AIVP ADVANCES IN IMAGE AND VIDEO PROCESSING
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 3
ISSN: 2054 - 7412

On Integration of Error Concealment and Authentication in JPEG2000 Coded Images

Qurban A Memon
Associate Professor, EE department, UAE University, Al-Ain 15551, United Arab Emirates
qurban.memon@uaeu.ac.ae

ABSTRACT

Nowadays, it is widely understood that data compression is not only essential to speed up the transmission rate but also to provide other gains like low storage. In order to counter data manipulations and tampering during transmission, the image authentication has turned out to be equally important. But the drawback of compressed data transmission is that the compressed data are susceptible to channel impairments. In this paper, an error concealment approach is integrated with low cost image authentication scheme to benefit better visual quality as well as content author and user satisfaction. The image authentication includes content based digital signature that is watermarked and diffused in the whole image before JPEG2000 coding. To tackle noise, the error detection and concealment technology is examined to include edge information as part of error concealment approach. The edge image is sent along with JPEG2000 coded image to determine corrupted coefficients. The simulation results are conducted on test images for different values of bit error rate to judge confidence in noise concealment within the received images**.**

1 INTRODUCTION

The two common standards to compress and code images before transmission and storage are JPEG and JPEG2000. The JPEG standard is based on the discrete cosine transform (DCT) while JPEG2000 is based on the Wavelet transform. JPEG is the older standard and still widely used. The JPEG2000 is the newer standard.

Data compression reduces the use of channel bandwidth; however compressed data are more vulnerable to channel noise. Therefore, the transmitted data must be resilient to channel noise and other impairments due to channel coding of binary bits [1-4]. Several techniques have been proposed in the literature to address the problem of transmission errors by making transmitted data more robust to channel noise and to conceal corrupted data at the receiver. The authors in [5] present a scalable scheme for robust JPEG 2000 images and video transmission to multiple wireless clients, using an adaptive bandwidth estimation tool. In

DOI: 10.14738/aivp.23.313
Publication Date: 30th June 2014
URL: http://dx.doi.org/10.14738/aivp.23.313

another research work [6], the authors present the results of an initiative to transmit imagery content through a Link-16 tactical network using JPEG2000 compatible approach (involving wavelets to compress images). Specifically, the JPEG2000 code-stream is mapped into Link-16 free-text messages. The most important part of the JPEG2000 compressed image is transmitted through a more error resistant (and anti-jamming) Link-16 packed structure and the remaining of the image in less robust data structures but at higher data rates. The results presented are preliminary and dependent on Link-16 network resources.

The need for high compression and artifacts free imaging has made JPEG2000 a capable and sustaining algorithm that is replacing the current JPEG which is applied and used till today [7]. The discrete version of Wavelet Transform in two dimensions is called two dimensional discrete wavelet transform (2-D DWT). The implementation requires digital filers and down-samplers. In JPEG2000, typically images are decomposed to five wavelet levels to accomplish higher compression ratio. In multimedia communication and data storage, the drawback of compression is that the compressed data are vulnerable to channel noise during transmission. The area of compressed data transmission through noisy channels is still active in research, and needs further investigation. On the other hand, authentication of transmitted data is equally important to justify all image transmission related activities. Recently, protection of image data transmitted or stored over open channels is also getting serious attention.

The paper is structured as follows. In the next section, the literature review is presented to highlight important contributions to this area of research. The section III details proposed approach. In section IV, the experiments conducted on test images are discussed and results presented. The section V presents discussion on these test results, followed by conclusions in section VI.

2 LITERATURE REVIEW

Typically, watermark techniques protect the right of service providers, while digital signature covers customers. As an example, a customer wants to verify the seller of the image and that the purchased image is in fact bought from the legal one. In this case, digital signature comes as a useful tool. In terms of approaches, for example, in [8], the authors investigate the invariant features, which are generated from fractionalized bit-planes during EBCOT (Embedded Block Coding with Optimized Truncation) procedure in JPEG2000. These are then coded and signed by the sender's private key to generate one crypto signature (hundreds of bits only) per image, regardless of the image size. The authors in [9] discuss a scheme, where scalability and robustness is achieved by truncating bit planes of wavelet coefficients into two portions in JPEG2000 codec based on lowest compression bit rate (CBR). The invariant features, which are generated from upper portion, are signed by the sender’s private key to generate a crypto-signature. By embedding the signature in upper portion, the scheme has the ability for content authentication as long as the final transmitted bit rate of the image is not less than the lowest CBR. In another work [10], a secure encryption scheme is proposed, where only some sensitive precincts of the entire image are encrypted. Thus, the code stream is parsed to select only packets containing code-blocks which belong to the selected precincts. The remaining packets are sent without encryption.

The authors in [11] select LL coefficients as authentication code (AC) since root nodes preserve the most important energy. To embed AC in image with imperceptibility, AC is further scaled and rearranged into bit planes. The embedding procedure inserts the AC bit plane into multi-resolution images according to progressive image transmission. In [12], the authors employ Dugad technique [13] to resolve security issues in medical images by adding watermark technology to JPEG2000 compression. The authors in [14] have proposed watermarking and image authentication scheme to be performed in the frequency domain (with DCT coefficients). The authors claim to integrate ownership (through watermarking) and integrity of the image through signature process.

In [15], the main features of the proposed authentication system include integration of both content based (semi-fragile) authentication and code-stream based (complete) authentication into one unified system. This gives users more freedom to choose a proper type of authentication according to their specific requirements in the application.

***Scrambling and Encryption**:* Recently, a great deal of concern has been raised regarding the security of an image transmitted or stored over public channels. The authors in [16] have proposed a new image encryption algorithm using random pixel permutation based on chaos logistic maps and prime modulo multiplicative linear congruential generators. In another work [17], a neural network based encryption has been suggested as a part of encryption and decryption. At the receiving end, it uses neural network to obtain the original image. Scrambling has also been investigated by many authors for example in [18], where authors achieve encryption by dividing the image into random overlapping square blocks, generating random iterative numbers and random encryption order, and scrambling pixels of each block using Arnold transform. In another work [19], the authors use fast image scrambling algorithm using a multidimensional orthogonal transform and a cipher image. The security is achieved by a large number of multi-dimensional orthogonal sequence. The authors in [20] use wavelet decomposition to apply encryption on high-frequency sub-band image. After that, wavelet reconstruction is introduced in order to spread the encrypted part throughout the whole image. A second encryption process follows to complete the encryption process.

***Noise Removal*:** Once data is received at the receiver, errors are detected and if possible, they are also corrected. Since compressed data are more vulnerable to channel noise, therefore, the transmitted data must be resilient to channel noise and other impairments. The techniques to address this problem have been classified into three groups. The first technique is Forward Error Concealment in which the encoder makes the data more immune to transmission errors with the objective to decrease corresponding effect to a minimum. The second technique is error concealment by post processing, where the decoder a major job in concealing errors without depending on additional data from the encoder. The third technique is interactive error concealment (IEC) in which the encoder and decoder work jointly through a feedback channel to minimize the impact of transmission errors. As a reference, various error concealment errors are discussed in [21].

Summary of Issues: Though image authentications techniques have grown to be mature technologies, but the current state of the art approaches do not completely solve the problem of unauthorized copying, provide protection from digital data privacy and image authentication through noisy channel. Furthermore, there exist many image editing applications that enable easy manipulation of image data, and this problem becomes serious in applications like medical imaging and area surveillance. In this work, an approach is investigated that collectively addresses security and privacy of (compressed) image data transmitted through noisy channels. Noise removal and image authentication at different levels are the main contributions of this work.

3 PROPOSED APPROACH

In this section, an approach as shown in Figure 1 is presented that achieves two major objectives in image transmission: (i) embeds authentication in JPEG2000 image before transmission, (ii) uses edge image to help in identifying corrupted regions, in the receiver. Each of the steps, as shown in Figure 1, is discussed as follows:

3.1 Edge Extraction

Edge detection is the most useful approach in detecting valuable or important changes in the value of the intensity. This kind of detection is achieved using first order or second order derivative of intensity values. When there is a change in the intensity, the direction of the gradient vector can be determined by calculating the angle of the maximum rate of change. This also means that where ever there is a detection of an edge, there is going to be an important difference between the pixels. This kind of difference denotes the level variation between intensity densities. Moreover, one of the reasons that could make this variation high is the existence of high frequency (noise) at that area. At the transmitter, the N_L-scale wavelet transform is applied as a first step in JPEG2000 coding standard, and the edge image is extracted from these wavelet coefficients. For the purpose of edge detection, Canny edge detector [22] with convenient thresholds is applied to the wavelet transformed image. The resulting binary edge_image undergoes scrambling to protect data and lossless compression to minimize transmission overhead through noisy channel, as discussed below.

3.2 Scrambling

In literature [23], it has been shown that block level scrambling provides better results than pixel based scrambling, and that it is computationally efficient. For the same purpose, sub-bands of the edge image are decomposed into non-overlapping blocks of pixels, with block size dependent on the level of scrambling. In the next step, these blocks are permuted using 2-D Arnold transform, and these permutations again depend on the level of scrambling. The 2-D Arnold transform is given as [23]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & \mathrm{b} \\ \mathrm{a} & 1+\mathrm{ab} \end{bmatrix} \begin{bmatrix} \mathrm{x} \\ \mathrm{y} \end{bmatrix} \bmod (\mathrm{N}) \tag{4}$$

where *N* is the order of the image matrix, and *a*, *b* being positive control parameters are further randomly generated through 2-D coupled logistic map, given below:

$$\begin{aligned} \mathrm{x}_1(\mathrm{n}+1) &= \mu_1\, \mathrm{x}_1(\mathrm{n})\,(1-\mathrm{x}_1(\mathrm{n})) + \gamma_1\, \mathrm{x}^{2}{}_{2}(\mathrm{n}) \\ \mathrm{x}_2(\mathrm{n}+1) &= \mu_2\, \mathrm{x}_2(\mathrm{n})\,(1-\mathrm{x}_2(\mathrm{n})) + \gamma_2\, (\mathrm{x}^{2}{}_{1}(\mathrm{n}) + \mathrm{x}_1(\mathrm{n})\mathrm{x}_2(\mathrm{n})) \end{aligned} \tag{5}$$

This logic map has three coupling terms to show its complexity. It is shown in [23] that the map is chaotic if $2.75 < \mu_1 \le 3.4$, $2.7 < \mu_2 \le 3.45$, $0.15 < \gamma_1 \le 0.21$, $0.13 < \gamma_2 \le 0.15$. Thus, the chaotic sequence in equation (5) is generated for $0 < x_1, x_2 < 1$, and then *a*, and *b* are generated through x_1 and x_2. Once *a*, and *b* are generated, then equation (4) is applied on blocks of each sub-band of the edge image, up to k-level scrambling, to get the overall scrambled image. Since the steps of this scrambling are deterministic, it seems easy to apply it in reverse order to descramble image at the receiver. It should be noted that since higher subbands of the edge image contain relatively little visual information about the edge, hence scrambling can only be applied to lower band subbands and leaving higher subbands untouched.

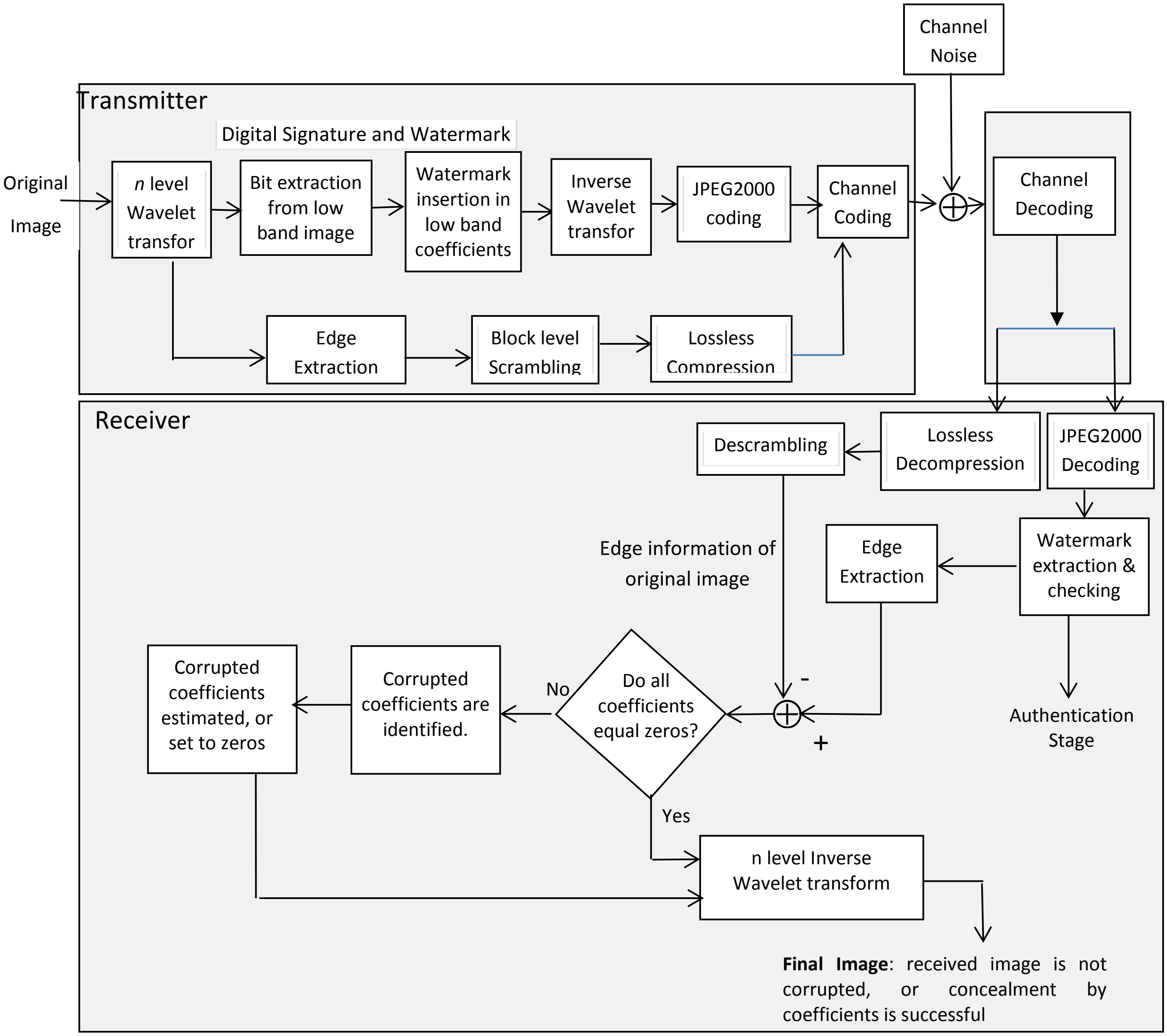
Channel Noise
Transmitter
Digital Signature and Watermark
Original Image
n level Wavelet transfor
Bit extraction from low band image
Watermark insertion in low band coefficients
Inverse Wavelet transfor
JPEG2000 coding
Channel Coding
Edge Extraction
Block level Scrambling
Lossless Compression
Channel Decoding
Receiver
Descrambling
Lossless Decompression
JPEG2000 Decoding
Edge information of original image
Edge Extraction
Watermark extraction & checking
-
+
Authentication Stage
Corrupted coefficients estimated, or set to zeros
Corrupted coefficients are identified.
No
Do all coefficients equal zeros?
Yes
n level Inverse Wavelet transform
Final Image: received image is not corrupted, or concealment by coefficients is successful

Figure 1: Block diagram of Proposed Algorithm

3.3 Lossless Compression:

The objective of this step is to reduce the size of overhead that results due to transmission of the encrypted edge_image. The lossy approach can't be used here as the edge image is to be used for error concealment in the received image, thus any lossless compression scheme that reduces the size of this overhead can be used. Since higher subbands of the edge image contain a lot of zeros, the lossless compression of these bands would yield a bigger compression gain. In this approach, run length encoding is adopted for simplicity. The idea is pick up identical patterns present in the binary edge image and represent them as *nd*, where *n* is the number of consecutive occurrences, and *d* is the data string.

3.4 Embedding Authentication:

In order to present digital signature extraction and watermark insertion into image, it is seems reasonable to define parameters. For simplicity, we assume image and block of square size. Let original image $f(x, y)$ be of size N x N, and its low band subband be represented as LL_n (i, j), where n represents the decomposition scale of the image and i, j are indices of the image band in the range $0 \leq i \leq N/2^n$ and $0 \leq j \leq N/2^n$. In order to extract digital signature from the image, it is proposed to divide the lowest image subband into blocks S_k (k=1, 2, 3, .., M) to enable bit extraction across whole subband image. The total extracted number of bits is MxL, where L is number of bits generated per block. Moreover, it seems satisfying for customers and image providers to have content dependent digital signature extracted from within the image rather than selecting external bits as digital signature, and sent separately across the channel. These extracted bits are later inserted as watermark in the same subband. Though the approach of digital signature extraction and its insertion as watermark may help in detecting channel manipulation of bits at the receiver, but at the moment it is not addressed in this approach.

3.5 Digital Signature

The digital signature extraction is based on two main points: (a) any low band image coefficient cannot be made larger or smaller without causing significant perceptional changes to the image, thus all similarly looking blocks (whether watermarked, un-watermarked, or attacked) in the wavelet transformed low band image will have same signature bits (b) a variable threshold is used in generating bits from the low band image blocks in such a way that 50% of the projections lie on either side of the threshold to ensure maximum information content in extracted bits. The adaption of the threshold is done to counter changes in information content from block to block due to data manipulations, for example certain image processing operations such as histogram stretching, watermarking, noise adding, compression, filtering, etc. In order to extract bits from low band subband, a secret key K (to be chosen, say by image provider or author) is used to generate L random sequences with values uniformly distributed in the interval {0, 1}. These matrices are later smoothed out by a low pass filter, and made zero mean to represent subband variations only. Later, image block S_k, as a vector, is projected on each zero mean smoothed random pattern L_i, and then its absolute value is compared with a threshold to generate corresponding bit c_i, as follows:

$$c_i = 1, \ \ if \ |S_k. L_i| > 0 \qquad (6)$$

$$c_i = 0, \ \ if \ |S_k. L_i| < 0$$

Based on this approach, it can be easily seen that (i) resulting projected values change with a change in K (ii) resulting projected values change if S_i is dissimilar than S_j where $i \neq j$. Thus, bits c_i are sensitive to key K and vary continuously with subband block S_k.

3.6 Watermarking

As described above, the signature bits that are extracted from LL_n are inserted back as watermark in the lowest subband. This is ensured by using a quantization process, and mean amplitude of the lowest subband. Furthermore, it is desired that inserted watermark be extracted without having access to the original image, and that process be robust against common image processing application such as JPEG compression. Mathematically, watermarking process can be described as:

$$LL'_{n} = W_F\ (LL_n,\ c,\ K) \tag{7}$$

where $LL_{n'}$, W_F, LL_n, c, K represent watermarked subband, watermark (forward) coding process, unwatermarked subband, signature bits and key respectively. Similarly, the inverse process can be described as:

$$c' = W_R\ (LL'_n,\ K) \tag{8}$$

where c' and W_R represent recovered bits and watermark (reverse) coding process respectively. Finally, c and c' go through similarity index check using a threshold T_2 to determine whether correct watermark has been recovered.

For embedding watermarking bits into the subband, the procedure starts as follows:

i. Select embedded intensity as a quantization step size B_t, and calculate the mean m_k of each block S_k. Set $b_k = int\ [m_k/B_t]$.

ii. Compute the difference $diff_k$ as:

$diff_k = abs\ (b_k - \text{trunc}\ [m_k/B_t])$

iii. Modify b_k using c_k, b_k and $diff_k$ as:

If b_k *is an odd number and* $c_k = 0$,

OR if b_k *is an even number and* $c_k = 1$, *then*

$b'_k = \{\ b_k + 1$ *for* $diff_k = 0$

$b_k - 1$ *for* $diff_k = 1\}$ *else* $b'_k = b_k$

iv. Update wavelet coefficients of block S_k of $LL_n\ (i, j)$ as:

$LL_{nk}\ (i, j) = LL_{nk}\ (i, j) + (b'_k \times B_t - m_k)$

where $LL_{nk}\ (i, j)$ stands for wavelet coefficient (i, j) of block S_k in lowest subband.

v. Compute and save new mean m_t of $LL'_n\ (i, j)$, and construct watermarked image using inverse wavelet transform.

Once the image arrives at the receiver, the watermarked bits are extracted as follows:

i. The mean m_r of the received lowest subband $LL_n^{-}(i, j)$ is calculated, and difference is computed as:

$\delta_m = m_r - m_t$

ii. The received lowest subband $LL_n^{-}(i, j)$ is decomposed into blocks S^{-}_k and mean m^{-}_k is calculated.

iii. Compute the quantization value as:

$B_r = int\ [(m^{-}_k - \delta_{m)}/\ B_t]$

iv. Extract the embedded bit as:

If B_r is even, then $c_k = 0$, else $c_k = 1$.

3.7 JPEG2000 and Channel Coding

Once the watermarked image is available, it is ready for JPEG2000 coding and transmission through noisy channel. Furthermore, scrambled and lossless compressed edge image is also ready for transmission through the same channel. As the size of compressed edge image is significantly lower than the original image, it can be coded using robust channel coding schemes to void distortion due to noise. Thus it is assumed that it is correctly received at the receiver. So at the receiver, watermarked-noisy-compressed image and noise free lossless-compressed edge image are received. The channel noise assumed is the burst noise i.e., the two-state Markov channel model is used to represent bursty noise channel. This noise is added to transmitted data before it reaches the receiver.

3.8 Receiver operations

The receiver steps follows exactly as shown in Figure 1. The steps just invert the operations stated in sections *e*, *d*, *c*, *b*, and *a* respectively. Once edge is extracted from wavelet coefficients image, it is termed as extracted edge image respectively. Next extracted edge image is subtracted from the received edge image of the original image. If the difference between the received edge image and the extracted edge image is zero or below a certain threshold level then the received image is correct or corruption is unobjectionable. In the case where the received edge image differs from the extracted edge image at different regions, these regions are marked as corrupted regions. In JPEG2000, the corrupted regions will have different sizes since the wavelet coefficients at different levels represent different sizes of blocks in the reconstructed image. The block sizes can range from 2 by 2 pixels to 32 by 32 pixels, and generally this depends how many levels of wavelet transform are computed at the transmitter. The spatial pattern of the corrupted region may help to determine if the corrupted region is in the horizontal, vertical, or diagonal *sub-band*.

Concealing errors at higher *sub*-band**:** This step deals with existence of the corrupted regions or blocks in received wavelets coefficients. The location of the corrupted block in the received wavelet coefficients may be used to determine the location of the wavelet coefficient within the *sub-band*. Effectively, all of these sub-bands may be processed in parallel to determine corrupted wavelet coefficients. Once it is possible to locate the corrupted wavelet coefficients, then their values may be set to zero if the coefficients belong to higher sub-bands at higher level lower level or may be estimated by adjacent coefficients if the coefficients belong to higher sub-bands at lower level. Then the image is reconstructed. The loss of image information by setting the values of the wavelet coefficients to zero is unobjectionable especially for coefficients located at higher *sub-bands*.

Concealing errors at lower *sub-band:* If the corrupted coefficients are in the lower *sub-band* then it is proposed to estimate their values from the neighborhood of affected coefficients. For example, if the corrupted coefficients are the approximation coefficients, then it is proposed to estimate their values using the uncorrupted adjacent approximation coefficients.

4 EXPERIMENTAL SETUP AND RESULTS

A set of five 1024×1024 8-bit monochrome images were selected based on various image details to test the approach presented in the previous section. The Figure 2 shows these images: *woman* and *pirate* images (with low image detail), *boat* and *goldhill* (with medium level of detail) and *baboon* image (with large image detail). All of these images were transformed using an arbitrary five-scale (N_L=5) wavelet transform with implicit quantization μ_0=8 and ε_0= 8.5.

A canny edge detector with convenient thresholds was applied on wavelet coefficients sub-images in order to extract the edge image. The resulting binary image, termed as 'edge_image' undergoes scrambling. It should be noted that, as discussed in previous section, only lowest subband undergoes scrambling. Once initial block size is selected, at each level the blocks are permuted using the equation 4. The arbitrary values (to be used in equation 5) for initial conditions and parameters for secret key selected were: x_0=0.0215, y_0=0.5734, μ_1=2.93, μ_2=3.17, γ_1=0.197, γ_2=0.139, and t=100. The values a and b are then generated as in [23]. The final scrambled image is reached once number of levels starting from $y=1$ reaches $log_2(Y)$-1, where Y is the initial block size.. All variables were set to double with 15-digit precision, and decimal fractions of the variables are multiplied by 10^{14}. The scrambled subbands levels together with remaining binary edge image subbands were then losslessly compressed using run length coding.

The next step on the transmission side is to embed authentication in the image. As discussed in the previous section, only lowest subband is to be used for digital signature extraction and watermark insertion. For signature extraction, first the lowest subband image is divided into blocks of arbitrary size of 8x8 pixels, thus generating 16 blocks. Using an author name as secret key, L=32 random sequences were generated with values uniformly distributed in the interval {0, 1}, followed by smoothing, and zero mean steps. Each subband block is finally projected onto each random sequence (and using equation 6) to generate a total of 16x32 = 512 signature bits. In order to insert these signature bits back into lowest subband as a watermark, the quantization step size was arbitrarily selected as B_t = 10. Using the watermarking algorithm stated in previous section, the wavelet coefficients of each block in the lowest subband are modified. The mean m_t of resulting coefficients in the lowest band is also saved. Finally, inverse wavelet transform is applied on the modified wavelet coefficients together with remaining subbands to generate watermarked image.

The watermarked image finally undergoes JPEG2000 coding using an arbitrary five-scale (N_L=5) wavelet transform, with implicit quantization μ_0=8 and ε_0= 8.5. The resulting JPEG2000 coded image together with mean value m_t and edge image were channel coded before transmission. The size of wavelet coefficients resulting from JPEG2000 coding and watermarked image together with mean value is 1024KB, whereas edge image size is ~3KB only. Since edge image is required to be with zero distortion at the receiver, this is coded with channel coding technique to withstand noise in the channel. This step added up to 5KB extra to the edge image. The added noise to the channel is the burst noise, which was simulated by two-state Markov channel model. After generating the two-state Markov noise, this noise (with bit error rate equal to 0.004, 0.006, 0.009 to represent different noise scenario) was added logically to the binary Huffman coded data. The method of addition was done simply by applying the exclusive OR logical operation and the result was an image with noise distortion. The image mixed with noise is transmitted using JPEG2000 protocols and was the one received at the receiver.

Figure 2: Test images (a) *woman* (b) *pirate* (c) *goldhill* (d) *boat and* (e) *baboon*

After data is channel decoded, two images are available. One is the lossless compressed image that undergoes inverse operations done at the transmitter. Firstly, it undergoes lossless decompression followed by descrambling exactly in reverse order of transmission. Since this image was channel coded using a robust channel code, hence there was no distortion in the received edge image. On the other end, the second image was JPEG2000 decoded, followed by watermark extraction. Using the algorithm stated in previous section, the watermark bits were extracted. The method used to validate authentication of received image included number of mismatched bits exceeding a predefined threshold T2. It was found out that in all cases of noise (for all images), the bits were recovered with an average of 96.8% accuracy. It must be noted here that distortion in the received image included noise in the channel, imprecision added due to watermark, and JPEG2000 coding/compression. With various levels of compression, it was noted that as compression rate increased, watermark bit extraction success rate decreased.

However, higher scale decomposition used in wavelet transform improved the success rate as bits diffused from lowest scale to full image size. The quantization step size also affected the quality of the watermarked image i.e., the higher the quantization level, higher the degradation observed in all of the test images.

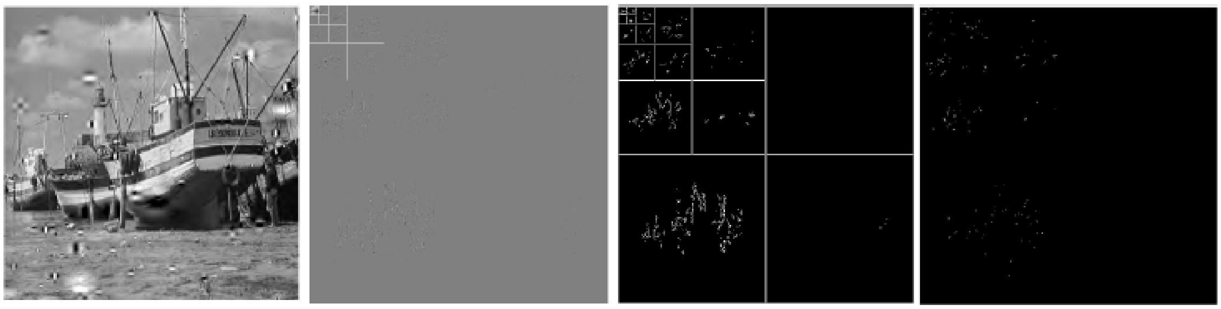

Figure 3: (a) Top left: Original image received with BER=0.009 (b) Top right: The displayed wavelet coefficients (c) Bottom left: Edge extraction of received wavelet coefficients (d) Bottom right: Result of subtracting extracted_edge_image from the received edge_image

Once watermark authentication is completed, edge image from received wavelet coefficients is computed. This image is termed as 'extracted_edge_image'. This new extracted_edge_image is then subtracted from the received 'edge_image' to determine the corrupted regions resulting due to distortion in transmission channel. As an example, the Figure 3(a) shows the received image reconstructed after passing through noisy transmission channel with *BER* = 0.009. The Figure 3(b) shows the displayed wavelet coefficients of the received image, the Figure 3(c) shows the edge extraction of displayed wavelet coefficients, and the Figure 3(d) shows the location of the corrupted regions resulting by subtracting the extracted_edge_image of received coefficients from the received edge_image of coefficients of the original image.

In order to minimize distortion in the reconstructed image, error concealment method was adopted to handle corrupted regions in wavelet coefficients domain. In this work, selective corrupted regions are processed for error concealment, though the approach can be extended to all subbands. As an implementation, all corrupted coefficients for all sub-bands on level 5 are estimated using a median filter [24] on 3x3 neighborhood of the corrupted coefficient. The filter selection and its neighborhood size was arbitrary. The rest of corrupted coefficients on the higher sub-bands were simply set to zero. Once corrupted region coefficients are identified and estimated, the inverse wavelet transform is applied to reconstruct image. This approach was repeated on all five test images with different bit error rates, and the result for one image is shown in Figure 4. It seems clear that the proposed approach does conceal errors introduced in the noisy channel. In order to judge quality of reconstructed images, root mean square error (*rms*) and peak signal-to-noise ratio (PSNR) were calculated for test images against different BER values. Mathematically, this is described as:

$$PSNR = 10\ \log_{10}\left(\frac{255^2}{mse}\right) \tag{9}$$

where *mse* stands for mean square of the difference between the original and reconstructed image. From results shown in Table 1, it is clear that almost all distortion due to channel noise have been removed due to error concealment and quality images restored. It can easily be inferred from Table 1 that as BER increases, *rms* values get increased. However, after concealment, these values are largely reduced. Likewise, PSNR values improved after concealment, with improvement ranging from 10-15 decibels.

Table 1: The *rms* and *PSNR* values for test images with channel BER=0.004, 0.006, 0.009

Woman image	Received Image		Concealed Image	
	RMS	*PSNR (dB)*	*RMS*	*PSNR (dB)*
BER=0.004	5.24	33.51	1.15	46.62
BER=0.006	6.39	32.18	0.98	48.18
BER=0.009	9.85	28.25	2.85	38.76
Pirate image	Received Image		Concealed Image	
	RMS	*PSNR (dB)*	*RMS*	*PSNR (dB)*
BER=0.004	11.68	26.95	1.67	43.48
BER=0.006	13.56	25.52	3.41	36.25
BER=0.009	14.21	25.69	2.15	41.11
Boat image	Received Image		Concealed Image	
	RMS	*PSNR (dB)*	*RMS*	*PSNR (dB)*
BER=0.004	8.58	29.52	2.11	41.69
BER=0.006	11.72	26.40	3.54	37.11
BER=0.009	17.32	23.41	2.67	39.57
Goldhill image	Received Image		Concealed Image	
	RMS	*PSNR (dB)*	*RMS*	*PSNR (dB)*
BER=0.004	9.25	28.75	3.96	36.02
BER=0.006	9.38	28.59	1.87	42.18
BER=0.009	10.71	27.64	2.38	40.44
Baboon image	Received Image		Concealed Image	
	RMS	*PSNR (dB)*	*RMS*	*PSNR (dB)*
BER=0.004	7.48	30.73	2.37	40.45
BER=0.006	8.57	29.49	3.21	38.51
BER=0.009	10.61	27.57	3.50	37.09

5 DISCUSSIONS

The objective of this research was to supplement transmission of JPEG2000 image data with authentication and noise handling capability. Image authentication method proposed in this approach was to counter unauthorized manipulations in the image. The lowest subband was used to extract signature bits and place watermark inside. The purpose behind content driven signature extraction was simplicity as opposed to different signature taken from the author or the publisher. It was found out that as number of decomposition levels increases, so is the diffusion rate of this watermark within the whole image after reconstruction. The authentication level at the receiver can be adjusted based on how much percentage of error is allowed.

The edge image was used to tackle channel distortion. In order to ensure minimum overhead on transmission, and noise free reception at the receiver, it was scrambled, lossless compressed and then followed by channel coding. Though it causes overhead, but it provides tradeoff with respect to visual quality of the image. Besides, this overhead is minimal as total overhead amounts to few kilo bytes. This step is optional and can be removed if channel has least noise distortion.

The advantages gained through proposed approach can be compared, for example, with the approaches described in [8-11]. In [8], the authors discuss digital signature extraction scheme for semi-fragile content through combination of hashing, public/private key for digital signature, and transmission of watermarked image along with cryptographic signature. The approach proposed in our paper is generic and more flexible than the one in [8], because it is independent of public/private infrastructure, and carries noise concealment ability. Similarly, the approach in [10] targets only medical images and encrypts some of the JPEG2000 coded image data using permutations, and remaining image data is not processed. This approach only fits some local network applications that secure only partial content. Likewise, the approach in [9] embeds watermark in the JPEG coded image using private key and lowest compression bit rate. There is no immunity against noise or how the encrypted image is degraded by noise. Additionally, there is no way to know regions where degradation or tampering may have occurred. In [11], the authors propose watermarking scheme for progressive image transmission along with compensation mechanism to reduce embedding distortion. This approach considers low band coefficients, and uses it as an authentication code to be embedded into other bands. It fails to consider effects of noise during transmission and how this noise affects compensation algorithms proposed in [11]. The approach is not generic and fits only an specific application.

6 CONCLUSIONS

An image authentication approach was proposed in this research that embedded content driven digital signature as a watermark before JPEG2000 coding. A separate edge image data was integrated with image authentication as a supplement to offset effects of noisy channel on image transmission. Effectively, edge image data added turned out to be very small of about 0.78% fraction of the actual image data. The approach provides system robustness, security, and better visual quality. Three advantages were clearly noted: (a) the selected data for scrambling and that for signature extraction and watermarking was small resulting in reduced computational complexity (b) data rate remains unchanged as effectively individual coefficients in selected subbands were replaced by equivalently by same number of new modified values (c) noise concealed by this approach is significant compared to overhead cost of about 0.78% on transmission.

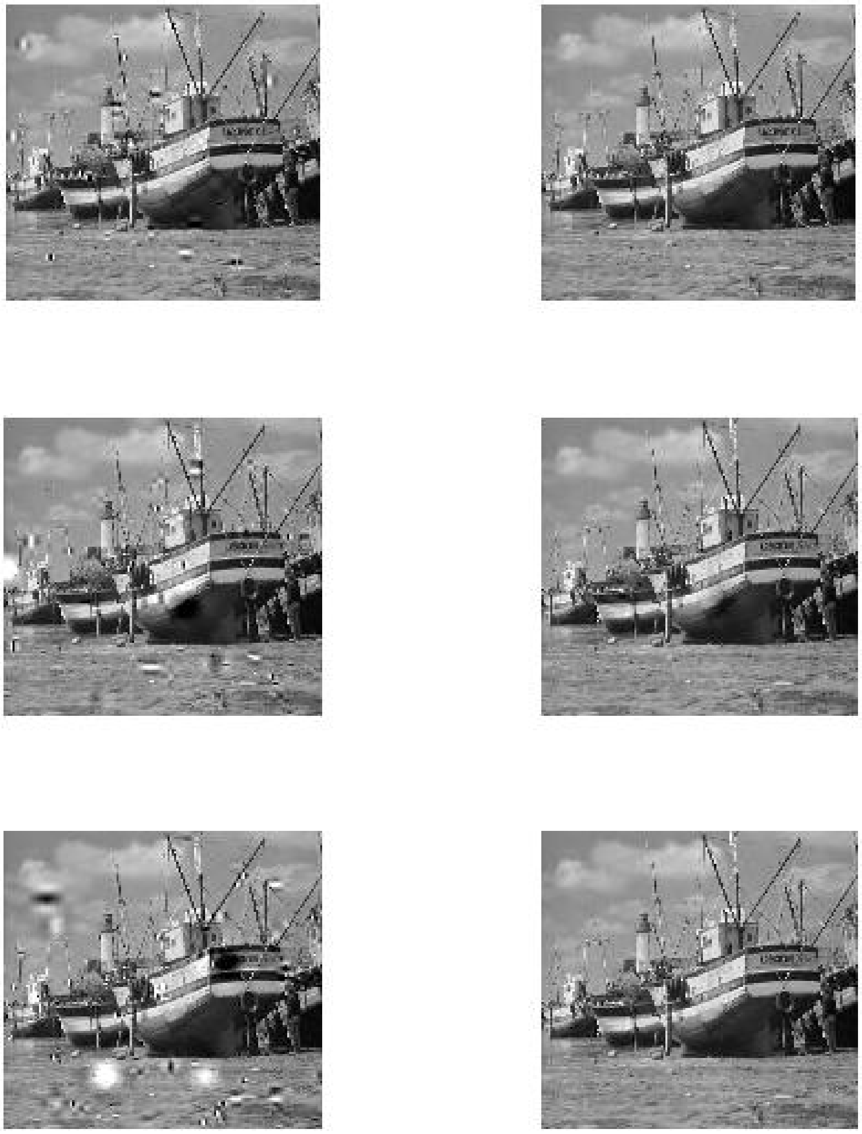

Figure 4.: The received and concealed images for boat image: Top: (a) and (b) for BER=0.004; Middle: (c) and (d) for BER=0.006; Bottom: (e) and (f) for BER=0.009

ACKNOWLEDGMENTS

The author would like to express sincere thanks to the Research Affairs unit of College of Engineering at United Arab Emirates University for financial support of this project under grant code number EE-21N151.

REFERENCES

[1]. S. Khalid, Introduction to Data Compression, New York, Morgan Kaufmann Publishers, 2000

[2]. L. Hanzo, P. Cherriman, J. Streit, Wireless Video Communications: *IEEE Series*, NY: IEEE Press, 2001.

[3]. Y. Wang and Q. Zhu, “Error control and concealment for video communication: A Review,” *Proceedings of the IEEE*, Vol. 86, No. 5, pp. 974-996, May 1998.

[4]. Qurban Memon, "A New Approach to Video Security over Networks", *International Journal of Computer Applications in Technology,* Vol. 25, No. 1, 2006, pp. 72-83.

[5]. Mairal, C. and Agueh, M. , "Scalable and robust JPEG 2000 images and video transmission system for multiple wireless receivers", *2010 IEEE Latin-American Conference on Communications* (LATINCOM), ECE, LACSC, Paris, France.

[6]. Martinez-Ruiz, M., Artes-Rodriguez, A., Diaz-Rico, J.A., Fuentes, J.B., "New initiatives for imagery transmission over a tactical data link. A case study: JPEG2000 compressed images transmitted in a Link-16 network method and results", *Military Communications Conference*, 2010, pp. 1163-1168.

[7]. P. Schelkens, A. Skodras & T. Ebrahimi. The JPEG 2000 Suite. Wiley, Series: Wiley-IS&T Series in Imaging Science and Technology, 2009.

[8]. Sun, Q., “A Secure and Robust Digital Signature Scheme for JPEG2000 Image Authentication”, *IEEE Transactions on Multimedia*,, Vol.7, No.3, pp.480,494, June 2005, doi: 10.1109/TMM.2005.846776

[9]. Wen, J., Wang, J., Feng, F., Zhang, B., “A Reversible Authentication Scheme for JPEG2000 Images”, The Ninth International Conference on Electronic Measurement & Instruments, vol., no., pp.4-486,4-489, 16-19 Aug. 2009

[10]. Zahia Brahimi, Z., Bessalah, H., Tarabet, A., Kholladi, M., “A new selective encryption technique of JPEG2000 codestream for medical images transmission”, 5th *International Multi-Conference on Systems, Signals and Devices*, 2008.

[11]. Tsai, P., , Hu, Y., Yeh, H., Shih, W., “Watermarking for Multi-resolution Image Authentication”, *International Journal of Security and Its Applications* Vol. 6, No. 2, April, 2012.

[12]. Lim,,S., Moon, H., Chae, S.,, Yongwha Chung, Y., Pan, S., “JPEG2000 and Digital Watermarking Technique Use in Medical Image”, *IEEE International Conference on Secure Software Integration and Reliability Improvement*, pp. 413-416, 2009

[13]. R. Dugad, K. Ratakonda and N. Ahuja, "A New Wavelet-based Scheme for Watermarking Images", *Proceedings of IEEE International Conference on Image Processing*, Chicago, IL, USA, Oct. 1998, 419-423.

[14]. Kung, C., Chao, S., Yan, Y., Kung, C., "A Robust Watermarking and Image Authentication Scheme used for Digital Content Application", *Journal of Multimedia*, Vol. 4, No. 3, June 2009, pp. 112-119

[15]. Sun, Q., Zhang, Z., "A Standardized JPEG2000 Image Authentication Solution based on Digital Signature and Watermarking", *China Communications*, pp. 71-80, October 2006

[16]. Sathishkumar , G., Ramachandran, S., Bagan, K., "Image Encryption Using Random Pixel Permutation by Chaotic Mapping", *IEEE Symposium on Computers and Informatics*, 2012, pp. 247-251

[17]. Joshi, S., Udupi, V., Joshi, D., "A Novel Neural Network Approach for Digital Image Data Encryption/Decryption", *IEEE International Conference on Power, Signals, Controls and Computation*, pp.1-4, 3-6 January, 2012

[18]. Tang, Z., and Zhang, X., "Secure Image Encryption without Size Limitation using Arnold Transform and Random Strategies", Journal of Multimedia, Vol. 6, No. 2, April 2011, pp. 202-206

[19]. Li, S., Wang, J., Gao, X., "The Fast realization of Image Scrambling Algorithm using Multi-Dimensional Orthogonal Transform", *IEEE Congress on Image and Signal Processing*, pp. 47-51, 2008

[20]. Yu, Z., Zhe, Z., Haibing, Y., Wenjie, P., Yunpeng, Z., "A Chaos-Based Image Encryption Algorithm Using Wavelet Transform", 2nd *International Conference on Advanced Computer Control*, Vol.2, pp. 217-222, 27-29 March, 2010

[21]. Y. Wang and Q. Zhu, "Error control and concealment for video communication: A Review," *Proceedings of the IEEE*, Vol. 86, No. 5, pp. 974-996, May 1998

[22]. J. Canny, "A Computational Approach to Edge Detection," *IEEE Transactions on Pattern Analysis*, Vol. PAMI-8, No. 6, pp. 679-698, Nov. 1986.

[23]. Musheer Ahmad, A., Haque, E., Farooq, O., "A Noise Resilient Scrambling Scheme for Noisy Transmission Channel", *International Conference on Multimedia, Signal Processing and Communication Technologies*, pp. 91-94, 2011

[24]. Memon, Q., Kasparis, T., "Block median filters", *International Symposium on OE/Aerospace Sensing and Dual Use Photonics*, pp. 100-109, Orlando, 1995.