	688	36	0.673	6	41.72dB
1023	563	51	0.550	8	40.82dB
1023	503	58	0.492	9	40.59dB
1023	348	87	0.340	12	39.88dB
1023	288	95	0.282	15	30.78dB
1023	238	109	0.233	17	28.46dB
1023	203	117	0.198	19	22.50dB

3 Results

We conducted three experiments to evaluate performance of the proposed algorithm. The first experiment is to assess watermark imperceptibility, and in the second experiment the modified area detection and the recovery capability of the proposed algorithm are evaluated. Finally, in the third experiment, the watermark robustness to incidental or intentional modification such as noise insertion is evaluated.

3.1 Watermark imperceptibility

The imperceptibility of the watermark was evaluated using 95 images. It was calculated employed the PSNR which compares the similarity between the original image and the watermarked image.

Fig. 2 shows the relationship between PSNR of watermarked image and ECC rate. The ECC rates close to 1 have less redundancy and the payload is smaller, so the imperceptibility of the watermark (PSNR) is high. The number of bit planes used in the embedding phase is shown also in this table, which are divided into 3 parts, one each for HL_2, LH_2 and HH_2.

Table 1 shows the values of some parameters used during the evaluation. The numerical values from Fig. 2 are also shown in the table. In most proposed systems the end user does not have the option to choose that values should be used in the embedding process; however the proposed system was evaluated using different ECC rates give the end user this option to select which one is more suitable for his application.

The Fig. 3 shows the relationship between PSNR and payload size . If the payload is large the PSNR values start to fall.

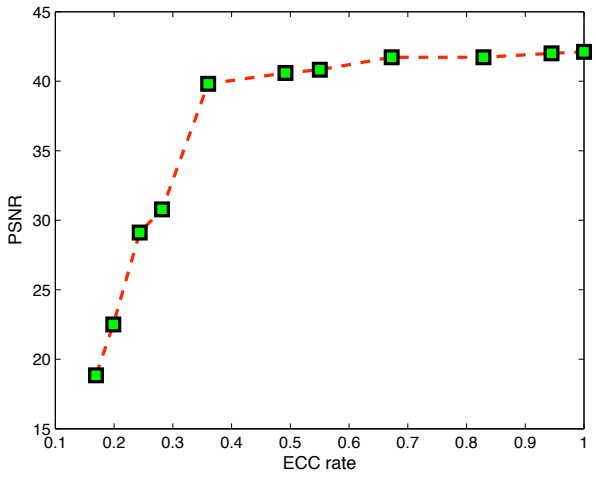

Figure 2: Relationship between PSNR of watermarked image and ECC rate

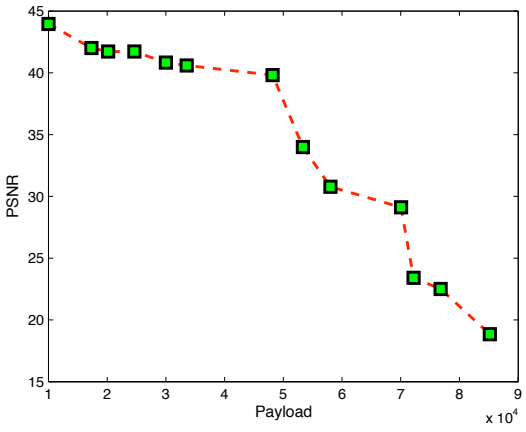

Figure 3: Relationship between PSNR of watermarked image and payload

3.2 Modified area detection and recovery capability

Tamper area detection capability is evaluated, by modifying the contents of images, adding objects or deleting objects. Figures 4 and 5 shows the a) original image, b) watermarked image, c) digest image, d) modified image, e) detection result of tampered image and f) recovered image. Twelve bit planes are used: 4 for High-Low HL_2, 4 for Low-High LH_2 and 4 for High-High HH_2, and ECC parameters $n = 1023, k = 348, t = 87$.

From the point of view of tamper detection the system detects successfully which areas have been modified. The tampered areas are represented using black blocks.

Figure 4: (a) Original image (b) Watermarked image with PSNR = 40.7969 dB (c) Digest image PSNR=30.8485 dB (d) modified watermarked image (e) detection result (f) Recovered image

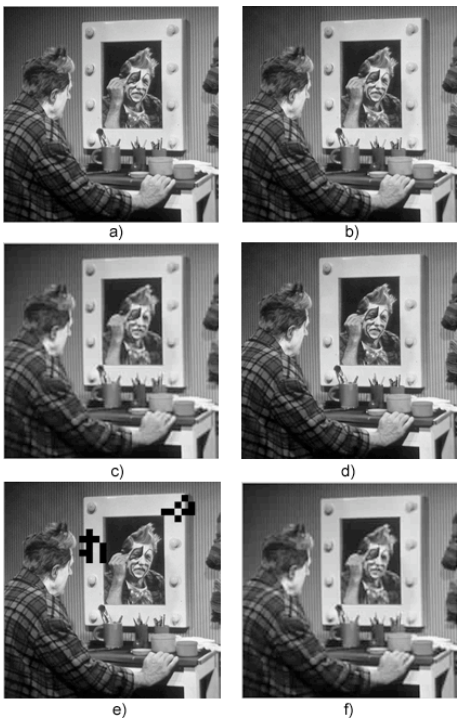

Figure 5: (a) Original image (b) Watermarked image with PSNR = 40.6218 dB (c) Digest image PSNR=30.0816 dB (d) modified watermarked image (e) detection result (f) Recovered image

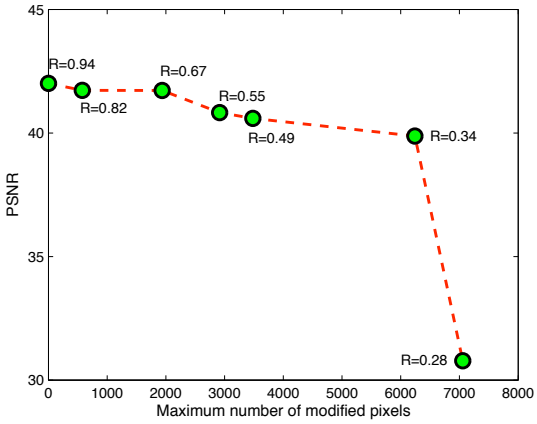

Figure 6: Relationship between PSNR of watermarked image, maximum number of modified pixels and ECC rate.

3.3 Watermark robustness intentional attacks

The watermark robustness is evaluated using the maximum number of modified pixels that the system is able to recover.

Table 2 shows the bit error rate (BER) produced by addition of blocks of different sizes to the watermarked image, these errors are obtained in the extraction phase after applying the inverse permutation and before performing BCH decoding. The BER was calculated using different ECC rates. Table 2 shows also the t/n which represents the maximum percent error-correction capability of the ECC per codeword. It is observed that BER is smaller than t/n, this is because large burst errors are produced in some codewords, exceeding the error-correction capability of BCH code. Table 3 shows the BER and PSNR of digest image using ECC parameters $n = 1023, k = 348, t = 87$.

In Fig. 6 shows the relationship between PSNR and maximum number modified pixels and ECC rate, recovering 100% of the digest image. Fig. 7 shows relationship between PSNR of digest image, number of modified pixels, using ECC parameters $n = 1023, k = 348, t = 87$, with different percent of recovering of digest image.

3.4 Watermark robustness non intentional attacks

The non intentional noise insertion in the signal can be attributable to different factors. The great majority of the previous works are not able to resist noise insertion, but the proposed system using ECC it has

Table 2: Bit error rate (BER) and maximum number of modified pixels.

R=k/n	t/n	BER	Modified Pixel
0.945	0.007	0.0007	1
0.829	0.017	0.0063	576
0.673	0.035	0.0149	1936
0.550	0.049	0.0252	2916
0.492	0.056	0.0309	3481
0.340	0.085	0.0525	6242
0.281	0.092	0.0592	7056

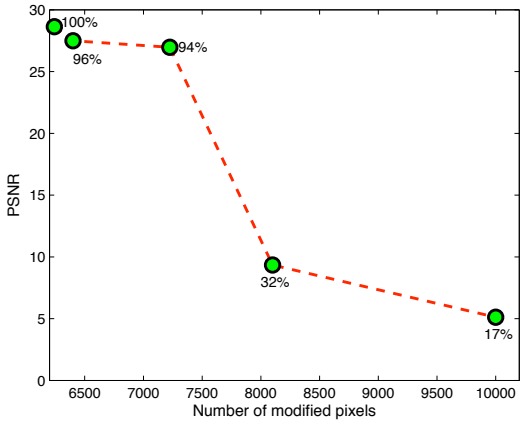

Figure 7: Relationship between PSNR of digest image, number of modified pixels using rate ECC parameters $n = 1023, k = 348, t = 87$.

Table 3: BER and PSNR of digest image using ECC parameters $(n = 1023, k = 348, t = 87)$.

PSNR	BER	Modified Pixel
28.633	0.0525	6242
27.497	0.0579	6400
26.965	0.0647	7225
9.339	0.0709	8100
5.116	0.0873	10000

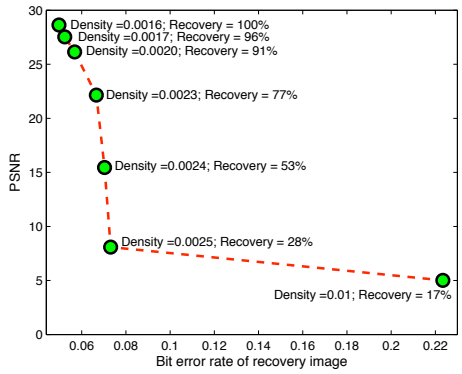

Figure 8: Relationship between PSNR of digest image, bit error rate and salt and paper noise.

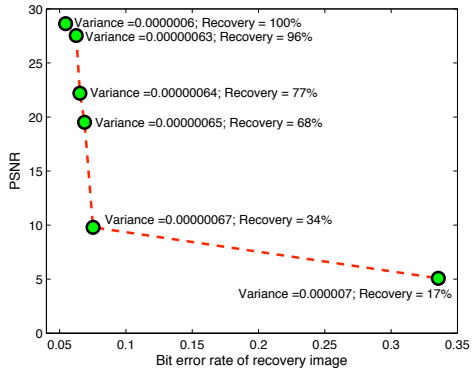

Figure 9: Relationship between PSNR of digest image, bit error rate and Gaussian noise.

the capability to resist noise insertion. Fig. 8 shows the relationship between salt and pepper noise density and bit error rate. Using ECC parameters $n = 1023, k = 348, t = 87$ it is possible to tolerate close to 5 percent errors in order to recover the 100% of digest image. Figure 9 shows relationship between bit error rate with inserted Gaussian noise. In this case the proposed system is able to correct a little more than 5% of errors, giving us the possibility to recover 100% of the original information.

4 Conclusions

In this paper an image authentication algorithm is proposed where the modified areas in an image are detected, in addition, it has recovery capability. One semi-fragile watermark (w_1) is used for authentication phase. A second watermark makes possible the recovery of digest image because this is compressed using an arithmetic code, then redundancy is added by applying a BCH error correcting code before being embedding into the image using IWT. The proposed scheme was evaluated from different points of view: watermark imperceptibly accuracy detection of tamper area, robustness against non intentional attacks including different kinds of noise insertion. Experimental result show the system detects accurately where the image has been modified, and the recovered image has high quality.The proposed system is robust to large modifications of the image and it is able to tolerate noise insertion.

Acknowledgements: This research was sponsored by the UEC Japan through the JUSST program, and the CONACyT of Mexico.

References:

[1] C. S Lu, H. Y. Liao, *Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme.* IEEE Trans. Multimedia, vol. 5, no. 2, 2003, pp. 161–173.

[2] J. Dittmann, A. Steinmetz, and R. Steinmetz, *Content-based digital signature for motion pictures authentication and content-fragile watermarking.* IEEE Int. Conf. Multimedia Computing and Systems, vol. II, pp. 209–213, 1999.

[3] R. XIE, K. Wu, C. LI and S. I Zhu, *An Improve semi-fragile digital watermarking scheme for image Authentication.* Anticounterfeiting, Security, Identification 2007 IEEE International Workshop.

[4] D. Kundur and D. Hatzinakos, *Digital watermarking for telltale tamper proofing and authentication.* Proc. IEEE, vol. 87, pp. 1167–1180, 1999.

[5] C. Lu and H. Liao, *Multipurpose watermarking for image authentication and protection.* IEEE Trans. Image Processing, vol. 10, pp. 1579–1592, Oct. 2001.

[6] R. Chamlawi, A. Khan, and I. Usman, *Authentication and recovery of images using multiple watermarks.* Journal of Computers and Electrical Engineering. Dic. 2009.

[7] R. Chamlawi, A. Khan, and I. Usman, *Dual Watermarking Method for Secure Image Authentication and Recovery.* Multitopic Conference 2009 INMIC 2009. IEEE 13th International.

[8] C. Cruz-Ramos, R. Reyes-Reyes, M. Nakano-Miyatake and H. Perez Meana , *Image Authentication Scheme Based on self-embedding Watermarking.* Springer vol. 5856/2009 pp. 1005–1012. Nov. 2009