Embedding Authentication and DistortionConcealment in Images – A Noisy Channel Perspective

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

***Abstract* - In multimedia communication, compression of data is essential to improve transmission rate, and minimize storage space. At the same time, authentication of transmitted data is equally important to justify all these activities. The drawback of compression is that the compressed data are vulnerable to channel noise. In this paper, error concealment methodologies with ability of error detection and concealment are investigated for integration with image authentication in JPEG2000.The image authentication includes digital signature extraction and its diffusion as a watermark. To tackle noise, the error concealment technologies are modified to include edge information of the original image.This edge_image is transmitted along with JPEG2000 compressed image to determine corrupted coefficients and regions. The simulation results are conducted on test images for different values of bit error rate to judge confidence in noise reduction within the received images.**

Indexing terms–Image authentication, JPEG2000, Error concealment

1. INTRODUCTION

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

As compressed data are more vulnerable to channel noise,therefore, the transmitted data must be resilient to channel noise and other impairments[1-3]. Several techniques have been proposed in the literature to address transmission errors by making transmitted data more robust to channel noise and in some cases conceal corrupted data at the receiver. As an example, the authors in [4] present a scalable scheme for robust JPEG 2000 image transmission to multiple wireless clients, using an adaptive bandwidth estimation tool. In another research [5], the authors present the results of an initiative to transmit imagery content through a Link-16 tactical network using JPEG2000 compatible approach. In that approach, 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 need for high compression and artifacts free imaging hasmade JPEG2000 a capable algorithm to replace the current JPEG which is still being applied today [6]. The implementation of two dimensional discrete wavelet transform (2-D DWT)requires digital filers and down-samplers. In JPEG2000, typically images are decomposed to five wavelet levels to accomplish higher compression ratio.

The edge detection is also useful for detecting valuable or important changes in the value of the intensity, and can be explored to hide image distortions introduced in the channel.This kind of detection is mostly achieved using first order or second order derivative of intensity values. Moreover, one of the reasons that could make this variation high is the existence of high frequency (noise) at that area.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 needs to be made resilient to channel noise and other impairments or post processing in the receiver needs to deployed. Such techniques have been classified into three groups. The first technique makes the encoder to play the major role by making the source data more immune to transmission errors.The second technique uses post processing in the decoder plays in concealing errors without depending on additional data from the encoder. The third technique uses interactive approach where encoder and decoder work cooperatively through feedback channel to minimize impact of transmission errors.

Digital Signature and Watermarking: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 implementation, for example in [7], the authors investigate the invariant features 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. The authors in [8] discuss a scheme, where scalability 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 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 [9], 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 belonging to the selected precincts. The remaining packets are sent without encryption.

The authors in [10] select LL coefficients as authentication code (AC) since root nodes preserve the most important energy. To embed AC in image, 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 [11], the authors employ Dugad technique [12] to resolve security issues in medical images by adding watermark technology to JPEG2000 compression.In [13], the main features of the proposed authentication system include integration of both content based authentication and code-stream based 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 [14] have proposed an image encryption algorithm using random pixel permutation based on chaos logistic maps and prime modulo multiplicative linear congruential generators. In another work [15], 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 [16], 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 [17], 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 sequences.

*Summary of Issues:*The area of compressed data transmission through noisy channels is still active in research, and needs further investigation.In multimedia communication, the 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. Though digital signature and watermarking techniques has grown to be mature technologies, but the current state of the art approaches do not completely solve the problem of unauthorized copying or provide protection from digital data privacy. 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. Image authentication and subsequent noise concealment in receiver at multiple levels are the main contributions of this work.

II. PROPOSED APPROACH

The proposed approach is shown in Figure 1. It 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 stepsis discussed as follows:

a. Edge Extraction: 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 edge detection, Canny edge detector [18] with convenient thresholds is applied to the wavelet transformed image. The resulting binary edge imageundergoes scrambling and lossless compression, as discussed below.

b. Scrambling: In literature [19], 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. These permutations again depend on the level of scrambling. The 2-D Arnold transform [19] is defined as:

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

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:

$$x_1(n+1) = \mu_1\, x_1(n)\,(1 - x_1(n)) + \gamma_1\, x^2{}_2(n) \qquad (5)$$

$$x_2(n+1) = \mu_2\, x_2(n)\,(1 - x_2(n)) + \gamma_2\,(x^2{}_1(n) + x_1(n)x_2(n))$$

This logic map has three coupling terms to show its complexity. It is shown in [19] that the map is chaotic if $2.75 < \mu_1 \le 3.4$, $2.7 < \mu_2 \le 3.45$, $0.15 < \gamma_1 \le 0.21$, $0.13 < \gamma_2 \le 0.15$.

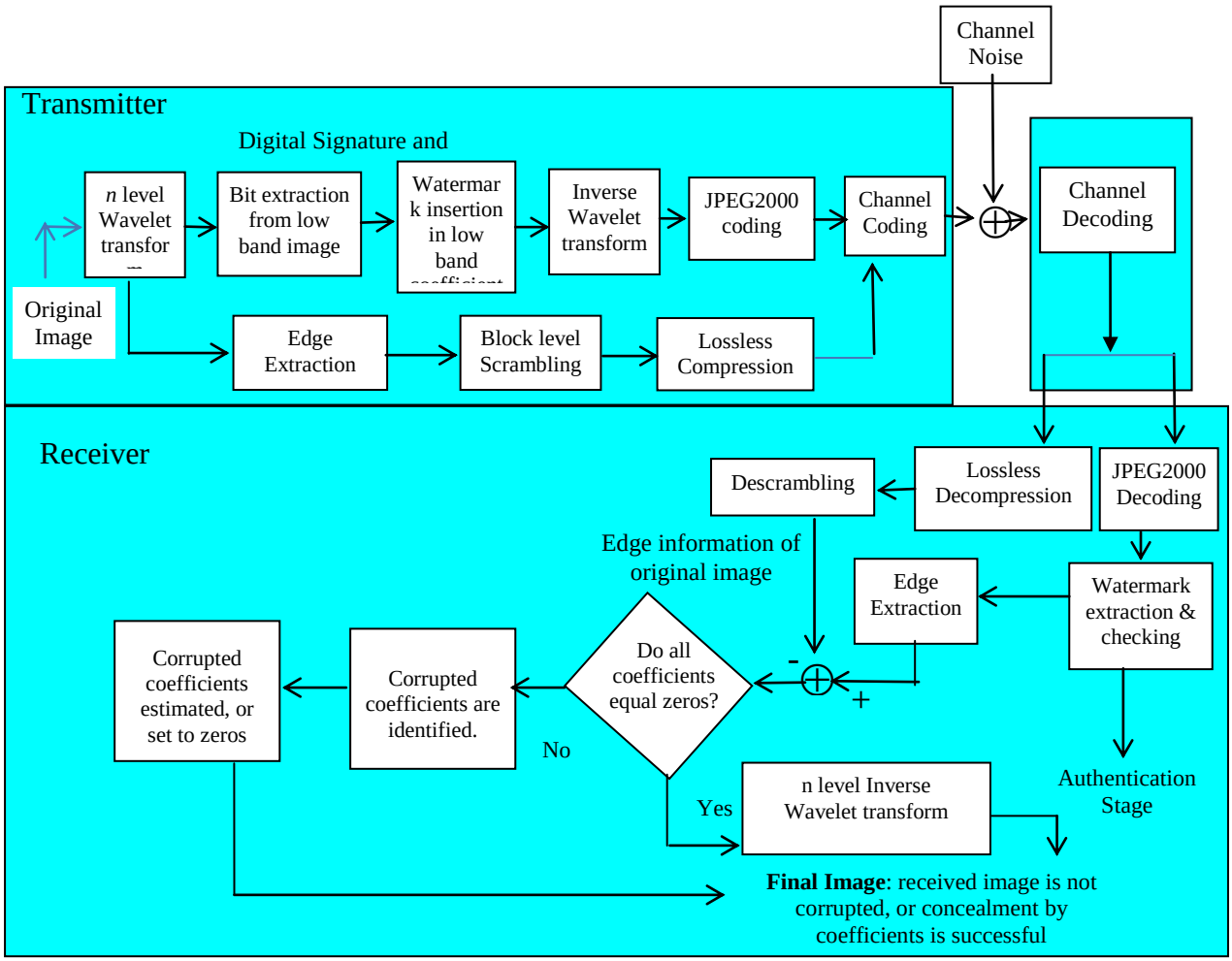

Figure 1: Block diagram of Proposed Algorithm

This logic map has three coupling terms to show its complexity. It is shown in [19] 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 use 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.

c. Lossless Compression: The purpose of this step is to reduce the 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 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.

d. 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 Nx 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 $0 \le i \le N/2^n$ and $0 \le j \le N/2^n$. 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 the whole subband. The total extracted number of bits is MxL, where L is number of bits generated per block. This content driven digital signature is more satisfying for customers and image providers to be extracted from within the image rather than selecting external bits as digital signature. These extracted bits are later inserted as watermark in the same subband.

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 similarly looking (watermarked, or attacked) blocks will have same signature bits (b) a 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 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 noise adding, compression, filtering, etc.In order to extract bits from low band subband, a secret key K 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 andvary continuously with subband block S_k.

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 in wavelet domain, and that process be robust against common image processing application such as JPEG compression. Mathematically, watermarking process can be described as:

$$LL'_n = W_F(LL_n, c, K) \qquad (7)$$

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

$$c' = W_R(LL'_n, K) \qquad (8)$$

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

$b'_k = \{ b_k + 1 \text{ for } diff_k = 0$
$b_k - 1 \text{ for } diff_k = 1 \} else \quad b'_k = b_k$

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 $\bar{LL}_n(i, j)$ is calculated, and difference is computed as:

$\delta_m = m_r - m_t$

ii. The received lowest subband $\bar{LL}_n(i, j)$ is decomposed into blocks $\bar{S}_k$ and mean $\bar{m}_k$ is calculated.

iii. Compute the quantization value as:

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

iv. Extract the embedded bit as:

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

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. For simulation purposes, this noise is added to transmitted data before it reaches the receiver.

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 original image. If the difference between the received edge image and the extracted edge image is zero or below a 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 corrupt. In JPEG2000, the corrupted regions will have different sizes since the wavelet coefficients at different levels represent different blocksizes 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 were computed at the transmitter. The spatial pattern of corrupted region may help to determine if the corrupted region is in horizontal, vertical, or diagonal *sub-band*.

Concealing errors at higher *sub*-band**:** This step deals with existence of corrupted regions or blocks in received wavelet coefficients. The location of the corrupted block in the received wavelet coefficients may be used to determine the location of thewavelet 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 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 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.

III. 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 section 2. 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 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 to extract the edge image. The resulting binary image, termed as 'edge_image' undergoes scrambling. It should be noted, 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 [19]. 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 subband 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 for JPEG2000 coded watermarked image together with mean value was252KB, whereas edge image size was ~3KB only. Since edge image is required to be with zero distortion at the receiver, this is coded with robust channel coding technique to withstand noise in the channel. This step added up to 7KB extra to the edge image. The added noise to the channel was 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 simply applying exclusive OR logical operation and the result was an image with noise distortion. The image mixed with noise was the one received at the receiver.

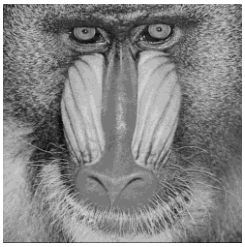

Figure 2: Images (a) *woman* (b) *pirate* (c) *goldhill* (d) *boat* (e) *baboon*

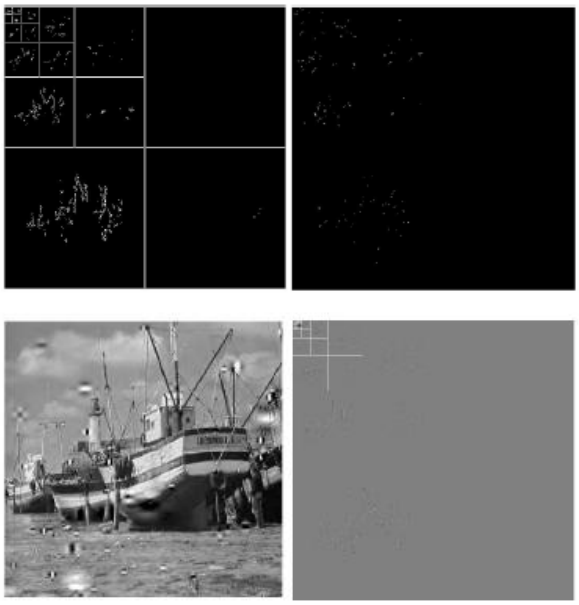

Figure 3: (a) Top left: Original image received with BER=0.009 (b) Top right: Its wavelet coefficients (c) Bottom left: Edge extraction of received wavelet coefficients (d) Bottom right: Subtracting extracted_edge_image from the received edge_image

After data is channel decoded, two images are available. The lossless compressed image undergoes inverse operations done at the transmitter. After lossless decompression,it is followed by descrambling exactly in reverse order of transmission. As theimage was channel coded using robust channel coding, 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 T_2. It was found out that in all cases of noise (for all five 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, and imprecision added due to watermark. 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.

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 As an example, the Figure 3(a) shows the image reconstructed after receiving through 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 after 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. As a reference, various error concealment errors are discussed in [20]. 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 [21] on 3x3 neighborhood of corrupted coefficient. The filter selection and its neighborhood size were arbitrarily set. The rest of corrupted coefficients on the higher sub-bands were simply set to zero.Once corrupted coefficients are identified and estimated, the inverse wavelet transform was applied to reconstruct image. This approach was repeated on all five test images with different bit error rates, and the resultfor one image is shown in Figure 4.

IV. CONCLUSIONS

The main focus of this research was to supplement transmission of JPEG2000 image with authentication and noise handling ability. An integrated approach was presented along with simulations. The lowest subband was selected to extract signature bits and place watermark inside and later diffuse it throughout the image. It was found out that as number of decomposition levels increases, so is the diffusion rate of this watermark within the whole image. The authentication level at the receiver can be adjusted based on how much percentage of error is allowed. A separate edge image data was used in this approach as a supplement to offset effects of noise and other data manipulations. In order to ensure its noise free reception, it was scrambled, lossless compressed and then followed by robust channel coding. Though it causes overhead, but it is minimal as total overhead data amounts to few kilo bytes. The channel coding is optional and can be removed if channel has least noise distortion. A number of parameters were used to judge quality of the reconstructed images at the receiver, and it was found that the error concealment improves visual quality of the reconstructed images.Two 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.

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] 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.

[5] 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.

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

[7] 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

[8] 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

[9] 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.

[10] 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.

[11] 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

[12] 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.
[13] Sun, Q., Zhang, Z., "A Standardized JPEG2000 Image Authentication Solution based on Digital Signature and Watermarking", *China Communications*, pp. 71-80, October 2006
[14] 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
[15] 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
[16] 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
[17] 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
[18] J. Canny, "A Computational Approach to Edge Detection," *IEEE Transactions on Pattern Analysis*, Vol. PAMI-8, No. 6, pp. 679-698, Nov. 1986.
[19] 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
[20] Memon, Q., Boumatar, A., "Robust Transmission of Images Based on JPEG2000 using Edge Information", *International Journal of Internet and Distributed Systems*, Vol. 3, No. 1, pp. 174-183, 2013
[21] Memon, Q., Kasparis, T., "Block median filters", *International Symposium on OE/Aerospace Sensing and Dual Use Photonics*, pp. 100-109, Orlando, 1995.

Figure 4.Received and concealed 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