INTERNATIONAL JOURNAL OF COMPUTERS
Issue 1, Volume 5, 2011

Image Authentication and Recovery Using BCH Error-Correcting Codes

Jose Antonio Mendoza Noriega, Brian M. Kurkoski, Mariko Nakano Miyatake, and Hector Perez Meana

***Abstract*—text In this paper an image authentication and recovery algorithm is proposed where the modified areas in an image are detected, and in addition an approximation of the original image, called a digest image C_{dig}, is recovered. Two different watermarks are used. One semi-fragile watermark w_1 is used for the authentication phase. The second watermark w_{dig}, is obtained by compressing the digest image C_{dig} using an arithmetic code, then redundancy is added by applying a BCH error correcting code (ECC). 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, detection of the tamper area and robustness against some non-intentional attacks. Experimental results show the system detects accurately where the image has been modified, and it is able to resist large modifications; for example, the system can tolerate modifications close to 10% of the total pixels of the watermarked image and recover the 100% of the digest image. The watermarked image and recovered digest image have good quality, with average PSNR 39.88 dB and 28.63 dB, respectively, using ECC rate 0.34. The proposed system also is robust to noise insertion. It is able to tolerate close to 5% errors produced by salt and pepper noise insertion, while recovering 100% of the digest image.**

***Keywords*—Semi-fragile watermark, recovery capability, DCT, Integer Wavelet Transform, BCH error-correction.**

I. 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]-[7]. 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 the capability to recover the tampered region without the original image [8]-[12]. In this paper, we will concentrate on watermarking schemes.

The proposed methods in [13], [14], [15] 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 [13] 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 (DCT). The compressed version is embedded in the middle frequency of a wavelet transform. 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 [14] the same authors proposed another authentication system where the original image is compressed using IWT and integer cosine transform (ICT), and before embedding, 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 [15] was proposed a scheme, in which the original image is divided into a region of interest (ROI) and a region of embedding (ROE); due to 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 and recovery algorithm is proposed where the modified areas in an image are detected, and an approximation of the original image, called the digest image C_{dig} 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} which is generated using DCT transform is compressed using an arithmetic code to reduce the payload and increase the quality of the watermarked image. Then redundancy is added by applying a BCH error correcting code (ECC) in order to protect the watermark against attacks or modifications. This 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 recovery possible because it is embedded into the image. In the authentication stage, the watermark from the suspicious image $\widehat{w}_1$ is extracted and compared with w_1. If the watermarks are different, the second watermark w_{dig} is extracted to recover the digest image.

Experimental results show the system detects accurately where the image has been modified, and it is able to resist large modification; for example, the system can tolerate the

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

Jose Antonio Mendoza Noriega is with Graduate Section of ESIME Culhuacan, National Polytechnic Institute, Mexico DF, Mexico. (e-mail: pentecostes7@msn.com)

Brian M. Kurkoski is with Department of Information and Communication Engineering University of Electro-Communications Tokyo 182-8585 Japan. (e-mail kurkoski@ice.uec.ac.jp)

Mariko Nakano Miyatake is with Graduate Section of ESIME Culhuacan, National Polytechnic Institute, Mexico DF, Mexico. (e-mail: mnakano@ipn.mx)

Hector Perez Meana is with Graduate Section of ESIME Culhuacan, National Polytechnic Institute, Mexico DF, Mexico. (e-mail: hmperezm@ipn.mx).

modification of close to 10% of the total pixels in the image, and recover the 100% of the digest image. The watermarked image and recovered digest image have good quality, with average PSNR 39.88 dB and 28.63 dB, respectively, using ECC rate 0.34. The proposed system also is robust to noise insertion. It is able to tolerate close to 5% errors produced by salt and pepper noise insertion, while recovering 100% of the digest image.

One of the unique aspects of this research is that the proposed system uses ECC to correct some errors introduced by an attack or modification. Reliable decoding is the key to robustness.

This paper is organized as follows: Section II shows how to generate and embbed both watermarks, additionally authentication and recovery is described. In Section III the experimental results are provided. Finally, conclusions of this paper are described in Section IV.

II. Proposed Method

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

A. Watermark generation

The first watermark w_1 is generated as a random sequence using a key k_1. The image size is $N \times N$ and the watermark size w_1 is $N/16 \times N/16$.

In addition the second watermark w_{dig} is generated as follows and is shown in Fig. 1.

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 the 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 [16].

After the C_{dig} sequence has been compressed, a BCH error correcting code (ECC) is applied which adds redundancy to the original message. The compressed and ECC-encoded image is the watermark to be embedded, w_{dig}. 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. The

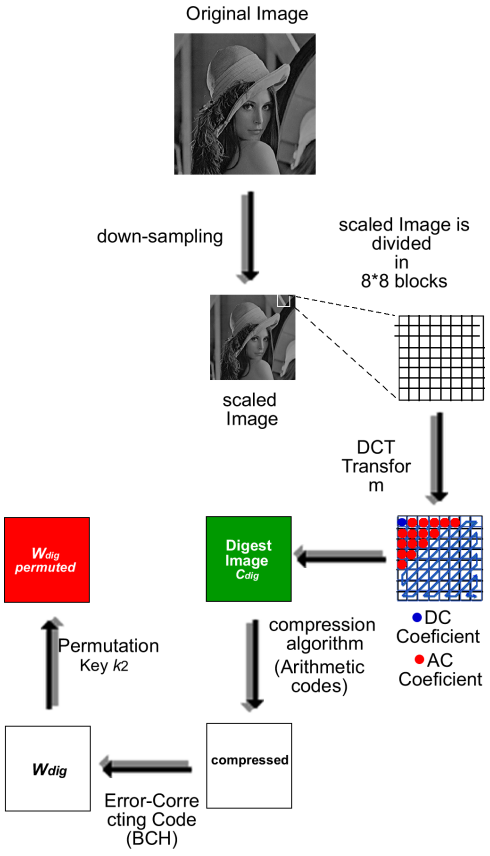

Fig. 1. Watermark Digest image w_{dig} generation.

ECC rate R can be interpreted as the number of information bits entering the encoder per transmitted symbol [17]. For a binary code $R = k/n$, $k \leq n$, or $R \leq 1$.

The length of w_{dig} depends on the efficiency of compression and the ECC rate.

B. Watermark embedding

The proposed watermark embedding process can be stated as follows and is similar to [3],[7]. Embed the first watermark w_1 for the authentication process:

1) Perform IWT on the original image, and embedding is done in low frequency LL_4 with a size of $N/16 \times N/16$.
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.

3) The following assignment rule is used to embed the watermark bit $w_{1(i,j)}$ into the selected coefficient $c_{(i,j)}$.
   a) If $f(c_{(i,j)}) = w_{1(i,j)}$ then no change in the coefficient is necessary.

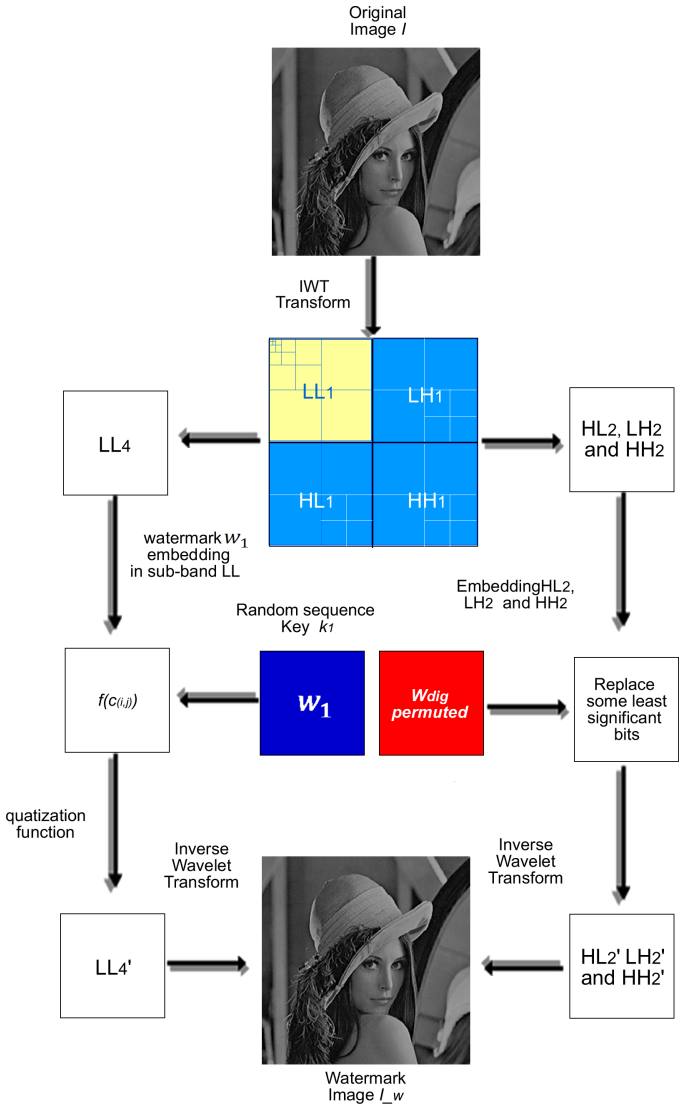

Fig. 2. Watermark embedding.

b) 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:

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

Embed the second watermark w_{dig} for recovery of the digest image as follows; as is shown in Fig.2.

1) Embedding is performed in the second decomposition level of the IWT using sub-band High-Low HL_2, Low-High LH_2 and High-High HH_2 where every coefficient is represented using eight bits.
For an image with size $N \times N$, after applying the second decomposition level, an IWT is obtained with coefficient matrix M_C. The M_C is an $N/4 \times N/4$ matrix. For example, if N = 256, then M_C has size 64×64.
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. 3.
3) Before being embedded w_{dig} is permuted using a key k_2. This permutation has two purposes: the first is to reduce effects of burst errors produced by some attacks or modification and the 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.

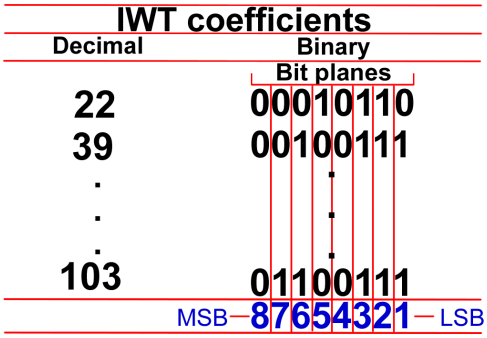

Fig. 3. Binary representation of IWT coefficients.

C. Authentication and recovery

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

1) The watermark w_1 is generated as before using the same key k_1.
2) The fourth level IWT is applied to the suspicious image, and using equation (1) the 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, 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 extracted sequence $\widehat{w}_{dig}$ as is shown in Fig. 4.

If the keys k_1 and k_2 are not the same values used in the embedding process, the watermark $\widehat{w}_1$ extracted and the original watermark w_1 will be completely different, moreover $\widehat{w}_{dig}$ and w_{dig} also be different, caused by in different inverse permutations.

III. Results

We conducted four experiments to evaluate the performance of the proposed algorithm. The first experiment is to assess watermark imperceptibility. In the second experiment, the modified area detection and the recovery tamper region are evaluated. In the third experiment, the watermark robustness to intentional modification is evaluated. A fourth experiment is carried out to evaluate watermark robustness to non-intentional modification such as noise insertion. In addition to these, the proposed method is contrasted against previous works in order to compare its capabilities.

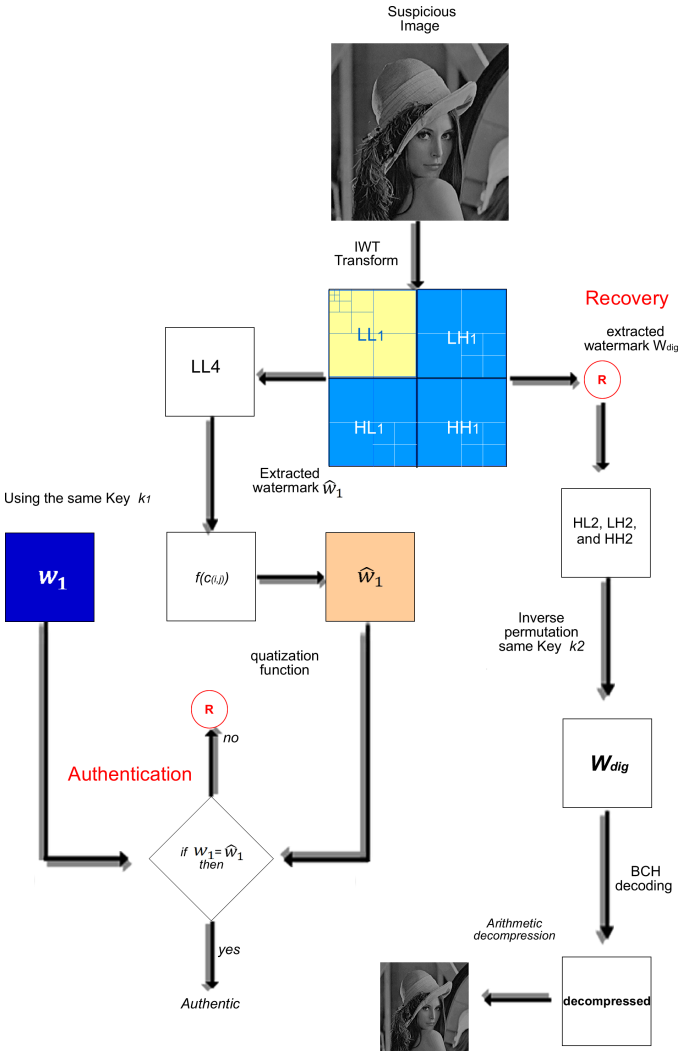

Fig. 4. Authentication and recovery.

Fig. 5. (a) ECC rate=0.34, PSNR=39.88 dB (b) ECC rate=0.282, PSNR=30.78 dB (c) ECC rate=0.198, PSNR=22.5 dB. Refer to TABLE I for more details.

A. *Watermark imperceptibility*

A watermark is imperceptible when the human visual system does not find a difference between an original image and a watermarked image. In the proposed system this imperceptibility depends on the ECC rate because high ECC rate reduces the payload size, and increases the quality of the watermarked image; therefore the watermark is imperceptible. On the other hand, if the ECC rate is low the quality of the image is low because the payload to embed is bigger. However, an advantage of low ECC rate is that its error correction capability is much greater and therefore the watermarked image is more robust. Fig. 5 shows some watermarked images with different ECC rates.

The imperceptibility of the watermark was evaluated using 95 images with $N \times N = 256 \times 256$. PSNR (dB) shows in equation (3) was used, which measures the imperceptibility between the original image and the watermarked image,

$$\text{PSNR} = 10 \log_{10} \frac{N \times N \times 255^2}{\sum_{i=0}^{N} \sum_{j=0}^{N} \left(I_{i,j} - I_{w(i,j)} \right)^2}. \quad (3)$$

Fig. 6 shows the relationship between PSNR of the watermarked image and the ECC rate. ECC rates close to 1 have less redundancy and the payload is smaller, so the imperceptibility of the watermarks (PSNR) is high.

Table I shows the values of some parameters used during the evaluation. The numerical values from Fig. 6 and the number of bit planes used in the embedding phase, which are divided into 3 parts, one each for HL_2, LH_2 and HH_2. are also shown in the table. In most proposed systems the end user does not have the option to choose the tradeoff between robustness and imperceptibility in the embedding process; however the proposed system was evaluated using different ECC rates to give the end user this option to select the tradeoff that is suitable for his application.

In Fig. 6 we can see if an ECC rate equal to 0.340 is selected a PSNR close to 40 dB is obtained, and the watermarks are imperceptible. For ECC rates lower than 0.34, the PSNR reduces dramaticaly.

Fig. 7 shows the relationship between PSNR and payload size for different ECC rates. If the payload is large the PSNR values start to fall.

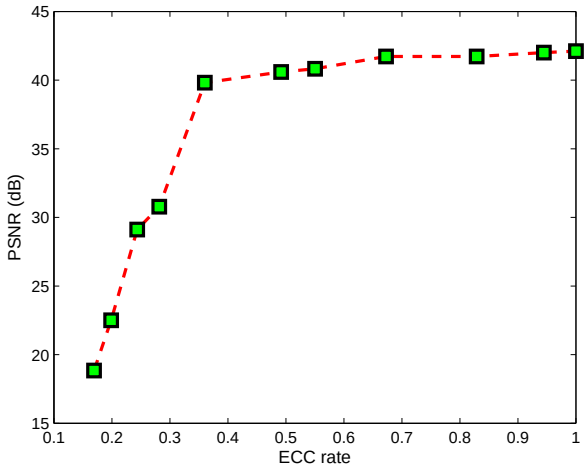

Fig. 6. Relationship between PSNR of watermarked image and ECC rate.

TABLE I
PARAMETER'S VALUES USED DURING EMBEDDING.

Δ	n	k	t	$R = k/n$	Number of Bit planes	PSNR
3	127	120	1	0.945	5	42.0dB
3	1023	848	18	0.829	5	41.7dB
3	1023	688	36	0.673	6	41.7dB
3	1023	563	51	0.550	8	40.8dB
3	1023	503	58	0.492	9	40.5dB
3	1023	348	87	0.340	12	39.8dB
3	1023	288	95	0.282	15	30.7dB
3	1023	238	109	0.233	17	28.4dB
3	1023	203	117	0.198	19	22.5dB

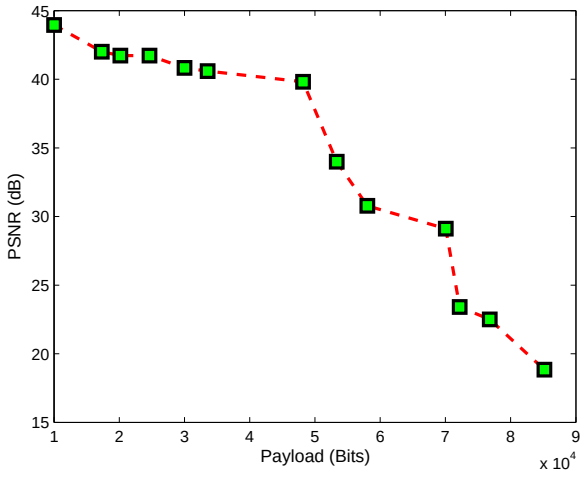

Fig. 7. Relationship between PSNR of watermarked image and payload.

B. Modified area detection and recovery capability

Tamper area detection capability is evaluated by modifying the contents of images, adding objects or deleting objects.

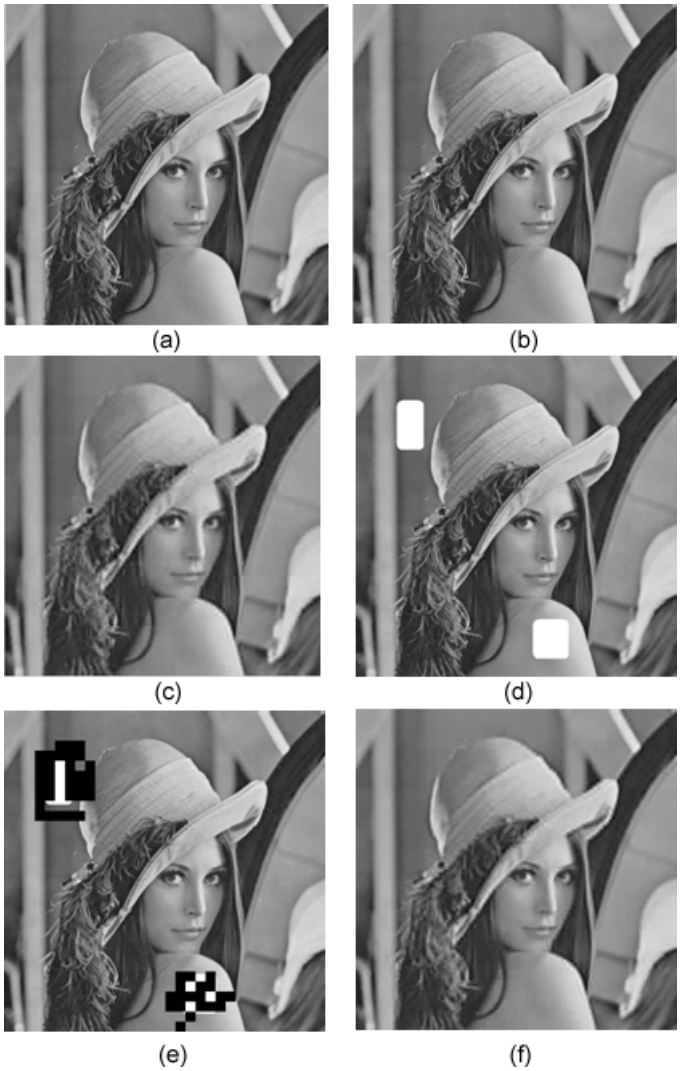

Fig. 8. (a) Original image (b) Watermarked image with PSNR = 40.7969 dB (c) Digest image PSNR=30.8485 dB (d) modified watermarked image (e) detection result (f) Recovered image, identical to (c) Digest image.

Figs. 8, 9 and 10 show 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 $n = 1023, k = 348, t = 87$, rate equal to 0.340.

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.

C. Watermark robustness to intentional attacks

An important consideration in watermarking is the need to keep a balance between the imperceptibility and the robustness of the watermark.

The watermark robustness is evaluated using the maximum number of modified pixels that the system is able to recover. We start with a small number of modifications that the system could easily correct. Then we increased the number of modifications by a small amount until the system was unable to

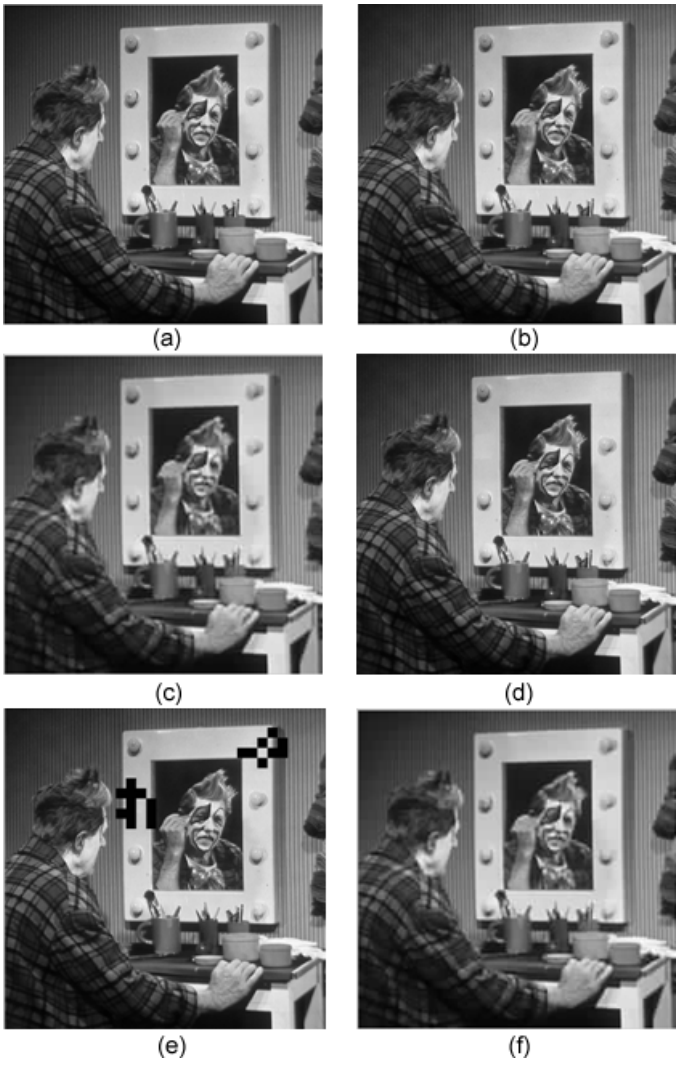

Fig. 9. (a) Original image (b) Watermarked image with PSNR = 40.6218 dB (c) Digest image PSNR=30.0816 dB (d) modified watermarked image (e) detection result (f) Recovered image, identical to (c) Digest image.

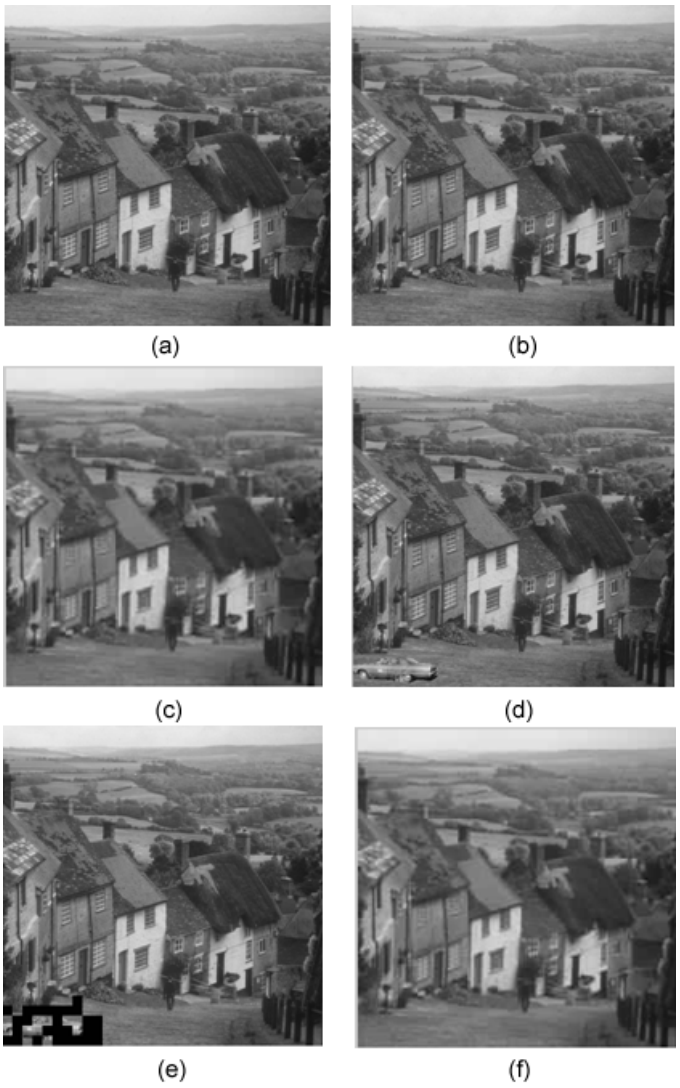

Fig. 10. (a) Original image (b) Watermarked image with PSNR = 40.7969 dB (c) Digest image PSNR=30.8485 dB (d) modified watermarked image (e) detection result (f) Recovered image, identical to (c) Digest image.

recover totally the digest image. A small number less than this is the maximum number of modified pixels. Percent modified pixels is the ratio of modified pixels to total image pixels ($N \times N$).

Fig. 11 shows the relationship between PSNR and maximum number of modified pixels, obtained for various ECC rates, recovering 100% of the digest image. It is observed that by selecting an ECC rate equal to 0.340 the proposed system can tolerate more than 6200 modified pixels, which represents close to 10% of the total pixels in the 256×256 image, which is enough to protect the human face and license plate number in cars.

Table II shows the bit error rate (BER) produced by addition of blocks of different sizes to the watermarked image. The numerical values from Fig. 11 are also shown in the table. These errors are obtained in the extraction phase after applying the inverse permutation and before performing BCH decoding. The BER was evaluated for different ECC rates. Table II shows also t/n which represents the maximum percent error-correction capability of the ECC per codeword. It is observed that the BER is smaller than t/n; this is because the errors are random, with more errors occuring in some codewords, exceeding the error-correction capability of the BCH code.

The PSNR of the digest image also was evaluated, in Fig. 12 is shown relationship between PSNR of the digest image, number of modified pixels, using ECC parameters $n = 1023, k = 348, t = 87$, with different percent of recovered of digest image, where its average PSNR is close to 30 dB.

Table III shows the BER and PSNR of digest image using ECC parameters $n = 1023, k = 348, t = 87$. Note that after BCH decoding the BER usually went to 0. This table shows how PSNR of the digest image deteriorates as the number of modified pixels increases beyond the maximum in Table II.

D. Watermark robustness to 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 has the capability to resist noise

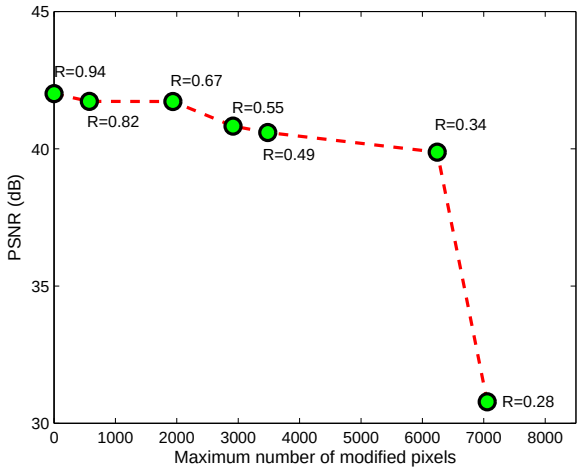

Fig. 11. Relationship between PSNR of watermarked image, maximum number of modified pixels and ECC rate.

TABLE II
BIT ERROR RATE (BER) BEFORE ECC DECODING AND MAXIMUM NUMBER OF MODIFIED PIXELS.

$R = k/n$	t/n	BER before Decoding	Max. Num. Modified Pixels	BER after Decoding	PSNR
0.945	0.007	0.0007	1	0	42.0dB
0.829	0.017	0.0063	576	0	41.7dB
0.673	0.035	0.0149	1936	0	41.7dB
0.550	0.049	0.0252	2916	0	40.8dB
0.492	0.056	0.0309	3481	0	40.5dB
0.340	0.085	0.0525	6242	0	39.8dB
0.281	0.092	0.0592	7056	0	30.7dB

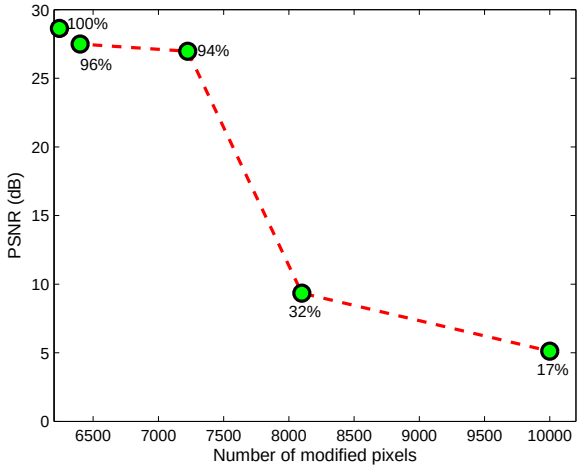

Fig. 12. Relationship between PSNR of digest image, number of modified pixels using ECC parameters $n = 1023, k = 348, t = 87$.

insertion. Fig. 13 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

TABLE III
BER AND PSNR OF DIGEST IMAGE USING ECC PARAMETERS $(n = 1023, k = 348, t = 87)$.

PSNR	BER before Decoding	% Modified Pixels	% Recovery	BER after Decoding
28.633 dB	0.0525	9.5	100	0
27.497 dB	0.0579	9.8	96	0.0005
26.965 dB	0.0647	11	94	0.003
9.339 dB	0.0709	12.35	32	0.037
5.116 dB	0.0873	15.3	17	0.35

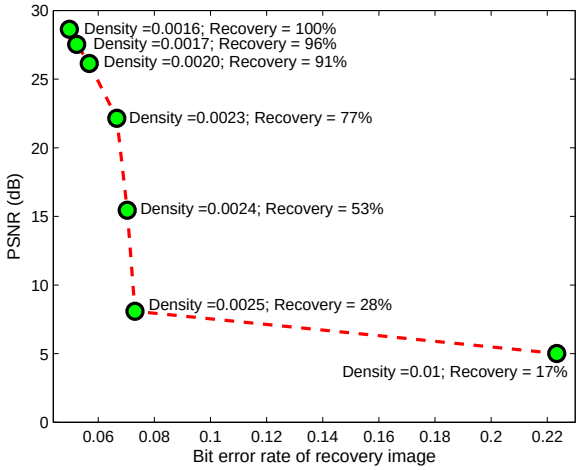

Fig. 13. Relationship between PSNR of digest image, bit error rate and salt and pepper noise.

percent errors and still recover the 100% of digest image.

E. Comparison with other methods

To compare capabilities of the proposed algorithm, it was compared with other methods that we call Chamlawi-I [13], Chamlawi-II [14] and Cruz-Ramos [15]. Table IV shows the comparison where we can observe Chamlawi-I's algorithm is not able to resist large modification because if the watermarked image is severally modified, the recovered image has low quality. In contrast Chamlawi-II's algorithm is not robust either to large modification because this scheme is based on Huffman coding and as a consequence if some bits in the Huffman code are modified due to a intentional or non-intentional attack, it is impossible perform reliable decoding. Table IV also shows Cruz-Ramos's algorithm is not able to protect the whole image because this scheme only can protect region of interest (ROI) and requires manual selection of ROI and it is not robust against noise insertion.

On the other hand, our proposed system is able to tolerate large modifications because the digest image is encoded using BCH error correcting code which gives the possibility to correct some errors after the watermarked image has been attacked but also is robust small amount of salt and pepper noise noise insertion.

TABLE IV
COMPARISON SUMMARY BETWEEN PROPOSED SYSTEM AND OTHERS METHODS

Capabilities	Proposed Method	Chamlawi-I [13]	Chamlawi-II [14]	Cruz-Ramos [15]
Accurate modified area detection	The four algorithms are able to detect where the image has been modified			
Security	The four algorithms use secret keys in some phase of the algorithm			
Robustness; large modification of the image	It can tolerate	They are not robust to large modifications		Is robust but only for ROI
Robustness; Salt and pepper noise	It is able to tolerate	They can not tolerate small amount of noise insertion		
Protect the whole image	They can protect whole image			It can not protect whole image

IV. 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 the digest image. This is compressed using an arithmetic code, then redundancy is added by applying a BCH error correcting code before being embedded 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 salt and pepper 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. The system is able to protect close to 10% of the total pixels and recover totally the digest image, which is enough to protect human face and license plate number in cars in case had been modified. The percent of protected pixels against modifications can be further increased using a stronger ECC like Reed-Solomon codes [18] or LDPC codes [19].

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] Chamidu Atupelage, and Koichi Harada, *"Perceptible Content Retrieval in DCT Domain and Semi-Fragil Watermarking Techniques for Perceptible Content Authentication",* WSEAS Transactions on Signal Processing, vol. 4, pp. 627-636. 2008.

[7] Chin-Man Pun, and I-Kuan. Kong, *"Adaptive Quatization of Wavelet Packet Coefficients for Embedding and Extraction of Digital Watermarks",* NAUM International Journal of Communication Issue 3, vol. 1, 2007 pp. 114-119. Nov. 2007.

[8] Kenji Sumitomo, M. Nakano-Miyatake and H. Perez Meana, *"Image Authentication and Recovery Scheme Based on Watermarking Technique",* 2da WSEAS Int. Conf on Computer Engineering and Applications (CEA'08), January 2008.

[9] Jiri Fridrich, and Miroslav Goljan, *"Images with Self-Correcting Capabilities",* ICIP'99, Kobe, Japan, October 25-28, 1999.

[10] P. -L. Lin, P. -W. Huang, and A. -W. Peng, *"A Fragile Watermarking Scheme for Image Authentication with Localization and Recovery ",* Proc. of the IEEE sixth Int. Symp. on Multimedia Software Engineering, 2004, pp. 146-153.

[11] P. -L. Lin, -K. Hsieh, and P. -W. Huang, *"Hierarchical Watermarking Scheme for Image Authentication and Recovery ",* IEEE Int. Conference on Multimedia and Expo, 2004, pp. 963-966.

[12] P. Tsai, and Y. -C. Hu, *"A Watermarking-Based Authentication with Malicious Detection and Recovery ",* International Conference of information Communication and Signal Processing, 2005, pp 865-869.

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

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

[15] 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.

[16] Sayood Khalid, *"Introduction to Data Compression",* San Francisco, Morgan Kaufmann, 2006.

[17] S. Lin, Daniel J. Costello *"Error Control Coding",* Person Prentice all 2004.

[18] W. Abdul, P. Carre and P. Gaborit, *"List Decoding of Reed Solomon Codes for Wavelet Based Colour Image Watermarking Scheme",* Image Processing ICIP, 16th IEEE International Conference 2009 pp. 3637-3640.

[19] A. Bastug, and B. Sankur, *"Improving the Payload of Watermarking Channels Via LDPC Coding",* Signal Processing Letters, IEEE pp. 90-92, 2004.