Conference or Workshop Item:
Bhowmik, D. and Abhayaratne, C. (2010) Robustness analysis of blind watermarking for quality scalable image compression. In: 18th European Signal Processing Conference (EUSIPCO-2010), August 23-27 2010, Aalborg, Denmark.

ROBUSTNESS ANALYSIS OF BLIND WATERMARKING FOR QUALITY SCALABLE IMAGE COMPRESSION

Deepayan Bhowmik, Charith Abhayaratne and Matthew Oakes

Department of Electronic and Electrical Engineering, The University of Sheffield
Sheffield S1 3JD, United Kingdom.
{d.bhowmik, c.abhayaratne, m.oakes}@sheffield.ac.uk

ABSTRACT

Robustness analysis of a blind wavelet based ranked-ordered watermarking scheme against quality scalable image compression is presented in this paper. The analysis considers a general wavelet-based compression scheme by modeling the bit-plane discarding, used in achieving quality scalability in JPEG2000. In this work we aim to improve the robustness by proposing the optimum modification for the selected coefficients in order to retain the watermark information. A relationship is established between the watermark detection algorithm and the number of bit planes discarded and this knowledge is used during the embedding procedure. The proposed model assumes the same embedding and compression wavelet kernel. The experimental results verify the proposed model and demonstrate improved performance in robustness to quality scalable compression in JPEG2000.

1. INTRODUCTION

In recent years, there has been an increase in use of scalable coded media. JPEG2000 (Joint Photographic Experts Group) for image coding and H.264/MPEG-4 advanced video coding (AVC) scalable extension are the main standards used in universal multimedia access (UMA) applications for seamless media content delivery. Digital watermarking addresses the issues related to multimedia security and digital rights management. In this context an increasing number of wavelet domain watermarking schemes are offered considering JPEG2000 image compression [1–5].

In UMA multimedia usage scenario, the emerging watermarking algorithms attempt to improve the robustness against scalable coding, either by incorporating the watermarking into the compression algorithm, as in JPEG 2000 Secured (JPSec) [6], or employing other wavelet domain embedding schemes independent of compression scheme. For example, in [7], a secure signature scheme is presented based on JPEG2000 image authentication. However, most of the algorithms do not provide an insight into how robust these algorithms to quality scalability or resolution scalability in JPEG2000 scalable image compression. Common models restrict their focus only on robustness to image processing and geometric attacks or conventional compression [8].

In this paper we present a model for improving the wavelet based blind watermarking robustness to quality scalable image compression attacks. To emulate the compression in JPEG2000, the wavelet based compression using a bit plane discarding model is considered. The model is derived by analyzing the effect of compression parameters in scalable image coding. In our previous work [9], the robustness of a non-blind watermarking scheme is analysed whereas here we have consider blind watermarking scheme and exploited a ranked-order-based blind watermarking algorithm described in [4]. The model shows the relationship between the compression parameters and the wavelet coefficients to be modified and uses that relationship to identify the optimum modification during watermark embedding. The proposed watermark embedding criteria ensures improved robustness under various quality scalability adaptations of JPEG2000 encoded bitstream. At the same time to improve the imperceptibility, an imperceptibility model [10] may be used to find the trade off. Without loosing the generality, we have implemented the model with an example case in [4]. However other blind watermarking algorithms can be modeled with a similar approach.

The rest of the paper is organized with a brief description on the general scalable coding framework and wavelet-based quantization error modeling in Sec. 2. A discussion is presented in Sec. 3 on the generalised framework of wavelet based watermarking schemes. The robustness model is presented in Sec. 4 followed by the experimental results in Sec. 5 with concluding remarks in Sec. 6.

2. SCALABLE IMAGE COMPRESSION

UMA uses scalable coded content to enable seamless multimedia consumption independent of the application device, network media, network speed, resource limitation and usage preferences. The input media is coded in such a way that the main host server keeps the full resolution content which can be decoded to produce maximum quality and spatial resolution. The supply of the scaled content, to a less capable display or to transmit through the lower bandwidth, is adapted in different nodes having different scaling parameters. At each node the scaling parameters might be different and a new bit stream can be generated. Finally a suitable decoded version is supplied to the end-user display terminals.

JPEG2000 uses the Discrete Wavelet Transform (DWT) as its core technology and offers scalable decoding with quality and resolution scalability. The scalable coders encode the image by performing the DWT followed by embedded quantizing and entropy coding. The coefficient quantization, in its simplest form, can be formulated as follows:

$$C_q = \left\lfloor \frac{C}{Q} \right\rfloor, \tag{1}$$

where C_q is the quantized coefficient, C is the original coefficient and Q is the quantization factor. Embedded quantizers

The work of Mr Bhowmik is supported by the BP-EPSRC Dorothy Hodgkin Postgraduate Award and the work of Mr Oakes is supported by the EPSRC Doctoral Training Award.

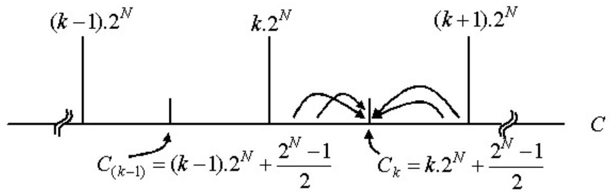

Figure 1: Quantization compression scheme considering N level bit-plane discarding.

often use $Q = 2^N$, where N is a non-negative integer. Such a quantization parameter within downward rounding (*i.e.,* using *floor*), can also be interpreted as bit plane discarding as commonly known within the image coding community.

At the decoder side, a reverse process of the encoding is followed to reconstruct the image. The dequantization process is formulated as follows:

$$\hat{C} = Q.C_q + \left(\frac{Q-1}{2}\right), \tag{2}$$

where $\hat{C}$ is the dequantized coefficient. In such a quantization scheme, the original coefficient values in the range $k.Q \leq C < (k+1).Q$, where $k \in \pm1, \pm2 \pm 3...$ and $Q = 2^N$ for bit plane wise coding are mapped to $\hat{C} = C_k$, which is the center value of the concerned region as shown in Fig. 1.

3. WAVELET-BASED WATERMARKING SCHEMES

In an attempt to generalization of wavelet based watermarking schemes, we have accommodated popular algorithms into a common framework [11] by dissecting the algorithms into common functional modules and deriving a basic embedding form as follows:

$$C'_{m,n} = C_{m,n} + \Delta_{m,n}, \tag{3}$$

where $C'_{m,n}$ is the modified coefficient at (m,n) position, $C_{m,n}$ is the coefficient to be modified and $\Delta_{m,n}$ is the modification due to watermark embedding. Based on the modification algorithms we have broadly categorized the algorithms into two groups: direct modification [1, 2] and quantization based modification [3–5]. The watermarking algorithms can also be grouped in two different categories: (1) Non-blind watermarking where the original image is required during the watermark extraction procedure and (2) Blind watermarking (no original host image needed). Due to the nature of embedding most of the direct modification algorithms defined under non-blind category where as majority of the quantization based schemes can be referred as blind.

Direct modification Direct modification algorithms are generalized in the following modification value $\Delta_{m,n}$ at (m,n) position:

$$\begin{aligned}\Delta_{m,n} = \quad & (a_1)\alpha(C_{m,n})^b W_{m,n} + (a_2)v_{m,n}W_{m,n} \\ & +(a_3)\beta C_w + (a_4)S_{m,n},\end{aligned} \tag{4}$$

where $a_1, ..., a_4$ are Boolean variables to identify the presence of each of the components for a given methodology, $C_{m,n}$ is the coefficient to be modified, α is the watermark weighting factor, $b = 1, 2...$ is the watermark strength parameter, $W_{m,n}$ is the watermark value, $v_{m,n}$ is the weighting parameter based on pixel masking in a human visual system model, β is an HVS-based fusion strength parameter in the case of fusion based scheme, C_w is the watermark wavelet coefficient and $S_{m,n}$ is any other value which is normally a function of $C_{m,n}$.

Quantization based modification The ranked ordered list based algorithms change the median value of a local area (typically a 3x1 coefficient window) considering the neighboring values. The modification value $\Delta_{m,n}$ is decided based on a quantization step δ $(-\delta \leq \Delta_{m,n} \leq \delta)$ within the range of the selected 3x1 window. Different functions are suggested in the literatures to find the value of δ and the functions normally consists of minimum (C_{min}) and maximum (C_{max}) value of the coefficients in each selected window.

$$\delta = f(\alpha, C_{min}, C_{max}), \tag{5}$$

where α is the weighting factor and predefined. These methods vary by the way the coefficients are chosen for the list, for example, choosing from the same subband (intra subband quantization) [4] and choosing from different subbands of the same level (inter subband quantization) [3].

4. ANALYSIS OF ROBUSTNESS TO QUALITY SCALABLE COMPRESSION

A ranked order based blind watermarking scheme [4] has been adopted here as the example case. As described previously in Sec. 3, a non-overlapping 3×1 running window is passed through the entire selected subband of the wavelet decomposed image. At each sliding position, a rank order sorting is performed on the coefficients C_1, C_2 and C_3 to obtain an ordered list $C_1 < C_2 < C_3$. The median value C_2 is modified to obtain C'_2 as follows:

$$C'_2 = f(\alpha, C_1, C_3, w), \tag{6}$$

where w is the input watermark sequence and $f()$ denotes a non-linear transformation. Referring Eq. (5), the quantization step δ is defined here as:

$$\delta = \alpha.\frac{|C_1| + |C_3|}{2}, \tag{7}$$

where α is the watermark strength parameter.

For the extraction of watermark bit sequence, the DWT is performed on the test image followed by a rank ordered sorting with a 3×1 running window to obtain sorted elements C_1, C_2 and C_3 at each position. The watermarked bit w_{ext} associated with the particular window position is extracted as follows:

$$w_{ext} \in (0,1) = \left\lfloor \frac{C_2^q - C_1^q}{\delta^q} \right\rfloor \%2, \tag{8}$$

where % denotes the modulo operator to detect odd or even number.

At this point we considered the quality scalable compression on test image and find the parameter which affects the robustness. We have defined a superscript q to each of the previously defined notations to represent the quantization compression including C_1, C_2, C_3 and δ to C_1^q, C_2^q, C_3^q and δ^q respectively.

Due to the quantization operation as discussed in Sec. 2, all coefficient values in any 3x1 running window are remapped to the center points of the corresponding clusters and

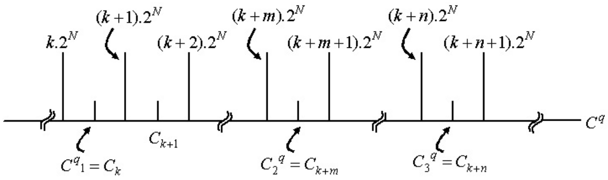

Figure 2: Mapping of coefficients after quantization compression considering N bit planes discarding.

the watermark extraction will be based on these new values. At this point, with the example of any selected window, we assume, C_1 is mapped to C_k $(= C_1^q)$, C_2 is mapped to C_{k+m} $(= C_2^q)$ and C_3 is mapped to C_{k+n} $(= C_3^q)$ as shown in Fig. 2, where $k,m,n \in \pm1, \pm2 \pm 3...$ To extract the watermark, new quantized values are taken in consideration. With reference to Eq. (2) and Eq. (7), the watermark quantization step value δ^q can be now defined as:

$$\begin{aligned} \delta^q = & \quad \alpha \frac{|C_1^q| + |C_3^q|}{2}, \\ = & \quad \alpha \frac{C_k + C_{k+n}}{2}. \end{aligned} \tag{9}$$

Using Eq. (2), we can write the center values of a cluster in Eq. (9) considering N bit planes are discarded:

$$\begin{aligned} \delta^q = & \quad \alpha \frac{k.2^N + \frac{2^N - 1}{2} + (k+n).2^N + \frac{2^N - 1}{2}}{2}, \\ = & \quad \alpha.2^{N-1}.(2k+n+1) - 0.5\alpha, \\ \approx & \quad \alpha.2^{N-1}.(2k+n+1), \end{aligned} \tag{10}$$

where considering a typical $\alpha = 0.1$ or 0.05 and the 0.5α term is ignored as this term is much smaller than the first part of the equation. With reference to Eq. (8) and Eq. (10), the extracted watermark bit w_{ext} can be expressed with the following equation:

$$\begin{aligned} w_{ext} \in (0,1) = & \quad \left[\frac{C_2^q - C_1^q}{\delta^q}\right] \%2, \\ = & \quad \left[\frac{C_{k+m} - C_k}{\delta^q}\right] \%2, \\ = & \quad \left[\frac{(k+m).2^N + \frac{2^N - 1}{2} - k.2^N - \frac{2^N - 1}{2}}{\alpha.2^N.(2k+n+1)}\right] \%2, \\ = & \quad \left[\frac{1}{\alpha} \cdot \frac{2m}{2k+n+1}\right] \%2, \end{aligned} \tag{11}$$

where $\%$ denotes the modulo operator to identify odd or even number with the condition that $0 < m \leq n$.

Thus using Eq. (11), it is possible to predict w_{ext} at a given number of discarded bit planes. We can use this relationship during the watermark embedding procedure. For any selected 3x1 running window, C_1 and C_3 are not being modified and hence it is possible to know the values of k and n in Eq. (11), where α is an user defined known parameter. Therefore the value of m can be decided during embedding in order to extract $'1'$ or $'0'$ correctly at N number of discarded bit planes. Based on the input watermark sequence and C_2 value, the optimum C_2' value can be calculated, so that w_{ext} sequence will be the same as the input watermark sequence. One can calculate the similar optimum value of C_2' for any other N value and find the common suitable optimum C_2' value for any N or lower number of bit plane discarding.

Table 1: Values of m and corresponding w_{ext} and C_2^q

m	w_{ext}	C_2^q
1	1	79.5
2	1	111.5
3	0	143.5
4	0	175.5
5	1	207.5

Table 2: Ranges of C_2' to embed $'1'$ and $'0'$ for different N being discarded

$N \rightarrow$	3	4	5	Combined
Embed $'1'$	184-192 & 192-200	160-176 & 192-208	192-224	192-200
Embed $'0'$	176-184 & 200-208	128-144 & 176-192	160-192	176-184

For an example, we assume $C_1 = 35, C_2 = 181, C_3 = 203$ and $\alpha = 0.1$. Referring to Eq. (11) at $N = 5$, other variables can be calculated as $k = 1$, $n = 5$ and $w_{ext} = [2.5m]\%2$. Now for different values of m we can estimate the value of w_{ext} and C_2^q as shown in Table 1.

Embed $'1'$: Based on the original C_2 value and with reference to calculated m, at $N = 5$, with minimum modification, the modified median coefficient C_2' should be in the range of $192 \leq C_2' < 224$ to embed $'1'$ for a correct extraction.

Embed $'0'$: Similarly using Table 1 the range for embedding $'0'$ can be calculated as $160 \leq C_2' < 192$.

The similar calculation can be done for $N = 1,2,3,4...$ and the range for C_2' can be found for a given 3x1 running window. The overlapping range for all N value can ensure correct watermark extraction at a given N or lower number of bit planes discarding. As an example case, we extended our previous example for $N = 3,4..$ and calculated the range to embed $'1'$ or $'0'$ as shown in Table 2. Now based on the calculated values for the modified C_2', to embed $'1'$ the coefficient must be within $(192-200)$ and to embed $'0'$ the range will be $(176-184)$ in order to retain the watermark information at $N = 3$, $N = 4$ or $N = 5$.

Hence using the above relationship we can optimally embed the watermark sequence in the example watermarking scheme for a guaranteed watermark extraction at a given compression ratio. Using a similar model, the watermark embedding criteria for any other blind watermarking schemes such as in [3,5] can be derived for better robustness performance.

5. EXPERIMENTAL SIMULATIONS

Experimental simulations of the derived model have been performed with respect to the example case mentioned in previous sections, considering quality scalable compression in JPEG2000. Two different experimental sets have been considered here. Firstly, in experiment set 1, we aim to verify the model against wavelet-based bit-plane discarding compression and then carried out similar experiment in JPEG2000 compression scenario. The experimental arrangements are shown below:

Experiment Set 1: Here we have considered the bit plane based quality compression effect. Firstly the embedding is done as it is suggested in [4], without considering the derived model. Then using the model, the wavelet coefficients are modified assuming different number of discarded bit planes (N) at the time of watermark embedding. The quality scalability is applied on watermarked image by discarding different number of bit-planes corresponding to quantization step $Q = 2^N$. The watermark is extracted from the compressed image and the Hamming distance is measured between the extracted and the original watermark. The results are shown in Fig. 3 with x axis representing quantization step Q and Hamming distance in y axis. A bi-orthogonal 9/7 wavelet kernel is considered here for embedding and compression in 3 level wavelet decomposition with α value of 0.08. In all cases the low frequency subband is considered for the watermark embedding.

Experiment Set 2: A similar experimental set up as in Experiment Set 1, is followed except the compression scenario. A JPEG2000 compression is applied to the watermarked images and the test images are produced at various compression ratio. The results are shown in Fig. 4 where x axis represents the compression ratio and y axis shows the hamming distance.

In both the experimental set up first two graphs represent individual image performances whereas the third graphs show the average Hamming distance for 31 test images within 95% confidence interval.

The robustness model derived here establishes the relationship between the quantization compression parameters and the choice of wavelet coefficients of the host image to be modified. The experimental simulations were performed by the optimum modification of the selected coefficients using the derived model. Firstly, the watermark embedding is performed with the original algorithm and robustness is measured against different compression scenario, i.e., different number of bit plane discarding. Then we embedded the watermark assuming different bit plane discarding ($N = 1 : 5$) and modified the wavelet coefficients accordingly. The experimental results shown in Fig. 3 indicates that the robustness is improved as more number of bit planes are considered during embedding. Hence the watermark is more robust to compression if higher value of N is considered during watermark embedding. This model also strongly supports JPEG2000 based quality scalable compression as shown in Fig. 4. Higher the N value considered during embedding gives better robustness. But at very high compression ratio the test images do not retain watermark information as the image pixel information is lost significantly. As a result a higher Hamming distance is noticed as shown in the figures.

As we conclude that a higher N value during embedding offers better robustness but at the same time it may cause higher embedding distortion. One can optimize the watermarking scheme to offer lower distortion and higher robustness by combining this model with the imperceptibility model in our previous work [10].

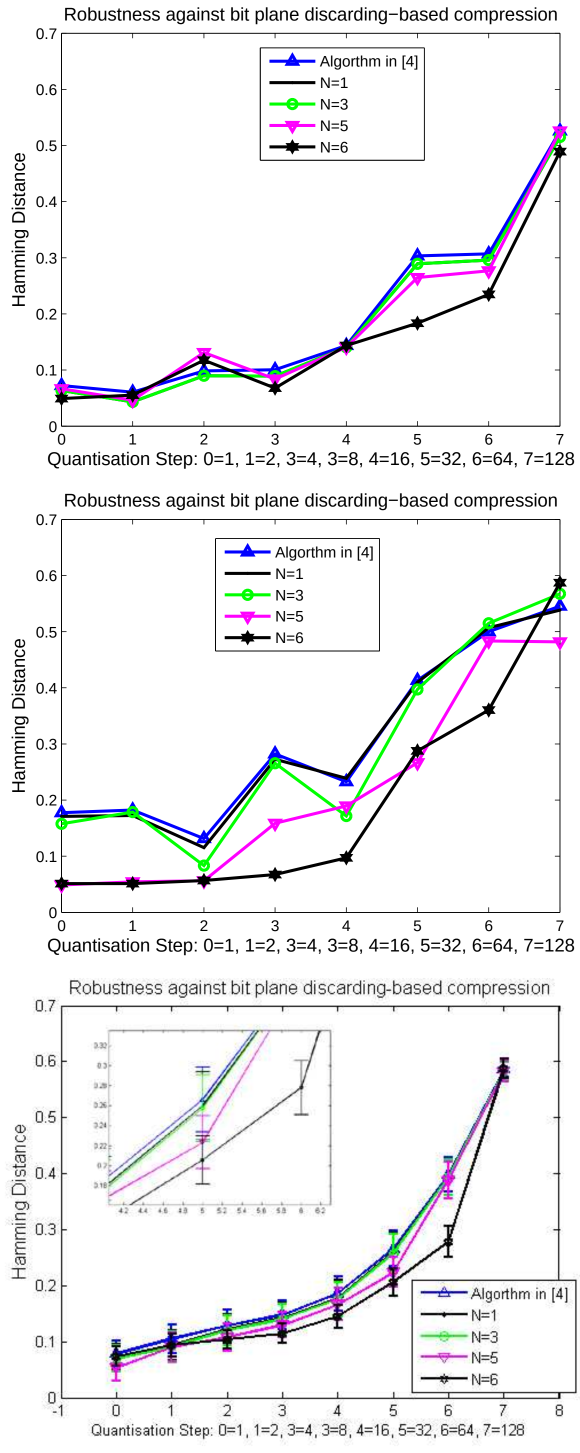

Figure 3: Robustness performance against quantization based compression for image 1 (Row 1), image 2 (Row 2) and average performance of 31 images (Row 3). Quantization steps: $Q = 2^1, Q = 2^2 ... Q = 2^6$. N = number of bit plane considered during embedding.

6. CONCLUSIONS

A mathematical analysis of robustness was presented in this work with reference to a blind wavelet-based watermarking scheme with reference to quantization based quality scalable compression including JPEG2000. Firstly, a relationship was established between the wavelet coefficients responsible for watermark embedding and the compression parameters

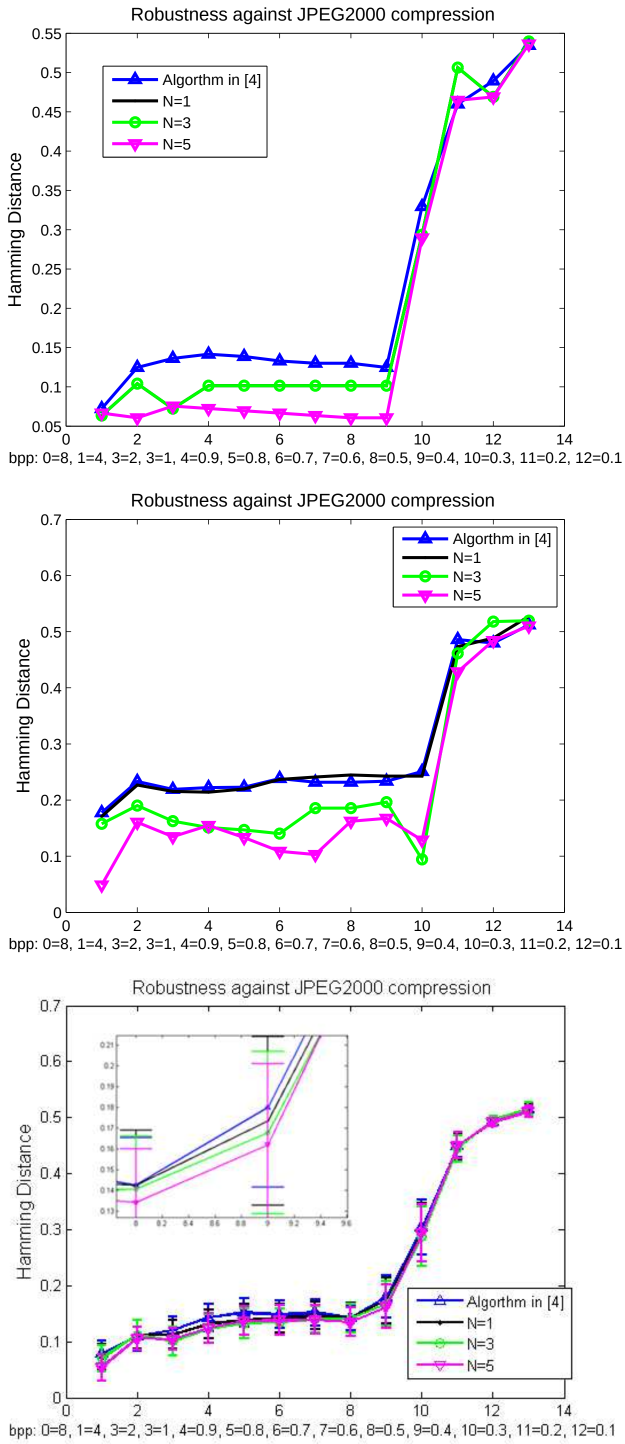

Figure 4: Robustness performance against JPEG2000 compression for image 1 (Row 1), image 2 (Row 2) and average performance of 31 images (Row 3). N = number of bit plane considered during embedding.

such as quantization step. Then necessary conditions were made to optimally modify the coefficients which can retain the watermark information at a given compression ratio. A bit-plane discarding based compression is considered to derive the scheme and experimental verification is done for the same. The derived model is also supported by experimental simulations against JPEG2000 compressions. Such an analysis is very useful to optimize the modification of the selected coefficient during watermark embedding which helps to reduce the embedding distortion while keeping better robustness.

REFERENCES

[1] X. Xia, C. G. Boncelet, and G. R. Arce, "Wavelet transform based watermark for digital images," *Optic Express*, vol. 3, no. 12, pp. 497–511, Dec. 1998.

[2] J. R. Kim and Y. S. Moon, "A robust wavelet-based digital watermarking using level-adaptive thresholding," in *Proc. IEEE ICIP*, 1999, vol. 2, pp. 226–230.

[3] D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," in *Proc. IEEE ICASSP*, 1998, vol. 5, pp. 2969–2972.

[4] L. Xie and G. R. Arce, "Joint wavelet compression and authentication watermarking," in *Proc. IEEE ICIP*, 1998, vol. 2, pp. 427–431.

[5] C. Jin and J. Peng, "A robust wavelet-based blind digital watermarking algorithm," *Information Technology Journal*, vol. 5, no. 2, pp. 358–363, 2006.

[6] T. Ebrahimi and R. Grosbois, "Secure JPEG 2000-JPSEC," 2003, vol. 4, pp. 716–719.

[7] Q. Sun and S. Chang, "A secure and robust digital signature scheme for JPEG2000 image authentication," *IEEE Trans. Multimedia*, vol. 7, no. 3, pp. 480–494, June 2005.

[8] M. Ejima and A. Miyazaki, "On the evaluation of performance of digital watermarking in the frequency domain," in *Proc. IEEE ICIP*, 2001, vol. 2, pp. 546–549.

[9] D. Bhowmik and C. Abhayaratne, "The effect of quality scalable image compression on robust watermarking," in *Proc. IEEE DSP'09*, 2009, pp. 1–8.

[10] D. Bhowmik and C. Abhayaratne, "A generalised model for distortion performance analysis of wavelet based watermarking," in *Proc. IWDW '08, Lect. Notes in Comp. Sc.*, 2008, vol. 5450, pp. 363–378.

[11] D. Bhowmik and C. Abhayaratne, "A framework for evaluating wavelet based watermarking for scalable coded digital item adaptation attacks," in *Proc. SPIE Wavelet Applications in Industrial Processing VI*, 2009, vol. 7248, p. 72480M (10 pages).