ROBUST IMAGE DATA HIDING USING GEOMETRIC MEAN QUANTIZATION

Mohammad Ali Akhaee, Shahrokh Ghaemmaghami†, Amir Nikooienejad, and Farokh Marvasti

Advanced Communication research Institute (ACRI), Sharif University of Technology
†Electronic Research Center (ERC), Sharif University of Technology
{akhaee, nikooienejad}@ee.sharif.edu, and ghaemmagh, marvasti@sharif.edu

ABSTRACT

In this paper, a novel quantization based watermarking method is proposed. For blind detection, a set of nonlinear convex functions based on geometric mean are investigated. In order to achieve minimum distortion, the optimum function set is found. The algorithm is implemented on the approximation coefficients of wavelet transform for natural images. In order to make the algorithm more robust and imperceptible, a new transform domain called Point to Point Graph (PPG), which converts a 1-D signal to a 2-D one, has been used. The error probability of the proposed scheme is analytically investigated. Simulation results show that this algorithm has great robustness against common attacks such as AWGN, JPEG and rotation in comparison with recent methods presented so far.

Index Terms— Geometric quantization, Minimum distortion, Image watermarking

1. INTRODUCTION

Data hiding is a process in which some information is embedded within a digital media so that the inserted data becomes part of the media. This technique serves a number of purposes such as broadcast monitoring, data authentication, data indexing and so forth [1]-[3]. A digital watermarking system must successfully satisfy trade-offs between conflicting requirements of perceptual transparency, data capacity and robustness against attacks [4]. These trade-offs are investigated in [5], [6] from an information-theoretic perspective.

Quantization Index Modulation (QIM) method is an important blind watermarking class performing close to the system capacity [7]. In this technique, data embedding is attained by quantizing the host feature stream with a quantizer that is selected among a set of quantizers which are associated with different messages. For example, the selection of a scalar quantizer results in a method named Dither Modulation (DM) with bit repetition or a Distortion Compensated version of DM (DC-DM) [8]. The main problem of this approach is the development of quantizer codebooks which are suitable for data embedding. To solve this problem, a new quantizer codebook which is signal-oriented has been introduced in our algorithm.

Here, in order to find an efficient quantizer codebook, first the requirements of suitable codewords are investigated. Then the geometric mean quantization as a class of functions that satisfies these requirements is introduced. The shape parameters of this quantization function are optimized in such a way that less distortion is imposed to the host samples. To have better robustness and transparency simultaneously, PPG mapping proposed in [9] has been used for data embedding. For simplicity, hard decoding is performed for data extraction. The performance of the proposed method is analytically studied and a close form solution for error probability is derived. For implementation, the algorithm is simulated on the wavelet coefficients of various images. Experimental results show a great robustness against common attacks in comparison with two recent techniques MWT-EMD [10] and WTGM [11], which are implemented in the wavelet transform domain.

The rest of the paper is organized as follows. In section 2 the problem of a generic data hiding system is modeled and then a general solution using quantization process is proposed. Section 3 introduces the proposed data hiding algorithm. The performance of the proposed technique is analyzed in section 4. Experimental results are demonstrated in section 5. Finally, section 6 concludes the paper.

2. MATHEMATICAL CONSTRAINTS AND SOLUTION

In this section, the problem of a blind watermarking algorithm is modeled. After investigating the requirements of this problem, a suitable set of functions will be introduced.

2.1. Problem Statement

The procedure of typical quantization based watermarking can be expressed as follows:

$$S = \{s_1, \ s_2, \ \ldots, \ s_n\} \in X$$

$$L = \{q_1, \ q_2, \ \ldots, \ q_m\} \in Q$$

where S and L are the host signal samples and quantization levels, respectively. We define functions $L_m(s) : X \rightarrow Q$

to map each sample to the appropriate quantization level according to the embedded bit m. One conventional example of $L(s)$ is a function which maps each sample to its nearest level. Another group of functions for this process is $f_m(s, q)$: $Q \times X \rightarrow Q$, which quantizes samples according to the appropriate quantization level and the host sample. These functions are applied to the host signal during watermarking procedure. As an example, the following process is applied to a specific host sample s_i and the watermarked one s_i' is obtained,

$$P_m(s_i) = s_i' = f_m(s_i, L_m(s_i)) \qquad (1)$$

where P_m represents the process of embedding bit m. To make the procedure blind, functions f_m and L_m should satisfy the following conditions:

- To meet the definition of a blind process, the algorithm should recognize whether process P_0 or P_1 is applied to the host signal S or not. In fact, finding monotonic processes P_0 and P_1 with different loci and no intersection in their ranges, can be a suitable answer to this problem. Therefore, by counting the number of points in each range, the embedded bit can be extracted.

- In order to have less distortion and good robustness, the distortion imposed to the host signal should be controllable.

Any set of functions that satisfy the above conditions can be used for blind watermarking procedure and the range of these functions can be considered as codewords.

2.2. Solution

2.2.1. General Solution

We introduce a set of functions (f, L) which satisfy appropriate conditions as follows:

$L_0(s)$ = The greatest quantization level smaller than s

$L_1(s)$ = The smallest quantization level greater than s

$$f_m(s_i, L_m(s_i)) = \sqrt[\alpha+\beta]{s_i^\alpha \cdot L_m(s_i)^\beta}, \quad m = 0, 1 \qquad (2)$$

Where α, β are the shape parameters that should be optimized to result in minimized distortion in the watermarking system. In fact, (2) is a generalized geometric mean between s_i and $L_m(s_i)$.

Since $\sqrt[k]{x}$ is a monotonically increasing function, it can be easily shown that:

$$L_0(s) \leqslant f_0(s, L_0(s)) \leqslant \sqrt[\alpha+\beta]{L_1(s)^\alpha \cdot L_0(s)^\beta}$$

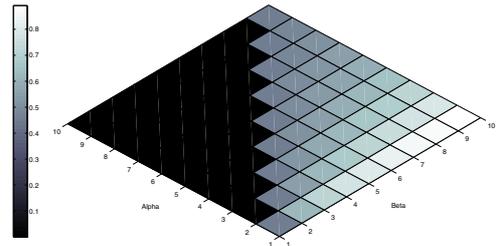$$\sqrt[\alpha+\beta]{L_0(s)^\alpha \cdot L_1(s)^\beta} \leqslant f_1(s, L_1(s)) \leqslant L_1(s)$$

Fig. 1. The amount of distortion $|s' - s|$ for different values of α and β

Therefore, the range of the process P_0 is

$$\left[L_0(s), \ \sqrt[\alpha+\beta]{L_1(s)^\alpha \cdot L_0(s)^\beta} \right]$$

and the range of the process P_1 is

$$\left[\sqrt[\alpha+\beta]{L_0(s)^\alpha \cdot L_1(s)^\beta}, L_1(s) \right]$$

In order to have blind detection, these ranges should be disjoint. Consequently,

$$\sqrt[\alpha+\beta]{L_1(s)^\alpha \cdot L_0(s)^\beta} \leqslant \sqrt[\alpha+\beta]{L_0(s)^\alpha \cdot L_1(s)^\beta}$$

As long as $\beta + \alpha \geqslant 0$, the above equation results in

$$L_0(s)^{\beta-\alpha} \leqslant L_1(s)^{\beta-\alpha}$$

As discussed in (2), we have $L_0(s) \leqslant L_1(s)$. Thus

$$\beta \geqslant \alpha \qquad (3)$$

2.2.2. Parameter Optimization

Here, the goal is to find the exact value of α and β which minimizes distortion in the data embedding procedure. Since we cannot solve this problem mathematically, we gain from numerical analysis. To this aim, we plot the expected value of the difference between $s' = f_1(s, L_1(s))$ and a Gaussian variable s with a fixed $L_1(s)$ for different values of α and β. This same process is performed for $f_0(s, L_0(s))$. As discussed earlier, this figure is valid for values where β is greater than α. In Fig. 1, light colors show more distortion, while dark colors show less distortion. It is obvious that distortions are equal along the line $\alpha = \beta$. As demonstrated in this figure, the optimum value for α, β is 1. Thus, the final solution for the problem is

$$f_m(s_i, L_m(s_i)) = \sqrt{s_i \cdot L_m(s_i)}, \quad m = 0, 1 \qquad (4)$$

3. PROPOSED METHOD

3.1. Data Embedding

In this section, according to the aforementioned solution, a method for data hiding is presented. We define the region for
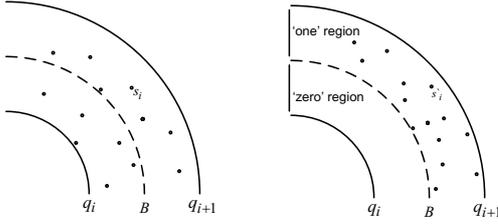
Fig. 2. The representation of samples before and after data embedding the bit '1'

'zero' and 'one' bits between two consecutive quantization levels.

Suppose q_{i-1}, q_i as two successive quantization level. The range of the process P_0 defined in the previous section, specifies the 'zero' area and the range of the process P_1 specifies the 'one' area between these two quantization levels. The main idea for making the process more robust against attacks, is changing these two areas for the next two quantization levels q_i and q_{i+1}, periodically. Therefore, the two regions before and after q_i is belong to the bit '1'. Consequently the same applies to the bit '0' in the quantization level q_{i+1}, and so on. It is noteworthy that these levels are concentric circular levels in 2-D PPG mapping and the codewords of bits '0' and '1' are concentric rings. The following steps explain the overall procedure of the data embedding:

- The host image is segmented into blocks and blocks with higher variance are selected.

- wavelet transform and 2-D PPG mapping are applied to the samples of the selected blocks.

- Quantization process takes place by applying the function $f_m(s_i, L_m(s_i))$ to all samples between two consecutive quantization levels according to bit m, with $L_0(s)$ and $L_1(s)$. In fact, this process moves each sample into the desired 'zero' or 'one' rings. This procedure can be explained briefly as follows:

$$\begin{cases} s' = \sqrt{s \cdot q_i} & i = \text{even} \\ s' = \sqrt{s \cdot q_{i+1}} & i = \text{odd} \end{cases} \quad \text{to embed bit '1'}$$

$$\begin{cases} s' = \sqrt{s \cdot q_i} & i = \text{odd} \\ s' = \sqrt{s \cdot q_{i+1}} & i = \text{even} \end{cases} \quad \text{to embed bit '0'} \quad (5)$$

and the separation line between 'zero' and 'one' rings is

$$B = \sqrt{q_i \cdot q_{i+1}} \quad (6)$$

- After applying geometric mean quantization, the inverse PPG and wavelet transform are applied to the manipulated samples and the stego image is reconstructed.

Figure (2) shows the original and watermarked samples after embedding the bit '1'.

3.2. Data Extraction

For data extraction, the watermarked image is segmented into blocks and selected blocks are chosen. The embedded bit is extracted by applying hard decoding. To this aim, the number of points in all 'one' and 'zero' regions is counted. Then, by comparing these two numbers the hidden bit is decoded. In other words, if the number of samples in 'zero' regions is more than the 'one' regions, the bit '0' will be detected and vice versa.

4. PERFORMANCE ANALYSIS

For performance evaluation, we assume samples to have i.i.d Gaussian distribution $N(0,1)$ which are contaminated by an additive white Gaussian noise $N(0, \sigma_n^2)$. This statistical model may be valid for low frequency components of natural signals after appropriate decimation [12]. If no quantization process is applied to the samples, since the mean of the samples is zero the distribution of noisy samples would be Rayleigh as:

$$f_R(r) = \frac{r}{\sigma^2} e^{\frac{-r^2}{2\sigma^2}} \quad r > 0 \quad (7)$$

where $\sigma^2 = \sigma_x^2 + \sigma_n^2$. After data embedding, the mean value of the point is no longer zero, therefore the distribution is not Rayleigh any more. As in (5), the new mean value for each sample component between levels q_i, q_{i+1} in 2-D plain depends on the embedded bit as well as i. Let these values be γ_x and γ_y for each component, respectively. If $\gamma_i = \sqrt{\gamma_{ix}^2 + \gamma_{iy}^2}$, the distribution of samples between these two levels is Rician as:

$$f_R(r|q_i) = \frac{r}{\sigma^2} e^{\frac{-(r^2+\gamma_i^2)}{2\sigma_n^2}} I_0(\frac{r\gamma_i}{\sigma}) \quad r > 0 \quad (8)$$

Thus, from (7), (8), the probability of being a typical sample in '0' region after quantization process would be,

$$P_Z = \int_{q_1}^{q_1+\delta_1} \frac{r}{\sigma^2} e^{\frac{-(r^2+\gamma_i^2)}{2\sigma_n^2}} I_0(\frac{r\gamma_i}{\sigma}) dr +$$

$$\sum_{i=3,odd}^{M} \int_{q_i-\gamma_{i-1}}^{q_i+\delta_i} \frac{r}{\sigma^2} e^{\frac{-(r^2+\gamma_i^2)}{2\sigma_n^2}} I_0(\frac{r\gamma_i}{\sigma}) dr \quad (9)$$

where δ_i is the distance between level q_i and the separation line between two areas discussed in (6). γ_i is the distance from this line to level q_{i+1}. In the same way, the probability of laying a sample in '1' region is,

$$P_U = \sum_{i=2,even}^{M} \int_{q_i-\gamma_{i-1}}^{q_i+delta_i} \frac{r}{\sigma^2} e^{\frac{-(r^2+\gamma_i^2)}{2\sigma_n^2}} I_0(\frac{r\gamma_i}{\sigma}) dr \quad (10)$$

where M is the number of quantization levels. Since samples after the last quantization level are not quantized, depending on the value of M, whether even or odd, for (9) or (10), δ_i is not included in upper bound of the integral. As a result, the

probability of other samples that are not included in the data hiding process would be,

$$P_{others} = 1 - P_Z - P_U \qquad (11)$$

Error occurs when the bit '0' is embedded while the number of points in the '0' region is less than the '1' region and vice versa. Therefore, the probability of error in two cases of embedding bits '1' or '0' is as follows,

$$P_{e|0} = \sum_{i_{others}}^{N} \binom{n}{i_{others}, i_1, i_0} \cdot (P_{others})^{i_{others}} \cdot (P_Z)^{i_0} \cdot (P_U)^{i_1}$$

$$\begin{cases} i_{others} + i_0 + i_1 = N \\ i_1 > i_0 \end{cases} \quad \text{For embedding bit '0'} \qquad (12)$$

$$P_{e|1} = \sum_{i_{others}}^{N} \binom{n}{i_{others}, i_1, i_0} \cdot (P_{others})^{i_{others}} \cdot (P_Z)^{i_0} \cdot (P_U)^{i_1}$$

$$\begin{cases} i_{others} + i_0 + i_1 = N \\ i_1 < i_0 \end{cases} \quad \text{For embedding bit '1'} \qquad (13)$$

Because of the symmetry, the total probability of error in this algorithm is,

$$P_e = \frac{1}{2}(P_{e|0} + P_{e|1}) \qquad (14)$$

5. SIMULATION RESULTS

Throughout our experiments, we use the Daubechies length-8 Symlet filters with two levels of decomposition to compute the 2-D DWT. The 2-D PPG mapping with the index parameter $k = 4$ has been applied to the second level approximation coefficients of each block. The results are obtained by averaging over 100 runs with 100 different pseudo-random binary sequences as the watermarking signal. In our implementation, the host image is segmented into small blocks of 16×16 and high variance blocks are chosen for bit embedding. Thus, in the decoding process the indices of these blocks are needed. However, there is an interesting approach proposed in [13] in which selected block indices are estimated using error correction codes. By combining this scheme with the proposed method, the blindness of the proposed scheme is guaranteed.

For our simulations, we use three natural images (*Lena, Baboon, and Peppers*) of size 512×512. These images are chosen for their different features. The original test images and their watermarked version using proposed method with 512 bits message length are shown in Fig. 3. The Peak Signal to Noise Ratio (PSNR) of the watermarked images are 39.12dB, 38.88dB, 39.29dB respectively. As shown in Fig. 3 the invisibility of the watermark is completely satisfied.

Fig. 4 shows the performance of the algorithm against AWGN attack. As demonstrated, great robustness is achieved even in highly noisy environment $\sigma_n = 20$. Fig. 5 emphasize
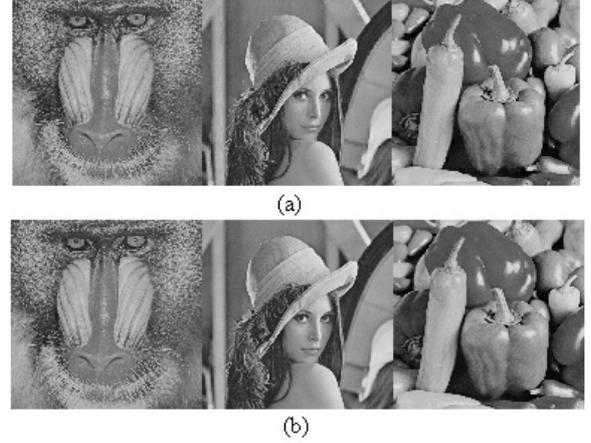

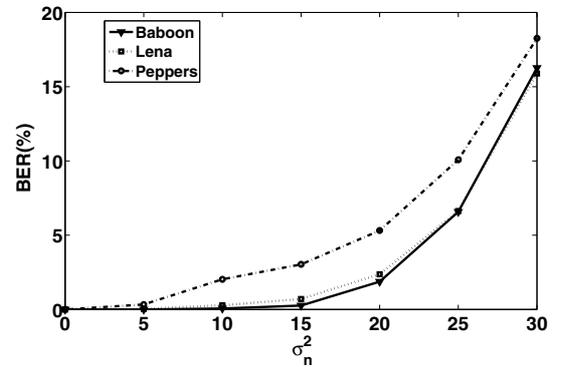**Fig. 3**. (a) Watermarked and (b) Original test images: *Baboon*, *Lena* and *Peppers*.

Fig. 4. Robustness of our method against AWGN attack. BER(%) versus Noise variance (σ_n^2)
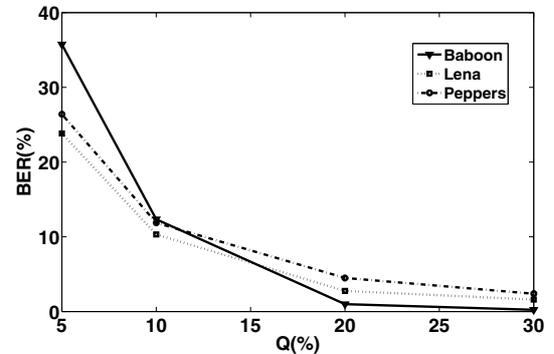

Fig. 5. Robustness of our method against JPEG compression attack. BER(%) versus Image Quality (%)

that this method has also a great performance against JPEG compression attack. The main reason that the algorithm is highly robust against noise and JPEG compression attack is that the embedding process is performed with minimal distortion on the approximation coefficients of image blocks.

In the table 1, robustness of the proposed algorithm against Median filtering and Rotation attacks has been depicted. This table shows that the method has outstanding resistance against these two attacks specially rotation.

Table 1. Robustness of Proposed Algorithm Against Median Filtering and Rotation Attack. BER(%)

Image	Rotation Angle (Degree)			Median Filtering	
	1	3	5	3×3	5×5
Lena	0.3	1.5	1.9	4.9	15.2
Peppers	0.7	1.9	2.8	5.4	15.6
Peppers	0.1	2.24	3.43	16.8	36.7

Table 2. Comparison Between Our Watermarking Method and MWT-EMD Method [10]. Under JPEG Compression and Median Filtering Attack. BER(%) (Message Length=64 Bits; PSNR=42 DB)

Method	Image	JPEG Quality Factor			Median Filtering
		5	10	20	3×3
MWT-EMD [10]	Baboon	4.6	0.0	0.0	12.5
Proposed	Baboon	4.1	0.0	0.0	7.5
MWT-EMD [10]	Peppers	6.2	0.0	0.0	7.8
Proposed	Peppers	4.0	1.0	0.0	4.2

Table 3. Comparison Between Our Watermarking Method and MWT-EMD Method [10]. Under Noise and Rotation Attack. BER(%) (Message Length=64 Bits; PSNR=42 DB)

Method	Image	Noisy Image PSNR		Rotation Angle (Degree)	
		17	15	1	2
MWT-EMD [10]	Baboon	1.0	6	53.1	43.7
Proposed	Baboon	1.1	4.7	0.0	0.6
MWT-EMD [10]	Peppers	1.1	5.9	62.5	48.44
Proposed	Peppers	2.4	5.2	0.0	0.0

Table 4. Comparison Between Our Watermarking Method and Tsai's WTGM Method [11]. Under Some Common Attacks. BER(%) (Message Length=512 Bits; PSNR=39 DB)

Method	Image	JPEG $Q = 30\%$	JPEG $Q = 50\%$	Median 4×4	Rot $1°$
WTGM [11]	Goldhill	8.4	3.1	22.0	10.9
Proposed	Goldhill	1.1	0.2	14.1	0.0
WTGM [11]	Peppers	2.4	0.2	17.6	6.2
Proposed	Peppers	1.6	1.3	10.7	0.5

To be robust against rotation attack a synchronization technique should be performed which is rather time consuming. Here, we propose a synchronization technique to estimate the rotation angle, rotate back the image, and then decode the watermark code. To find the exact rotation angle, we divide our range of acceptable rotation angles in $[-5°, 5°]$ to 20 small segments to find the rotation angle with the accuracy of $0.5°$. By counting the number of points in '0' and '1' regions of each block, we evaluate the ratio of this two numbers for all blocks. An angle which maximizes this ratio for most of the blocks is considered as rotation degree. After recognizing this angle, we rotate the watermarked image by the inverse angle and the image would be ready for data extraction process.

5.1. Comparison With Other Techniques

We have compared our watermarking algorithm with its nearest competitors, namely the algorithms in [10] and [11], which are blind and non-blind techniques, respectively. The methods in [10] and [11] were chosen since both methods were implemented in the wavelet transform domain. To be fair, the bit rate and the power of watermark of the propopsed technique are set with those reported in their papers. According to Table 2, we see that the proposed scheme outperforms MWT-EMD except in JPEG with quality factor 10. Since the image Pepper is rather smooth the performance of the proposed method a little decreases. In Table 3, it is shown that our method is highly robust against rotation attack while the MWT-EMD completely fails in this case. However, in the noisy environment the BERs of both methods are nearly similar. From Table 4, the magnificence of our algorithm compared with this recent technique is obvious.

6. CONCLUSION

Here, the requirements of the blind quantization based watermarking scheme is analytically investigated. By modeling the constrains of this problem, geometric mean quantization is introduced as a class of solution functions. The shape parameters of this quantization based method is optimized to yield the minimum distortion to the host signal. Consequently, the proposed method works near the capacity rate. The PPG and Wavelet transform are used to increase the robustness and invisibility simultaneously. Experimental results show great robustness of the proposed algorithm against common attacks in comparison with recent schemes. As a future work, the soft decoding will be implemented for data extraction.

7. REFERENCES

[1] J. Seitz, *Digital watermarking for digital media*, Information Science Publishing, 2005.

[2] C.S. Lu, *Multimedia security: Stenography and digital watermarking techniques for protection of intellectual property*, Idea Group Publishing, 2004.

[3] G.C. Langelaar, I. Setyawan, and R.L. Lagendijk, "Watermarking digital image and video data: A state-of-the-art overview", *IEEE Trans. Signal Process. Magazine*, vol. 17, no. 5, pp. 20–46, 2000.

[4] S. Katzenbeisser and F.A.P. Petitcolas, *Information hiding techniques for steganography and digital watermarking*, Artech House, Boston, 2000.

[5] P. Moulin and J.A. O'Sullivan, "Information-Theoretic Analysis of Information Hiding," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 563–593, 2003.

[6] A. Maor and N. Merhav, "On joint information embedding and lossy compression in the presence of a stationary memoriless attack channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3166–3175, 2005.

[7] B. Chen and G. Wornell, "Quantization Index Modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Trans. on Information Theory*, vol. 47, pp. 1423-1443, May, 2001.

[8] J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding," *IEEE Trans. on Signal Process.*, vol. 4, pp. 1003-1019, Apr, 2003.

[9] M. A. Akhaee, M. J. Saberian, S. Feizi and F. Marvasti, "Robust Audio data hiding using correlated quantization with histogram based detector," *IEEE Trans. on Multimedia*, vol. 11, no. 5, pp. 834-842, Aug. 2009.

[10] N. Bi, Q. Sun, D. Huang, Z. Yang, and J. Huang, "Robust image watermarking based on multiband wavelets and empirical mode decomposition," *IEEE Transactions on Image Processing*, vol. 16, no. 8, pp. 1956–19966, 2007.

[11] M. J. Tsai and C.H. Shen, "Wavelet Tree Group Modulation (WTGM) for digital image watermarking," *Proc. of int. Conf. on Acoustics, Speech and Signal Processing*, vol. 2, pp. 173–176, 2007.

[12] M. A. Akhaee, S. M. E. Sahraeian, B. Sankur, and F. Marvasti, "Robust Scaling-Based Image Watermarking Using Maximum-Likelihood Decoder With Optimum Strength Factor," *IEEE Trans. on Multimedia*, vol. 11, no. 5, pp. 822-833, Aug. 2009.

[13] K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Robust image-adaptive data hiding based on erasure and error correction," *IEEE Trans. Image Process.*, vol. 13, no. 12, pp. 1627–1639, Dec. 2004.