Quantization Based Data Hiding Scheme for Efficient Quality Access Control of Images using DWT via Lifting

Amit Phadikar[1], Santi P. Maity[2], Malay K. Kundu[3]

[1]Department of Information Technology, MCKV Institute of Engineering, Liluah, Howrah 711204, India.
[2]Department of Information Technology, Bengal Engineering and Science University, Shibpur, Howrah 711 103, India.
[3] Machine Intelligence Unit & Center for Soft Computing Research, Indian Statistical Institute, Kolkata 700 108, India.
(e-mail: amitphadikar@rediffmail.com, santipmaity@it.becs.ac.in, malay@isical.ac.in)

Abstract

This paper proposes a transform domain data-hiding scheme for quality access control of images. The original image is decomposed into tiles by applying n-level lifting-based Discrete Wavelet Transformation (DWT). A binary watermark image (external information) is spatially dispersed using the sequence of number generated by a secret key. The encoded watermark bits are then embedded into all DWT-coefficients of n^{th}-level and only in the high-high (HH) coefficients of the subsequent levels using dither modulation (DM) but without complete self-noise suppression. It is well known that due to insertion of external information, there will be degradation in visual quality of the host image (cover). The degree of deterioration depends on the amount of external data insertion as well as step size used for DM. If this insertion process is reverted, better quality of images can be accessed. To achieve that goal, watermark bits are detected using minimum distance decoder and the remaining self-noise due to information embedding is suppressed to provide better quality of image. The simulation results have shown the validity of this claim.

1. Introduction

Using communication network and World Wide Web (WWW) digital image(s) can be distributed and transmitted easily and efficiently to the distant places. Unfortunately such applications become insubstantial whenever image security is required. Moreover, for efficient transmission and storage purposes, digital media such as digital images are generally represented in their compressed form like JPEG, more recently in JPEG 2000. Manufacturers and the vendors have always two different objectives in their mind. They need to place their large volume of valuable works in the website for wide publicity and at the same time they want to restrict full quality access to the general users in order to maintain their commercial benefits. This has created a pressing demand to the manufacturers and the vendors to develop a quality access control scheme in transform domain, which allows all the receivers of the broadcast channel to display a low quality image with no or little commercial value. But in the meantime, the scheme also allows image access at higher quality levels depending on each receiver's access rights that usually are determined by the subscription agreement.

Research in access control is now in its very early stage. Scrambling, cryptography and visual cryptography are the few widely used methods adopted either to fully deny or partial accessing of the media. Digital data hiding, although originally developed for copyright protection, ownership verification and authentication are now being used for access control due to commercial or security reasons [1]. In literature, active data hiding (popularly known as watermarking) is commonly used for former class of applications while the latter purpose is served by passive data hiding methods. Passive data hiding is a technique used for media identification where it is expected that signal distortions caused due to data hiding can be reverted by the authorized user to enjoy the full quality. Manipulation in the image for controlling its access to the different categories of users are generally guided by the content of the original image. Access control may find an important application in future generation mobile communication system where billing is expected to be performed based on the fulfillment of degree of quality of services (QoS).

The need of access control has received widespread attention and a number of solutions have been proposed in [2]–[6]. On the contrary, limited research works are so far reported that focused on the use of data hiding scheme to achieve this goal. Access control is normally done in transform domain by modulating the coefficients like DCT (Discrete Cosine Transform), DWT etc. using the secret key. Grosbois et al. [2] propose an authentication and two access control (on image resolutions and qualities) techniques of an image in wavelet domain that can be easily integrated in a JPEG 2000 codec, while remaining compliant with the standard. Imaizumi et al. [3] offer a new private-key encryption for JPEG 2000 code streams for flexible access control of layers, resolution levels and color components. Chang et al. [4] propose a structure to perform layered access control on scalable media by combining encryption and robust data hiding. Pickering et al [5] suggest a blind data-hiding scheme in complex wavelet for access control of video where compliant DVD player deny access to the pirated copy of video. Phadikar et al. [6] recently propose a quality access control of gray scale image in DCT compressed domain. This paper focuses on Quantization Index Modulation (QIM) based data hiding scheme using DWT via lifting for the application of quality access control of images.

The majority of the conventional DWT and DCT based access control schemes reported in the literature suffer form various shortcomings. The most prominent shortcoming is high computation complexity that makes the algorithms

978-0-7695-3476-3/08 $25.00 © 2008 IEEE
DOI 10.1109/ICVGIP.2008.23

unsuitable for faster implementation. It is reported in the literature that compared to DCT, conventional DWT has less computational cost. But in the case of an image having large size, it is still a problem when DWT applied to a whole image [7] [8]. The issue becomes important as many algorithms in recent times demanded real time implementation for which hardware realization becomes a viable alternative. Lifting scheme is an effective method to improve the computation speed of conventional DWT as well for digital design. Integer wavelets transform allows to construct lossless wavelet transform, which is important for quality access control scheme. More over, though 80 % of image and video data are still available in DCT compressed form but future generation multimedia storage and transmission rely on DWT based coding technique. Thus the development of cost effective access control for DWT compressed image and video become an important research issue.

Quantization index modulation (QIM) has recently become a popular form of data hiding based on the framework of communications with side information [9]. QIM-based techniques embed the information by performing quantization of the original sample values. Typical QIM is accomplished by modulating a signal with the embedded information. Quantization is then performed with the associated quantizer. Chen et al. [10] have proposed a watermarking technique using dither modulation (DM), which is a special case of QIM for full self-noise suppression.

In this paper, we propose a quantization based data hiding scheme for quality access control of digital image. The proposed scheme embeds the watermark in the DWT domain via Lifting using DM. The embedding method serves the dual purposes of watermarking as well as data hiding. Lifting technique is used to achieve lower computational complexity. The main contribution of our work lies in an improvement of the quality of the watermarked image through the suppression of the remaining self-noise by the subscriber who has the subscription agreements. Low computational time required for the implementation of the algorithm is other positive point. Moreover, the scheme is entirely blind as it eliminates the use of the original host image at decoder side.

The rest of the paper is organized as follows: Basic principles and key features of lifting are outlined in section-2. Section-3 describes proposed watermark encoding and decoding scheme while in section-4 the performance evaluation of the scheme is demonstrated. Conclusions are drawn in section-5 along with the scope of future works.

2. Basic principles and key features of lifting based DWT

The lifting scheme is a technique for both designing fast wavelets and performing the discrete wavelet transform. The technique was introduced by Wim Sweldens. The discrete wavelet transform applies several filters separately to the same signal [11]. On the other hand the signal is divided like zipper for the lifting scheme. Then a series of convolution-accumulate operations across the divided signals is applied. Generally speaking, lifting scheme includes three steps that are splitting, prediction and update. The basic idea of lifting is described here briefly [12]:

Split: The original signal is divided into two disjoint subsets. Although any disjoint split is possible, we will split the original data set $x[n]$ into $x_e[n] = x[2n]$, the even indexed points and $x_o[n] = x[2n+1]$, the odd indexed points.

Predict: The wavelet coefficients $d[n]$ is generated as error in predicting $x_o[n]$ from $x_e[n]$ using prediction operator P.

$$d[n] = x_o[n] - P(x_e[n]) \quad (1)$$

Update: $x_e[n]$ and $d[n]$ are combined to obtain scaling coefficients $c[n]$ that represent a coarse approximation to the original signal $x[n]$. This is accomplished by applying an update operator U to the wavelet coefficients and adding the result to $x_e[n]$:

$$c[n] = x_e[n] + U(d[n]) \quad (2)$$

These three steps form a lifting stage. Iteration of the lifting stage on the output $c[n]$ creates the complete set of DWT scaling and wavelet coefficients $c^j[n]$ and $d^j[n]$. At each scale we weight the $c^j[n]$ and $d^j[n]$ with k_e and k_o respectively as shown in Fig. 1. This normalizes the energy of the underlying scaling and wavelet functions.

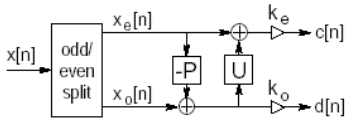


Fig. 1: Lifting steps

The lifting steps are easily inverted even if P and U are nonlinear, space-varying, or noninvertible. Rearranging equation (1) and (2) we have

$$x_e[n] = c[n] - U(d[n]), x_o[n] = d[n] + P(x_e[n]) \quad (3)$$

The original signal will be perfectly reconstructed as long as the same P and U are chosen for the forward and the inverse transforms. The inverse lifting stage is shown in Fig. 2.

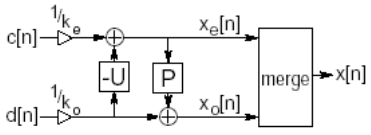


Fig. 2: Typical inverse lifting steps

Lifting scheme has several advantages over classical wavelet based transform and are described below [13].

- Easy to understand and implement.
- Faster(*x2*, but still *O (n),* where *n* is length of signal).

- Inverse transform is easier to find.
- Inverse transform has exactly the same complexity as the forward transform.
- Transforms signals with an arbitrary length (need not be 2^n, where n is length of signal)
- Requires less amount of memory.
- All wavelet filters can be implemented using the lifting scheme.
- Simple extensions to an integer transform possible.

The next section describes lifting based low complexity quality access control scheme of an image.

3. Proposed watermark encoding and decoding scheme

In this section, we present the encoding and the decoding schemes of the proposed method. The objective of the encoding scheme is to hide a watermark in the cover image. On the other hand, the decoding scheme removes the watermark from the watermarked image to obtain the better quality cover image.

3.1. Watermark Encoding

The block schematic of the proposed encoding scheme is shown in Fig. 3. The encoding process is performed in different steps as follows:

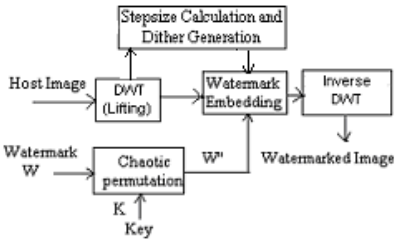


Fig. 3: Block diagram of watermark process: encoder.

Step 1: Permuted Watermark Calculation
The watermarks considered in this work are typically the binary images. Fig. 4(a) shows an example of binary watermark (where the pixel value is either 0 or 1) with size 32x32.

In order to construct a good watermark for embedding, the original watermark is spatially dispersed to obtain a pseudo random sequence as shown in Fig. 4(b), which is uncorrelated with the original watermark. This is done by performing bit wise X-OR operation between the original watermark bits and the random bits. The random bits are generated using a secret key. Then the output sequence is permuted using the same or different secret key to get the desired results. Let the original watermark (W) and a 2-D chaotic binary sequence K (which will be used as a secret key), each with size $n \times n$, be described as follows:

$$W = \{w(i,j), 1 \le i,j \le n, w(i,j) \in (0,1)\} \quad (4)$$

$$K = \{k(i,j), 1 \le i,j \le n, k(i,j) \in (0,1)\} \quad (5)$$

The permuted watermark is calculated as follows:

$$W' = W \oplus K$$

where $\oplus$ denotes the XOR operation. The permuted watermark W' is obtained using the key K.

(a) (b)

Fig. 4: (a) Original watermark; (b) Permuted watermark

Step 2: Image Transformation
Lifting-based n-level 2D-DWT is performed on the original image.

Step 3: Coefficients Selection Criteria for One Bit of Watermark Embedding
One bit of spatially dispersed watermark (W') is inserted into different energy level so that it can resists against low and high pass filtering. Moreover, in case of scalable decoding if only the high-energy subbands are sent to the decoder, watermark can be detected efficiently from those subbands without waiting for the others. Fig. 5 shows the group of selected coefficients (G) for one bit of watermark insertion when the image is decomposed using 3-level DWT. The subbands *LL, HL, LH* and *HH* denote low-low, high-low, low-high, high-high coefficients at various levels. In the case of 3-level decomposition of an image, total 24 coefficients (G) (four coefficients from *LL, HL, LH* and HH_3, four coefficients from HH_2, 16 coefficients from HH_1) are selected for one bit of watermark insertion.

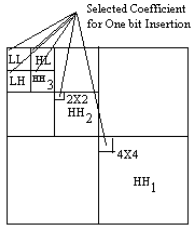


Fig. 5: Selected coefficients for One Bit of Watermark Embedding.

Step 4: Categorization of coefficients
The selected coefficients (G) are divided into b number of different categories (C) depending on the subband they fall.

$$C = (C_1, C_2, C_3, ...C_b) \quad (6)$$

In our scheme the numbers of categories (b) are of 5 types as we take same category for the coefficients in LH and HL subbands. One may also take different category for LH and HL subband for more efficient access control.

Step 5: Selection of Steps Size for QIM based Dither Modulation

Different types of step sizes (Δ) are selected for the coefficient(s) of different category (b). It has been shown that the bit error rate (P_e) in binary watermark decoding is related to the standard deviation of cover image coefficients [14] as follows:

$$P_e = \frac{2(M-1)}{M}\Upsilon\left(\sqrt{\frac{Nd_0{}^2}{4\sigma_x{}^2}}\right) \tag{7}$$

where d_0 indicates step size (Δ) with different values as $\Delta = (\Delta_1, \Delta_2, \Delta_3, ..., \Delta_b)$, M indicates the number of different level of step sizes, $\sigma_x{}^2$ is the variance of an image block, $\Upsilon(.)$ indicates the complimentary error function and N is the number of cover signal points over which a single watermark bit is embedded. As P_e is inversely proportional to the standard deviation, we select small step-size for the coefficients in LL subband since it contains most visual information of the image and large step size (Δ) for HH_1 subband. The step-sizes used for the other subbands lie in between them.

Step 6: Generation of Binary Dither for Each Subband.

Let the number of DWT coefficient(s) for a particular category be denoted by L. For coefficient(s) in category b, two dither sequences, with length L, are generated pseudo randomly using a *key* as follows:

$$d_{b,q}(0) = \{\Re(key) * \Delta_b\} - \Delta_b / 2 \qquad 0 \le q \le L-1 \tag{8}$$

$$d_{b,q}(1) = \begin{cases} d_{b,q}(0) + \Delta_b/2 & if\ d_{b,q}(0) < 0 \\ d_{b,q}(0) - \Delta_b/2 & if\ d_{b,q}(0) \ge 0 \end{cases} \tag{9}$$

where $\Re(key)$ is a random number generator. Note that the elements of $d_{b,q}$ are real-valued. The distance between the corresponding elements of two dither levels ($d_{b,q}(0)$ and $d_{b,q}(1)$) is $\Delta_b / 2$. The sequences $d_{b,q}(0)$ and $d_{b,q}(1)$ are used, respectively, for embedding the bit 0 and bit 1.

Step 7: Watermark Insertion

The bits of the permuted watermark W' are now embedded into the DWT coefficients of different subbands. The q-th watermarked DWT coefficient S_q corresponding to a category b obtained as follows:

$$S_q = \begin{cases} Q\{X_q - k' \times d_{b,q}(0), \Delta_b\} + d_{b,q}(0) & if\ W'(i,j) = 0 \\ Q\{X_q + k' \times d_{b,q}(1), \Delta_b\} - d_{b,q}(1) & if\ W'(i,j) = 1 \end{cases} \tag{10}$$

where X_q is the original q-th DWT coefficient, Q is a uniform quantizer (and dequantizer) with step Δ_b for category b. The factor k' represents the degree of quality degradations for the image. The value of k' is set to 2 in this paper. Note that depending on the value of the permuted watermark bit $W'(i,j)$ calculated in step 1, one of the dither sequences, $d_{b,q}(0)$ or $d_{b,q}(1)$ is used for embedding in the DWT coefficients of the entire group of coefficients (G). After watermark embedding, inverse lifting based DWT is applied and the watermarked image is formed.

3.2. Watermark Decoding

The proposed data hiding method developed to serve the purpose of access control should be blind in the sense that the decoding process does not require the original/host image. The block schematic for watermark decoding is shown in Fig. 6 and the different steps are described as follows:

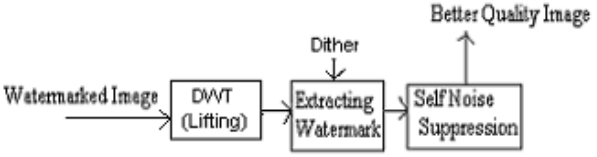


Fig. 6: Block diagram of watermark process: decoder.

Step 1: Steps 2, 3, 4 and 6 of watermark encoding, are performed on the watermarked or possibly distorted watermarked image. The same step size (Δ) is selected for respective category of block that was used at the time of encoding.

Step 2: Watermark Bit Extraction

The detection method uses the principal of minimum distance decoding to determine which quantizer has been used at the encoder side. A watermark bit ($\tilde{W}(i,j)$) is decoded by examining the group of coefficients (G) of different subbands (Fig. 5) using the following rule.

$$\mathrm{A} = \sum_{q=0}^{L-1}\left(\left|Q(Y_q - d_{bq}(0), \Delta_b) + d_{bq}(0) - Y_q\right|\right) \tag{11a}$$

$$B = \sum_{q=0}^{L-1}\left(\left|Q(Y_q + d_{bq}(1), \Delta_b) - d_{bq}(1) - Y_q\right|\right) \tag{11b}$$

where Y_q is the q-th DWT coefficient (possibly distorted) of the received signal for category b. The watermark bit $\tilde{W}(i,j)$ corresponding to a group of selected coefficients (G) is now decoded using the following rule.

$$\tilde{W}(i,j) = \begin{cases} 0 & if\ A < B \\ 1 & otherwise \end{cases} \tag{12}$$

Note that A and B indicate the distance corresponding to the two different watermark bits, and the distance is obtained by calculating the correlation between the received signal and dither vectors used. The relative distance between A and B indicates decoding reliability of the binary watermark where the large distance indicates low probability of decoding error. This in other word indicates noise immunity of the proposed method which in turn offers better quality access control even after signal modification of the watermarked images.

Step 3: Noise Cancellation for Access Control

The remaining self-noise due to watermark embedding is suppressed to get better quality of image using following equation.

$$Y'_q = \begin{cases} Y_q + (k'-1)\times d_{b,q}(0) & \text{if } \tilde{W}(i,j) = 0 \\ Y_q - (k'-1)\times d_{b,q}(1) & \text{if } \tilde{W}(i,j) = 1 \end{cases} \quad (13)$$

Where Y'_q is the watermarked signal after noise elimination. Then inverse lifting based DWT is applied to get relatively high quality of the watermarked image.

Step 4: Decoding of Watermark Bit

The extracted watermark ($\tilde{W}$) bits are reversely permuted i.e. spatially rearranged and are *XOR*ed with random bits to get the decoded watermark ($\hat{W}$). The random bits are generated using the same secret key that was used during the time of watermark permutation at encoder.

Step 5: Decision of Watermark Existence

We calculate the normalized cross correlation (*NCC*) between the original watermark image (W) and the decoded watermark ($\hat{W}$) in order to make a binary decision for a given watermark to exist or not. We choose 0.5 as the threshold of quantitative measure for the particular watermark to exist or not. The normalized cross correlation is defined by equation 14 below.

$$NCC = \frac{\sum_i \sum_j W_{ij} \hat{W}_{ij}}{\sum_i \sum_j (W_{ij})^2} \quad (14)$$

where $W_{i,j}$ and $\hat{W}_{i,j}$ are respectively the original and the decoded watermark bits at $(i,j)^{th}$ position. A watermark is said to be detected if the NCC value exceeds a given threshold.

4. Performance evaluation

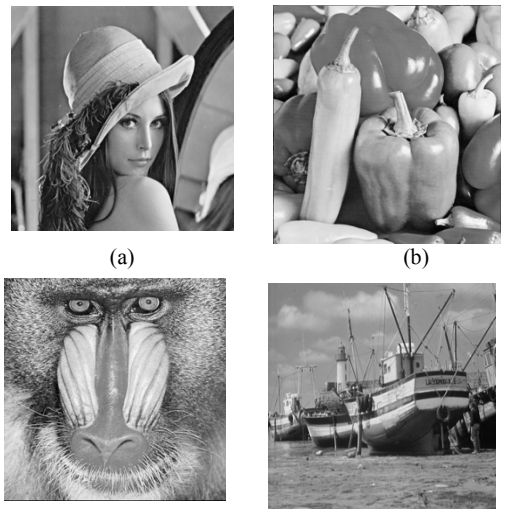
The performance of the proposed algorithm is evaluated over a large number of benchmark images [15][16] including four popular test images: Lena, Pepper, Baboon and Boat shown in Fig. 7. All of the test images are of size (256x256), 8 bit/pixel gray scale image. The length of the dither is of 24 as the level of DWT decomposition taken into consideration is 3. The step sizes (Δ) for dither are taken as 11, 12,13,14,15 for LL, HL &LH, HH_3, HH_2 and HH_1 respectively. These numerical values are chosen during the experimentation over large number of images. The present study uses Peak-Signal-to-Noise-Ratio (PSNR)[17] and Mean Structure Similarity Index Measure (MSSIM)[18] as a distortion measure for the watermarked image under inspection with respect to the original image.

4.1. Visibility Measure

Table 1 illustrates PSNR and MSSIM before and after decoding process for four test images. A normal user without the knowledge of the key can view lower quality images with PSNR as shown in column 2 of Table 1. However, a user with a valid key can decode a superior quality image with PSNR shown in 5th column. Fig. 8 provides a visual comparison between images before and after decoding. Fig 8(a) shows the watermarked image after embedding watermark of size (32x32) and Fig 8(b) is the same after self-noise suppression. Table 2 shows the variation of the image quality (calculated on large number of images) after removal of watermark (with the different size or strength of the watermark).

Table1: PSNR and MSSIM before and after decoding process.

	Before Decoding			After Decoding	
Name of Image	PSNR (dB)	MSSIM	NCC	PSNR (dB)	MSSIM
Lena	31.57	0.89	1	34.63	0.92
Perer	31.61	0.89	1	34.84	0.92
Babbon	31.67	0.95	1	34.94	0.97
Boat	31.67	0.92	1	34.76	0.94



(a) (b) (c) (d)

Fig. 7: Test images. (a) Lena, (b) Pepper, (c) Baboon, and (d) Boat.

PSNR-31.57dB, MSSIM-0.89 PSNR-34.63dB, MSSIM-0.92

(a) (b)

Fig. 8: Watermarked images (a) before and (b) after decoding.

Table 2: Results of variation of the image quality for different watermark size.

Size of Watermark	8x8		16x16		24x24		32x32	
	PSNR (dB)	MSSIM	PSNR (dB)	MSSIM	PSNR (dB)	MSSIM	PSNR (dB)	MSSIM
Before Decoding	43.37	0.9913	38.82	0.9651	33.89	0.9345	31.92	0.8788
After Decoding	47.36	0.9952	40.60	0.9758	37.21	0.9559	34.65	0.9332

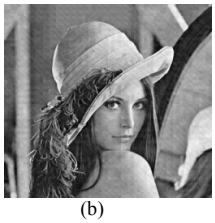
4.2. Robustness Test

To test the robustness of the proposed access control scheme, some typical signal processing attacks, such as filtering, sampling, histogram equalization, various noise addition, dynamic range change, and lossy JPEG compression are performed. The term robustness implies here the ability of quality access control through self-noise submission after various signal processing operation. It is to be noted that these signal processing operations are quite common for storage and transmission or common user may perform as internet is an open system. Fig. 9 shows the watermarked Lena images after some signal processing operation.

PSNR-30.56, MSSIM-0.88

(a)

PSNR-22.08, MSSIM-0.87



(b)

PSNR-27.06, MSSIM-0.68

(c)

PSNR-19.85, MSSIM-0.34

(d)

PSNR-26.85, MSSIM-0.81

(e)

PSNR-18.77, MSSIM-0.71

(f)

PSNR-29.80, MSSIM-0.89

(g)

PSNR-27.38, MSSIM-0.87

(h)

PSNR-29.60, MSSIM-0.88

(i)

SNR-19.79, MSSIM-0.85

(j)

Fig. 9: (a) Watermarked image after lossy JPEG-70, (b) Watermarked image after dynamic range change,(c) Watermarked image after adding 'Spikel' noise with variance .005, (d) Watermarked image after adding 'Gaussian' noise with variance .005, (e) Watermarked image after adding 'Salt and Paper' noise with variance .005, (f) Watermarked image after Histogram equalization., (g) Watermarked image after down and up sampling by factor .75, (h) Watermarked image after mean filtering (3x3), (i) Watermarked image after median filtering (3x3), (j) Watermarked image after high pass filtering (3x3).

Robustness against such operations is essential as it is expected that an un-authorized user may distort the watermarked images so that the user having valid commercial agreement may not avail better quality of the images. The experimental results are shown in Table-3 for test image 'Lena'. It can be seen that our algorithm can successfully resist attacks like median and mean filtering, high pass filtering of mask size (3x3) each, sampling, histogram equalization and JPEG compression with quality factor 50. Moreover, the Table-3 also denotes that a little amount of improvement in the quality is achieved if the watermarked image is gone through common signal processing operations. Fig. 10 shows the improvement of quality in terms of PSNR. It is seen from the Fig. 10 that even the JPEG quality factor down to 50, the scheme still can extract the watermark effectively and based on the extracted watermark the scheme suppress reaming self noise, that results in the improvement of the quality. Fig. 11 shows the NCC values for JPEG compression with different quality factors. Fig. 11 suggests that the scheme can detect the presence of watermark even the JPEG quality factor down to 50.

Table 3: Results of test image 'Lena' with different attacks.

Strength	PSNR Before Deco.	MSSIM Before Deco.	PSNR After Deco.	MSSIM After Deco.	NCC
Median Filtering					
3X3	29.60	0.88	30.37	0.87	0.6963
Mean Filtering					
3X3	27.38	0.87	27.98	0.85	0.6130
High pass Filtering					
1.8	19.79	0.85	20.86	0.87	0.8099
Down & Up Sampling					
.90	30.39	0.90	31.69	0.90	0.8144
.75	29.80	0.89	30.84	0.89	0.7458
Histogram Equalization					
	18.77	0.71	18.60	0.73	0.7503
Dynamic Range Change					
[50- 200]	22.08	0.87	22.25	0.87	0.9381

Salt & Pepper Noise					
.001	30.52	0.88	32.35	0.90	1
.005	26.85	0.81	27.52	0.82	1
.009	24.89	0.73	25.31	0.75	1
Speckle Noise					
.001	30.22	0.83	31.45	0.83	0.7143
.005	27.06	0.68	27.53	0.68	0.5714
.009	25.25	0.60	25.54	0.60	0.5411
Gaussian Noise					
.001	19.79	0.34	19.86	0.34	0.5231
.005	19.85	0.34	19.89	0.34	0.5264
.009	19.87	0.34	19.88	0.34	0.5152

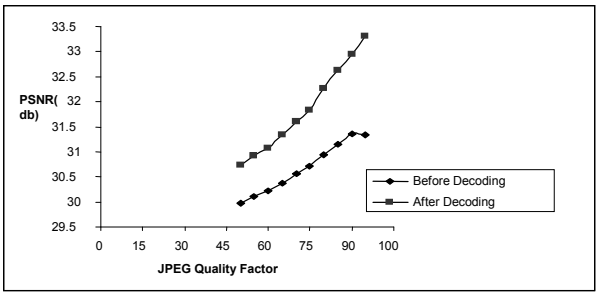


Fig. 10: Improvement of quality in PSNR (db) due to decoding for lossy JPEG compression operation.

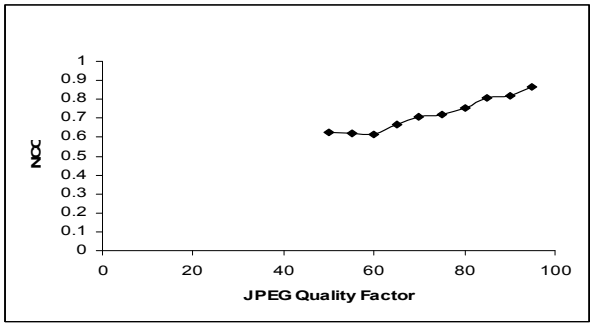


Fig. 11: Results of robustness for lossy JPEG compression operation.

4.3. Computational Complexity

We examine the time that is taken in one whole procedure of encoding and decoding for quality access control of image to depict the computational complexity. We also compare the computational load with the other methods. It is also known that the computational load of conventional DCT and DWT are of *O(n.log n)* and *O(n)* respectively for a signal of length *n*. Feig [19] also pointed out, "it only takes 54 multiplications to compute DCT for a block of size (8x8), unlike wavelet calculation depends upon the length of the filter used, which is at least one multiplication per coefficients". The access control schemes reported in literature are based on conventional DWT or DCT, which required high computational load. Our scheme is based on lifting-base DWT method that is two times faster (though complexity is *O (n))* and requires less amount of memory. So the scheme is efficient for real-time implementation of quality access control scheme. The computation time required for different algorithms are tested in Pentium IV, 2.80 GHz processor, with 504 RAM using MATLAB 7 version. Table-4 illustrates the encoding and decoding time in seconds. Results show that proposed algorithm is much faster than the existing methods.

Table 4: The encoding and decoding time in seconds for access control

Domain	Encoding Process (sec)	Decoding Process(sec)	Total Time (sec)
DCT[6]	3.9840	4.4370	8.4210
DWT[2]	2.2500	1.7190	3.9690
Lifting based DWT[proposed]	1.2250	0.8995	2.1245

4.4. Security

Kerckhoff's theory for encryption scheme states that the security of a system must depend in the choice of a secret key, not the algorithm used to encrypt the data. It is also applicable to the security of data hiding scheme. In our proposed scheme, it is computationally infeasible to acquire the correct secret key '*K*' and the exact embedding parameter simultaneously. The reasons are as below:

1. The watermark we select is of size 32X32. So we can generate 2^{1024} different binary pseudorandom matrices. It makes a large key space. It is very difficult to a would-be an attacker to identify the key used.

2. The dither vector which is used for watermark embedding also depends on the secret 'key'. With out the correct dither the attacker would be in vain to decode the watermark and access of the full quality of image.

Fig. 12 (a) shows the extracted watermark decoded by wrong key. Without the true key, the extracted signature is similar to Gaussion white noise. It demonstrates that our scheme is sensitive to key (*K*) and hence it is secure. Fig. 12(b) shows the decoded image if the watermarked image is decoded by dither generated by the key which is different to encoding key. It is seen that both PSNR and MSSIM values are decreased significantly.

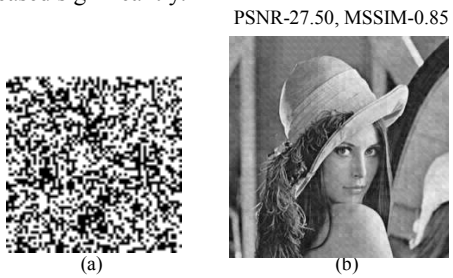


Fig. 12: (a) Extracted watermark using wrong key; (b) Decoded image using wrong key for dither generation.

5. Conclusions and scope of future works

In this paper, a novel lifting-based DWT domain data hiding scheme for quality access control of image using dither QIM is proposed. The extraction of the watermark depends only on the watermarked image and dither vectors,

which makes the scheme blind. The experimental results show that our scheme is robust against various image processing operations such as, filtering, lossy jpeg compression, noise addition, and histogram equalization, dynamic range change, down and up sampling leading to the access of better quality of the image by the authorized users. The scheme is simple, fast, cost effective and easy to implement. It is also secured scheme, only the one with the correct key can extract the watermark. All these characteristics make the scheme a possible solution for digital right management.

Future work will be concentrated to develop VLSI architecture of the proposed method for real-time implementation for image and video.

References

[1] Petitcolas, F.A.P., and H.J.Kim, *Digital Watermarking,* Berlin / Heidelberg: Springer, 2003.

[2]R. Grosbois, P. Gerbelot and T. Ebrahimi, "Authentication and Access Control in the JPEG2000 Compressed Domain," in *Proc. 46th SPIE Annual Meeting, Applications of Digital Image Processing,* San Diego, 2001, pp. 95-104.

[3]S. Imaizumi, O. Watanabe, M. Fujiyoshi, and H. Kiya, "Generalized Hierarchical Encryption of Jpeg 2000 Code streams for Access Control," *in Proc. IEEE International Conference on Image Processing,* Italy, 2005 , pp. 1094-7.

[4]F.C. Chang, H.C. Huang, and H.M. Hang , "Layered Access Control Schemes on Watermarked Scalable Media," *Journal of VLSI Signal Processing (Springer Netherlands),* vol. 49, June 2007, pp. 443 – 455.

[5]M. Pickering, L.E. Coria and P. Nasiopoulos, "A Novel Blind Video Watermarking Scheme for Access Control Using Complex Wavelets," *in Proc. IEEE International Conference on Consumer Electronics*, Las Vegas, 2007, pp. 1-2.

[6]A. Phadikar, M.K. Kundu and S.P. Maity, "Quality Access Control of a Compressed Gray Scale Image", *in Proc. National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG 08)*, India, 2008, pp: 13-19.

[7]X. Wu, J. Hu, Z. Gu, J. Huang, "A Secure Semi-Fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters", *in Proc. Australian Workshop on Grid Computing and E-Research*, New South Wales, 2005,pp. 75-80.

[8] P.Meerwald and A.Uhl, "A Survey of Wavelet-domain Watermarking Algorithms", *in Proc. of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents*, San Jose, USA, pp. 505-516.

[9] M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, May 1983, pp. 439–441.

[10] B. Chen and G.W.Wornell, "Digital watermarking and information embedding using dither modulation", *in Proc. IEEE Workshop on Multimedia Signal Processing,* Redondo Beach, CA, 1998, pp. 273-278.

[11] A. R. Calderbank, I. Daubechies, W. Sweldens, B.-L. Yeo, "Wavelet transforms that map integers to integers," *Applied and Computational Harmonic Analysis,* vol. 5, July 1998,pp. 332–369.

[12] R. L. Claypoole, R. G. Baraniuk, and R. D. Nowak, "Adaptive wavelet transforms via lifting", *in Proc. IEEE International Conference on Acoustics, Speech and Signal Processing*, Seattle, WA, 1998, pp.1513-1516.

[13] G.Uytterhoeven, D. Roose, and A. Bultheel, "Wavelet transforms using lifting scheme", *Technical Report ITA-Wavelets Report WP 1.1, Katholieke Universiteit Leuven, Department of Computer Science*, Belgium, April 1997.

[14] S.Voloshynovskiy and T.Pun , "Capacity-Security Analysis of Data Hiding Technologies", in Proc. IEEE International Conference On Multimedia And Expo, Lausanne, Switzerland,2002,pp. 477-480.

[15] http://www.cl.cam.ac.uk/fapp2/watermarking.

[16]http://www.petitcolas.net/fabien/watermarking/image_database /index.ht ml.

[17] Gonzalez, R.C., R. E. Woods, and S. L. Eddins, *Digital Image Processing Using Matlab*, Pearson Education, 2005.

[18] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image Quality Assessment: From Error Measurement to Structural Similarity," *IEEE Transactions on Image Processing*, vol. 13, Jan. 2004, pp. 1-14.

[19] E. Feig, "A fast scaled DCT algorithm", *in Proc. SPIE Image Processing Algorithms and Techniques*, 1990, pp. 2-13.