DATA HIDING FOR QUALITY ACCESS CONTROL AND ERROR CONCEALMENT IN DIGITAL IMAGES

Amit Phadikar[1], *Santi P. Maity*[2], *Claude Delpha*[2]

[1]Department of Information Technology, MCKV Institute of Engineering, Liluah, Howrah, 711204, India
[2]Laboratoire des Signaux et Systemes, CNRS, Universite Paris-Sud XI (UPS), SUPELEC, France
(amitphadikar@rediffmail.com, {santiprasad.maity, claude.delpha}@lss.supelec.fr)

ABSTRACT

This paper proposes a data hiding scheme to serve dual purpose of quality access control and error concealment of digital images. This is accomplished by projecting host image first on N-mutually orthogonal sample sets followed by embedding of an encoded binary watermark (host digest) using quantization index modulation (QIM) but without complete self-noise suppression. It is well known that due to insertion of external information, there would be degradation in visual quality of the host image. This has been used here to play the key role in access control through reversible process and error concealment using the extracted image digest. Decision variable for each bit of watermark decoding is formed from the weighted average of N-decision statistics that increases the correctness of extracted watermark bits. This improved detection enables self-noise suppression by authorized user, error concealment in fading radio mobile channel and thus leads to avail better quality image. Simulation results have shown the validity of our claims along with relative comparative results for other existing works.

Index Terms—Access control, error concealment, QIM watermarking, self-noise suppression, Orthogonal decomposition.

1. INTRODUCTION

One of the driving forces for the emergence of World Wide Web (WWW) is due to the tremendous growth in digital techniques that allow gross distributions of multimedia signals in digital form. With the increase in the number of users for Internet applications, the security issues and pivotal challenges like integrity verification, authentications etc. also go on increasing day-by-day. Access control technique may find its use to provide a kind of security either to deny fully or to allow partial accessing of the digital content. A large number of solutions are also proposed in literature [1]–[5]. Grosbois et al. [2] propose an authentication and two access control (on image resolutions and qualities) techniques of an image integrated in JPEG 2000 pipeline. Chang et al. [4] propose a structure to perform layered access control on scalable media by combining encryption and robust data hiding. Jeffrey et al. [5] discuss copy protection of video where compliant digital versatile disk (DVD) player denies access to the pirated copy of video. Phadikar et al. [6] recently propose a quality access control of gray scale image, for color image [7] in discrete cosine transform (DCT) compressed domain, where various drawbacks in [6] like key protection, their proper ordering, synchronization of keys and content etc. are solved in the latter.

The other issue for digital content protection is error resiliency that becomes important when image and video signals are transmitted over unreliable networks such as the Internet and the wireless mobile channels. The corrupted regions usually take the form of blocks or strips due to the block coding nature of the popular image/video codec like JPEG, JPEG 2000, MPEG etc. Automatic repeat request (ARQ) and forward error control coding (FEC) are two major error resilient approaches [1] used by encoder or sender. However, for real-time multimedia communication through radio mobile channel, ARQ is not always feasible due to the intolerable delay in retransmission. On the other hand, error concealment techniques reduce visual artifacts through post processing at the decoder [1]. Moreover, error concealment technique does not require the access to the original information and additional information from the encoder. This in other way suggests that only the valid authorized users would perform the concealment operation for the recovery of error blocks. This goal can be achieved by developing a quality access control scheme, which allows all the receivers of the broadcast channel to avail a low quality image if there is any loss due to transmission. But in the mean time, the scheme also allows image access at higher quality levels through post processing at the decoder. This can be done depending on each receiver's access rights that usually are determined by the subscription agreement. Several data hiding based error concealment methods are developed using region of interest (ROI) and integer wavelets [8], edge information [9], temporal information [10] and reversible data hiding [11] etc.

It is seen that performance of data hiding based access control and error concealment scheme depend on the correct detection/extraction of watermark bits. Although quantization index modulation (QIM) data hiding scheme that is robust against scale attack is also developed [12], however, this scale operation is not applicable for fading-like channel response. In other words, faithful recovery of watermark is essential when watermarked image, video and audio data are transmitted through real radio mobile channel. Thus design of QIM watermarking that is robust against fading-like operation becomes important. Recently, multicarrier communication, like orthogonal frequency division multiplexing (OFDM) becomes appealing to tackle inter symbol interference (ISI) problem for high data rate transmission in fading radio mobile channel. This concept may be used to embed watermark information in independent components of the host followed by defining a weighted decision variable for watermark detection in QIM data hiding scheme.

To this aim, this paper proposes a new model of QIM watermarking for quality access control and error concealment of digital images. Each watermark bit is casted over N-mutually orthogonal signal points (analogous to multicarrier concept in communication), thus a flavor of embedding on independent signal components is created. A digest for the host image is developed to use as watermark. Decision variable for each bit of watermark decoding is formed from the weighted average of N-decision statistics. Primary goal is to provide quality access

Thanks to French National Research program via the ANR project MEDIEVALS for funding.

978-1-61284-350-6/11/$26.00 ©2011 IEEE

control for the authorized users through error concealment in fading channel. Simulation results also show that improved performance in watermark extraction is possible to achieve even for a large class of other attacks. This in turn leads to better access control and error concealment compared to the existing works.

The rest of the paper is organized as follows: Section 2 describes proposed new model of QIM data hiding scheme, while Section 3 presents performance evaluation of the proposed scheme. Conclusions are drawn in Section 4 along with the scope of the future works.

2. NEW MODEL OF QIM DATA HIDING 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 (host digest) in the host (cover) image itself. On the other hand, the decoding scheme uses extracted watermark to remove the remaining self-noise for quality access control and/or uses the same for compensating the lost blocks through error concealment.

2.1 Watermark encoding

The block diagram representation of the proposed encoding scheme is shown in Fig. 1. The encoding process is performed in different steps as follows:

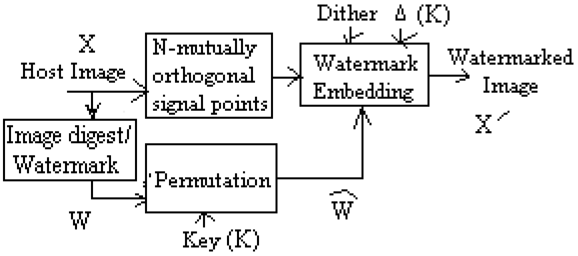


Fig. 1. Block diagram of watermarking process: encoder.

Step 1: Image Digest Generation: The host image (X) of size ($r \times r$) is resized into 1/uth of its original size. A halftoned image is generated from the resized host image using Floyd-Steinberg diffusion kernel $\mathbf{D_{FS}}$ [13] given by:

$$\mathbf{D_{FS}} = \frac{1}{16}\begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{P} & \mathbf{7} \\ \mathbf{3} & \mathbf{5} & \mathbf{1} \end{bmatrix} \qquad (1)$$

where **P** is the current pixel position and $\mathbf{D_{FS}}$ is typically applied on each (3×3) block of the image (X). The resulting halftoned image is denoted by (W) which is of size $\left(r/u \times r/u\right)$, where the symbol r denotes the number of rows/columns of the host image.

Step 2: Permutation of Image Digest: The halftoned image (W) is permuted to get a noise-like form of image digest *($\hat{W}$)* using a secret key (K).

Step 3: Orthogonalization of host: Host image (X) is first projected on *N*-mutually orthogonal signal points in *N*-dimensional signal space. The projection may be accomplished in various different ways like Gram-Schmidt orthogonalization process [14] or by down sampling the cover by a factor of *N*, to obtain a crude form of approximation. Host image X can mathematically be represented as $\mathrm{X} = \{\mathrm{X}_1, \mathrm{X}_2, \ldots, \mathrm{X}_\mathrm{N}\}$ where { X_i } is the signal coefficients corresponding to complete orthogonal basis function set. Theoretically large *N* value is desired for selecting mutually uncorrelated point sets that remove the inherent strong correlation among the host pixels/samples.

Step 4: Watermark Insertion: a) Generation of Binary Dither for QIM: Two dither sequences, with length n, are generated pseudo randomly using the key *(K′)* with step sizes (Δ) as follows:

$$d_q(0) = \left\{\Re(K') \times \Delta\right\} - \Delta/2 \qquad 0 \le q \le n-1 \qquad (2)$$

$$d_q(1) = \begin{cases} d_q(0) + \Delta/2 & \text{if } d_q(0) < 0 \\ d_q(0) - \Delta/2 & \text{if } d_q(0) \ge 0 \end{cases} \qquad (3)$$

where $\Re(K')$ is a random number generator within the range of 0 to 1. Dither is generated based on secret key (K′) that increases security of the proposed scheme. Hence unauthorized user can not extract the watermark from the watermarked image that ultimately results in poor quality of the decoded image after self noise elimination. Selection of the proper step size (Δ) would ensure the fidelity of the watermarked image. Dither $d(0)$ and $d(1)$ are used for embedding watermark bit '0' and '1', respectively.

b) Watermark bit Insertion: In QIM watermarking, host signal points are quantized using a quantizer $Q_\Delta\left(.\right)$. This is used to embed the permuted image digest ***($\hat{W}$),*** which is denoted here as message bit (m). The watermarked signal (X'_N) may also be looked as an *N*-dimensional vector $\{\mathrm{X}'_1, \mathrm{X}'_2, \mathrm{X}'_3, \ldots, \mathrm{X}'_\mathrm{N}\}$ and may be written as follows:

$$\mathrm{X}'_\mathrm{N} = \mathrm{Q}_\Delta\left(\mathrm{X}_\mathrm{N} + \mathrm{S} \times \mathrm{d(m)}\right) - \mathrm{d(m)}\,;\ m \in \left\{0,1\right\} \qquad (4)$$

where Δ is a fixed quantization step size, $d\left(.\right)$ is the used dither for embedding watermark bit. The factor 'S' represents the degree of quality degradations for the image. The value of 'S' is set to 2 here as that amount of distortion is sufficient for access control of image. The numerical value is determined from independent experimentations conducted over 250 test images having varied image characteristics.

2.2 Attack channel

Let us assume that an attacker modifies the *n*-th watermarked signal point by an amount α_n which takes values randomly from Rayleigh distribution. The rationale behind such assumption is due to the fact that watermarked data needs to be transmitted through radio mobile channel which may be modeled as frequency selective Rayleigh fading channel. Furthermore, we assume that the watermarked signal is also corrupted by additive white Gaussian noise (AWGN) when transmitted through the communication channel. The distorted and noisy watermarked image point, at the input of the watermark decoder, can be written as

$$\mathrm{X}''_{N.n} = \alpha_n \{Q_\Delta(X_{N.n} + S \times d(m)) - d(m)\} + \mu_n \qquad (5)$$

where μ_n is a Gaussian random variable with mean 0 and variance N$_0$/2. The symbol $X_{N.n}$ represents the nth element of X_N.

2.3 Watermark decoding

The block diagram for watermark decoding scheme is shown in Fig. 2. The steps for watermark decoding process are described as follows:

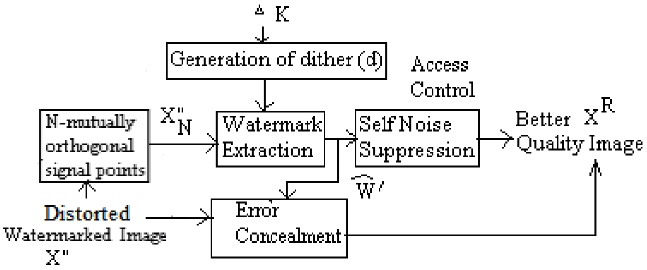


Fig. 2. Block diagram of watermarking process: decoder.

Step 1: Step 4(a) of watermark encoding is performed to generate binary dither using the same step size (Δ) and the key (K) that were used at the time of watermark embedding.

Step 2: Watermark Bit Extraction: The received distorted and noise corrupted watermarked image (X'') is first projected onto *N*-orthogonal signal points and requantized using *m*th dither resulting in $r^m = \{r_1^m, r_2^m, ..., r_N^m\}$. The decision variable for the *m*th dither at nth signal point is denoted by $r_{N.n}^m$ and can be written as follows:

$$r_{N.n}^m = \left| X''_{N.n} - Q_\Delta(X''_{N.n} + d(m)) - d(m) \right|; \quad m \in \{0,1\} \quad (6)$$

The decision variable (D^m) for *m*th watermark bit is obtained using minimum mean square error combining (MMSEC) strategy [14] as :

$$D^m = \sum_{n=1}^{N} r_{N.n}^m C_{nm} \quad (7)$$

where the weight factor C_{nm} is defined as,

$$C_{nm} = \frac{\alpha_n}{(\mathrm{var}(b_k) + N_0/2)} \quad (8)$$

The parameter b_k indicates k-th watermark bit. An estimation of α_n value or use of its actual value would certainly yield the best decoding performance. However, α_n value can be obtained from Rayleigh distribution and an average value obtained from large number of trials can be used. The decision variable (D^m) is fed to the decision device (minimum distance decoder), the output of which determines the binary bit pattern. Thus the correlator's outputs generate a decision vector $D = [D^1, D^2, ...D^K]$ which is used to obtain the embedded bits $\hat{b} = \{\hat{b}_1, \hat{b}_2, ..., \hat{b}_N\}$.

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.

$$X_N^e = X''_N - (S-1) \times d(\hat{b}) \; ; \quad \hat{b} \in \{0,1\} \quad (9)$$

where X_N^e is the watermarked image after self-noise elimination. This offers a better quality image to the authorized users through access control.

Step 4: Decoding of Watermark Bit: The extracted watermark bits ($\hat{b}$) 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 (*K*) that was used during the time of watermark permutation at encoder.

Step 5: Recovery of Lost Blocks (Error Concealment): The recovery of lost blocks is done based on the following steps.

a) The received error image is resized into *1/u*th of its original size. Floyd halftoning is done on the resized received error image. The lost pixels of resultant halftoned image are recovered with the help of $\hat{w}'$.

b) Inverse Floyd halftoning is done considering the output of Step 5(a) and resized error image as input. The output of inverse Floyd halftoning is then zoomed to the size of the original image ($r \times r$). Let X^{ht} is the resultant zoomed output.

c) Error concealment is done through the recovery of lost image pixel using following rule.

$$X^R(r,r) = \begin{cases} X'(r,r) & if \quad no \quad loss \\ X^{ht}(r,r) & else \end{cases} \quad (10)$$

where X^R is the error concealed image, $X'(r,r)$ is the pixel of the received image and $X^{ht}(r,r)$ is the pixel of the inverse halftoned image found in Step 5(b).

3. PERFORMANCE EVALUATION

This section describes performance of the proposed data hiding scheme for access control and error concealment through simulation over 250 test images having varied image characteristics. All of the test images are of size (512×512), 8 bit/pixel gray scale image. Two such test images and their corresponding image digests are shown in Figs. 3(a)-(c). We have tested our results both in spatial and full frame DCT domain, although one may use discrete Fourier transform (DFT), Fourier-Mellin, discrete Hadamard transform (DHT), discrete wavelet transform (DWT) etc. for watermark embedding domain. Spatial domain is selected as embedding space due to the advantages of simple and ease of implementation along with low computational cost. On the other hand, DCT domain is selected as 90% of image and video data are still available in DCT compressed form. Gram-Schmidt orthogonalization is then applied on image sample/coefficients. The present study uses peak-signal-to-noise-ratio (PSNR) in dB and mean-structural-similarity-index-measure (MSSIM) [15] as distortion measure for the watermarked images, while normalized cross-correlation (NCC) value to quantify the quality of extracted watermark.

Table 1 illustrates PSNR (dB) and MSSIM values before and after watermark decoding process for four popular test images. A normal user without the knowledge of key can view poor quality images with PSNR (dB) as shown in column 2 of Table 1. However, a user with a valid key can decode/enjoy a superior quality image with PSNR (dB) shown in 5th column. Fig. 4 provides a visual comparison between images before and after removal of embedded watermark through decoding process. Figs. 4 (a) and 4(c) show the watermarked images after embedding the corresponding watermark digest of size (32×32) shown in Fig. 3(c), while Figs. 4 (b) and 4(d) are the same after self-noise suppression in spatial and DCT domain, respectively. The symbols 'P' and 'M' associated with numerical values indicate PSNR in dB and MMSIM values. If quality access control application requires relatively low quality images to the general/unauthorized users, watermark power can be increased by using large step size (Δ) during implementation.

From Table 1 it is clear that implementation in both the domains offer almost similar image fidelity after watermark insertion (although DCT domain implementation offers a little better) and the image characteristics does not show greater impact on the fidelity of the watermarked image.

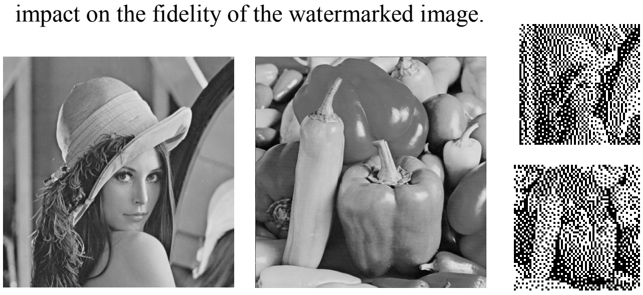
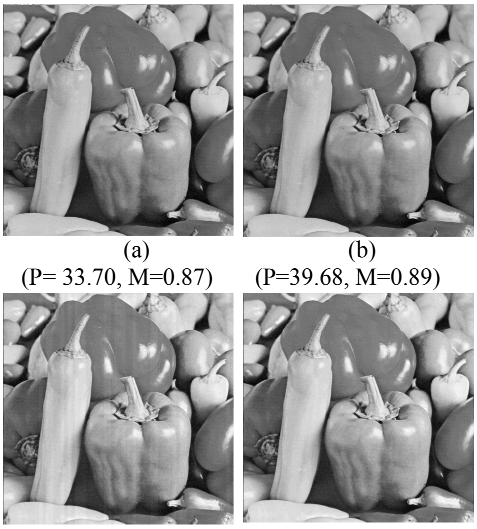

(a) (b) (c)

Fig. 3. Test images; (a): Lena; (b) Pepper (c) Watermark digest.


(P=33.46, M= 0.87) (P=38.24, M= 0.94)

(a) (b)

(P= 33.70, M=0.87) (P=39.68, M=0.89)

(c) (d)

Fig. 4. (a): Watermarked image in spatial domain, (b) decoded image of (a), (c) watermarked image in DCT domain, (d) decoded image of (c).

Table 1. PSNR (dB) and MSSIM before and after self-noise suppression

	Before Decoding			**After Decoding**	
Name of Image	***PSNR (dB)***	***MSSIM***	***NCC***	***PSNR (dB)***	***MSSIM***
Spatial Domain					
Lena	33.48	0.87	1	38.66	0.94
Pepper	33.46	0.87	1	38.24	0.94
Boat	33.47	0.90	1	38.32	0.93
Babbon	33.47	0.95	1	38.65	0.94
Full frame DCT					
Lena	33.63	0.87	1	39.72	0.96
Pepper	33.70	0.87	1	39.68	0.95
Boat	33.52	0.90	1	39.56	0.95
Babbon	33.92	0.96	1	39.63	0.96

To test robustness of the proposed data hiding scheme, some typical signal processing operations are performed on watermarked images. Robustness against such operations is essential as it is expected that an unauthorized user may distort the watermarked image with an objective that the users with valid commercial agreement would also be unable to avail better quality of the images. The comparative experimental results between spatial and full frame DCT domain are shown in Table 2.

Table 2. Results of test image with different image/signal processing operations

Stren-gth		**PSNR Before Deco.**	**M - SSIM Before Deco.**	**PSNR After Deco.**	**MSSIM After Deco.**	**NCC**
Median Filtering						
3×3	Spatial	31.91	0.82	33.16	0.83	0.91
	DCT	33.84	0.87	32.78	0.84	0.72
Mean Filtering						
3×3	Spatial	30.47	0.86	31.10	0.85	0.70
	DCT	31.38	0.87	30.64	0.85	0.84
High pass Filtering						
1.8	Spatial	20.06	0.82	20.39	0.80	0.38
	DCT	20.37	0.81	20.43	0.81	0.80
Down & Up Sampling						
0.90	Spatial	33.21	0.89	34.88	0.89	0.92
	DCT	34.71	0.90	33.91	0.88	0.87
0.75	Spatial	32.47	0.88	33.72	0.88	0.84
	DCT	33.83	0.89	32.92	0.87	0.81
Histogram Equalization						
	Spatial	19.95	0.68	20.13	0.68	0.40
	DCT	19.96	0.67	19.99	0.66	0.53
Dynamic Range Change						
[50-200]	Spatial	21.36	0.86	21.32	0.83	0.28
	DCT	21.36	0.86	21.37	0.86	0.93
Salt & Pepper Noise						
0.001	Spatial	31.29	0.85	32.99	0.88	1
	DCT	31.54	0.85	32.26	0.85	0.96
0.005	Spatial	27.10	0.76	27.65	0.79	1
	DCT	27.29	0.77	27.39	0.75	0.50
0.009	Spatial	25.23	0.69	25.57	0.72	1
	DCT	25.23	0.70	25.30	0.69	0.51
Speckle Noise						
0.001	Spatial	31.23	0.78	32.27	0.79	0.71
	DCT	31.42	0.78	32.04	0.78	0.91
0.005	Spatial	27.12	0.60	27.40	0.60	0.51
	DCT	27.16	0.60	27.20	0.59	0.50
0.009	Spatial	25.05	0.51	25.24	0.51	0.62
	DCT	25.03	0.51	25.06	0.50	0.50
Gaussian Noise						
0.001	Spatial	19.92	0.23	19.95	0.25	0.50
	DCT	19.92	0.25	19.93	0.25	0.56
0.005	Spatial	19.96	0.25	19.97	0.25	0.50
	DCT	19.94	0.25	19.95	0.25	0.49
0.009	Spatial	19.91	0.25	19.91	0.25	0.50
	DCT	19.89	0.25	19.90	0.25	0.51

Numerical values are obtained as the average value of 100 independent experimentations conducted over 250 test images having varied image characteristics. It can be seen that proposed data hiding based access control scheme can successfully resists attacks like median, mean, highpass filtering of mask size (3×3) each, sampling, histogram equalization and lossy JPEG compression at quality factor 50. Figs. 5 and 6 show the improvement in quality PSNR (in dB) and MSSIM, respectively after watermark decoding process i.e. self-noise suppression. From Figs. 5–6, it is also clear that the scheme can extract watermark effectively up to JPEG 50 and would be effective for quality access control. However, there is an overall degradation in PSNR and MSSIM values at low quality factor due to quantization in compression operation.

We have studied the effect of different watermark powers WP (dB) on the fidelity of the watermarked images. The watermark power is defined as

$$WP = 10\log_{10}\frac{\Delta^2}{12} \text{ dB} \qquad (11)$$

where the symbol Δ corresponds to the step size used for watermarking. Table 3 shows the variation of PSNR (dB) and MSSIM for different WP (dB). From Table 3 it is clear that the increase in WP (dB) would decrease the fidelity of the watermarked image, which is not appealing to an unauthorized user who does not have knowledge of key. However valid user is capable of regenerating the better quality of the host image data through self-noise suppression. The numerical values in Table 3 also highlight that the relative gains in PSNR vary from ~2.91 dB to ~3.02 dB, with the increase of watermark power from 7.27 dB to 15.22 dB (as depicted in Table 3) in spatial domain, while in DCT domain the similar values vary from ~ 2.44 dB to ~2.26 dB.

Table 3. Variation of quality for different WP (dB).

WP (dB)	**7.27**	**10.03**	**13.81**	**15.22**
Delta	8	11	17	20
Spatial Domain				
PSNR (Before)	37.94	35.12	31.31	29.86
MSSIM (Before)	0.95	0.91	0.81	0.75
PSNR (After)	40.85	38.09	34.33	32.88
MSSIM (After)	0.96	0.93	0.86	0.82
Full frame DCT				
PSNR (Before)	38.23	35.72	31.93	30.72
MSSIM (Before)	0.95	0.91	0.82	0.78
PSNR (After)	40.67	37.79	34.03	32.98
MSSIM (After)	0.96	0.93	0.85	0.82

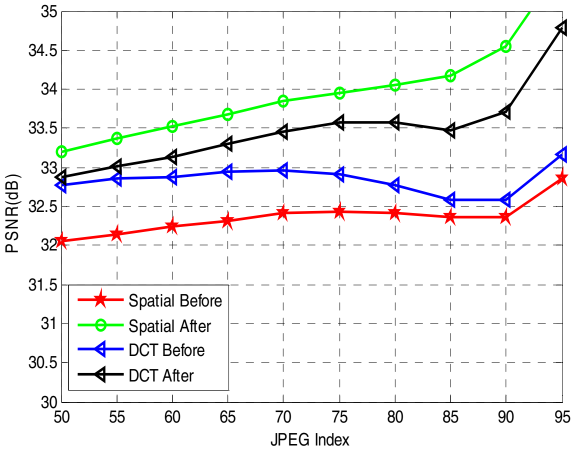


Fig. 5. Access control performance after JPEG in PSNR.

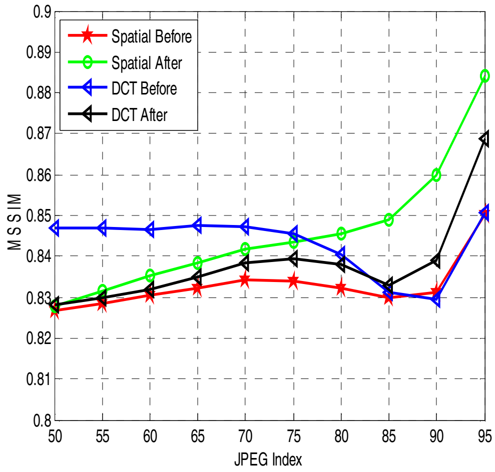


Fig. 6. Access control performance after JPEG in MSSIM.

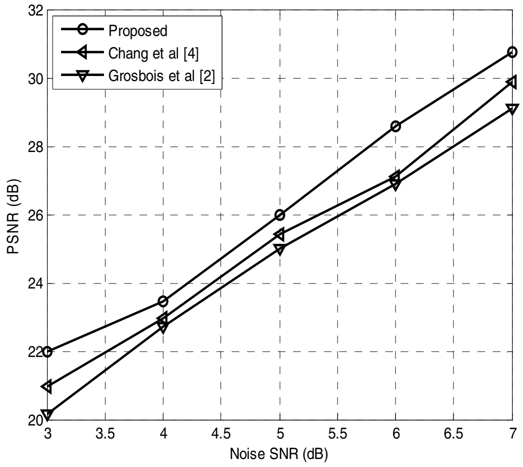


Fig. 7. PSNR (dB) after decoding images for different channel SNR.

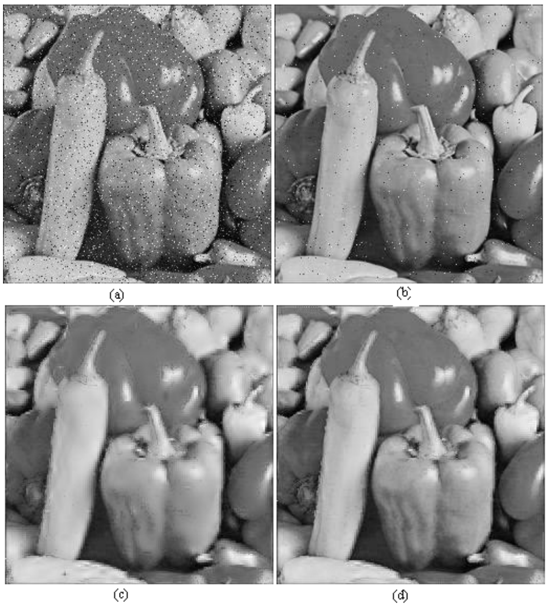


Fig. 8. Results under fading: (a) high; (b) medium; (c-d) results after concealment of (a-b), respectively.

Finally, we compare the performance of the proposed data hiding scheme for access control and error concealment with that of other methods against fading like operation. To this aim, data transmission is accomplished using multicarrier code division multiple access (MC-CDMA) through Rayleigh fading wireless channel with signal-to-noise-ratio (SNR) varying from 3 dB to 7 dB [16]. Small values of SNR represent that the channels are under deep fade, while high values of SNR represent the reverse. Fig.7 shows PSNR values of watermark decoded image (after removing the embedded watermark) vs SNR when corrupted by additive noise. De-noising is not done here but the effect of watermark removal highlights its suitability for access control. Fig. 7 shows that proposed method offers the best performance compared to [4] and [2] for access control. This is due to the fact that in [4], the decoding of one frame (image) depends on the previous frame (image). So if a frame when is decoded wrongly, it has an effect on subsequent decoding. On the other hand, the scheme in [2] shows poor value of quality as the decoding is scrambling based. An error in an encrypted data may lead to partially failed decryption and ultimately results in poor image quality after decoding.

Instead of self-noise suppression, a valid user can use the extracted image digest and improves image quality through error concealment. Figs. 8 (a) and (b) show received 'Pepper' images after passing through the fading channels when SNR values are 3 dB and 7 dB, respectively. Figs. 8 (c) and 8(d) show error concealed images of Figs. 8 (a) and (b), respectively. Numerical values for PSNR and MSSIM for the images shown in Fig. 8(a) and 8(b) are 19.10 dB, 0.36 and 23.55 dB, 0.74, respectively, while the same quantitative measures for Fig. 8(c) and 8(d) are 24.15dB, 0.78 and 25.38, 0.81 respectively. Relatively significant improvement in visual quality in other way suggests that proposed data hiding based error concealment scheme is very much effective for the deeply faded channel. Results show that proposed error concealment scheme can also be applied for the estimation of channel parameters for transmission of image and video signal over fading channel. Embedded watermark i.e. image digest may act as pilot signal without affecting the problem of bandwidth and synchronization like the existing pilot based system. Performance of the proposed method is compared with other data hiding [9, 10, 11] based methods designed for the application of error concealment. It is found from the results of Table 4 that our method offers best PSNR values even if packet loss rate (PLR) increases to 20%. This improvement is due to orthogonalization of host samples/coefficients in embedding space followed by stable decision statics obtained from the weighted average of N- independent decision statistics.

Table 4. Error concealment performance

PLR	3%	5%	10%	15%	20%
Lie et al. [11]	35.62	34.98	33.34	32.43	31.35
Wu et al. [10]	34.07	28.43	27.11	25.16	24.98
Ma et al. [9]	35.51	34.00	28.12	26.57	24.10
Proposed	39.10	38.30	36.55	34.07	32.55

4. CONCLUSIONS AND SCOPE OF FUTURE WORKS

This paper proposes a new model of QIM based data-hiding scheme for dual purpose of quality access control and error concealment of digital images. Watermark embedding on orthogonal components and subsequent decoding from the weighted average of N-decision statistics result in nearly 8% improvement in quality (PSNR) over traditional QIM based scheme. Simulation results also show that ~ 4.5 dB and ~2.5 dB improvement in PSNR are possible to achieve through error concealment at SNR 3 dB and 7 dB, respectively in frequency selective Rayleigh fading channel. Future work would explore this concept for synchronisation problem in audio watermarking as well as estimation of wireless channel parameter.

5. REFERENCES

[1] A. Phadikar, S. P. Maity and C. Delpha, "Image Error concealment and quality access control based on data hiding and cryptography," *Telecommun. System*, DOI 10.1007/s11235-010-9371-6.

[2] R. Grosbois, P. Gerbelot, and T. Ebrahimi, "Authentication and access control in the JPEG 2000 compressed domain," *Proc. 46th SPIE Annual Meeting, Applications of Digital Image Processing*, San Diego, pp. 95-104, 2001.

[3] S. Imaizumi, O. Watanabe, M. Fujiyoshi, and H. Kiya, "Generalized hierarchical encryption of JPEG 2000 code streams for access control," *Proc. IEEE International Conference on Image Processing*, Genoa, Italy, p. 1094-7, 2005.

[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 Netherland)*, vol. 49, no. 3, pp. 443 – 455, 2007.

[5] J. A. Bloom, I. J. Cox, T. Kalkar, J-P. Linnartz, M. L. Miller and B. Traw, "Copy protection for DVD video," *Proceedings of the IEEE.*, vol.87, pp. 1267-1276, 1999.

[6] A. Phadikar, M. K. Kundu, and S. P. Maity, "Quality access control of a compressed gray scale image," *Proc. National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics*, India, pp. 13-19, 2008.

[7] A. Phadikar, and S. P. Maity, "Quality access control of compressed color images," AEÜ - *International Journal of Electronics and Communications*, Elsevier, vol. 64, pp. 833–843, 2010.

[8] A. Phadikar, and S. P. Maity, "ROI based error concealment of compressed object based image using QIM data hiding and wavelet transform,'' *IEEE Trans. on Consumer Electronics,* vol. 56, pp. 971-979, 2010.

[9] M. Ma, O. C., Chan, S. H. G, and M. T. Sun, "Edge directed error concealment," *IEEE Trans. on Circuits and Systems for Video Tech*., vol. 20, no. 3, pp. 382–395, 2009.

[10] J. Wu, X. Liu, and Y. K. Yoo,, "A temporal error concealment method for H.264/AVC using motion vector recovery," *IEEE Trans. on Consumer Electronics*, vol. 54, no. 3, pp. 1880-1885, 2008.

[11] W. N. Lie, T. C. I. Lin, D. C. Tsai, and G. S. Lin, "Error resilient coding based on reversible data embedding technique for H.264/AVC video," *Proc. ICME*, Amsterdam, Nedherland, pp. 1174-1177, 2005.

[12] Q. Li, and I.J. Cox, "Using perceptual models to improve fidelity and provides resistance to valumetric scaling for quantization index modulationwatermarking," *IEEE Trans. on Information Forensics and Security*, pp. 127–139, 2007.

[13] R. Floyd and L. Steinberg, "An adaptive algorithm for spatial gray scale," *Proc. of SID International Symposium Digest of Technical* Papers, pp. 36-37, 1975.

[14] J. G. Proakis, "Digital Communication," McGraw Hill, Fourth Edition, 2001.

[15] 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, no.1, pp. 1-14, 2004.

[16] S. P. Maity and M. Mukherjee, "Subcarrier PIC scheme for high capacity CI/MC-CDMA system with variable data rates," *Proc. of IEEE Mobile WiMAX'09*, Canada, pp. 135-140, 2009.