A ROBUST SPREAD-SPECTRUM WATERMARKING METHOD USING TWO-LEVEL QUANTIZATION

Anthony T.S. Ho and Feng Shu

School of Electrical and Electronic Engineering
Nanyang Technological University
Nanyang Avenue, Singapore 639798
etsho@ntu.edu.sg

ABSTRACT

In this paper, we introduce a new robust watermarking technique, which is called *two-level quantization based spread-spectrum* (TQSS). In this method, the selected transform coefficients of the cover signal are two-level quantized to a pre-defined threshold, which is determined by the estimated bound of distortion. The two-level quantizer is again used for watermark retrieval. Thus, the watermark signal is essentially embedded into the polarities of the transform coefficients. Our simulation results showed that TQSS outperformed some common spread-spectrum (SS) methods under a variety of attacks, such as lossy compression, additive Gaussian white noise, filtering, scaling and print-and-scan process.

1. INTRODUCTION

The problems of illegally using, pirating and counterfeiting digital images, video, audio and electronic documents have led to the rapid development of digital watermarking. There exist different watermarks designed for various applications. A robust watermark is usually used to verify the ownership of the protected media and a fragile watermark is designed for authentication or tamper proofing and thus it must be sensitive to any accidental or intentional manipulations. In this paper, we focus on robust watermarking problems.

In a watermarking system, the watermark is inserted by modifying the cover data either in spatial or transform domain in a certain way. A significant number of watermark embedding methods have been proposed in the literature. Many early watermarking schemes embedded the watermark by using low-bit(s) modulation (LBM) [1]. In [2], Chen and Wornell proposed a new embedding method called quantization index modulation (QIM), in which the watermark message was viewed as an index to select a particular quantizer from an set of possible quantizers and then the watermark was embedded by applying the selected quan-

tizer. However, QIM is very sensitive to the scaling attack [3].

Cox et al. [4] suggested an additive spread-spectrum (SS) based embedding method, in which a noise-like watermark sequence was added to the frequency domain of the cover signal. In [5], Hartung and Girod proposed to spread the watermark bits by using a chip-rate, and then the spreaded sequence was modulated by a binary pseudo-noise sequence. For detection, the watermarked signal was first filtered by the pseudo-noise sequence, and the sign detector was used to extract the watermark bits. Other similar watermarking techniques can be found in [6, 7]. We call the above-mentioned methods traditional spread-spectrum (TSS) watermarking approaches. As the performance of these traditional SS based methods suffers from the interference of the cover signal, Malvar and Florencio [3] proposed an improved spread-spectrum (ISS) modulation technique to reduce the interference from the signal, which was proved to achieve a significant performance improvement over the TSS methods.

In this paper, we introduce a novel SS based approach for robust watermarking: two-level quantization based spread-spectrum (TQSS), which essentially embeds the watermark bits into the polarities of the frequency components of the cover signal. Section 2 introduces the background knowledge of the proposed method. Our proposed algorithm is presented in Section 3. In Section 4, we show the simulation results of TQSS and conclusions are drawn in the last section.

2. BACKGROUD

2.1. Two-level quantization

The two-level quantizer is defined as follows.

$$Q(x) = \begin{cases} 1 & x \geq 0 \\ 1 & \text{else} \end{cases} \qquad (1)$$

Many watermarking methods employed the two-level

quantizer as the sign detector for watermark detection [3, 5]. The sign detector addresses the problem of detecting signals by using very coarse information about the statistical behavior of the noise. In a robust watermarking scenario, the perturbation noise is unknown and thus its statistical characteristic may not be simply estimated [8]. therefore, the two-level quantization could be employed as a useful alternative detection method which achieves a good trade-off of robustness and complexity. In this paper, we employ the two-level quantizer for watermark retrieval. Furthermore, prior to embedding the watermark signal, we also quantize the selected frequency coefficients of the cover signal into two levels. Thus, instead of embedding the information by modifying the amplitude of the coefficients, we essentially insert the watermark bits to the polarities of the frequency components.

2.2. Distortion bound

In a general digital watermarking scheme, the embedded information is superimposed to the cover signal by introducing small modifications. The watermark embedding process can be described by

$$s = x + w \qquad (2)$$

where x denotes a representation (e.g., a sequence of transform coefficients) of the cover signal, w denotes the watermark signal and s the watermarked signal. The watermarked signal s generally goes through a distortion channel.

$$y = s + n \qquad (3)$$

where y and n denote the distorted watermarked signal and the perturbation noise, respectively. Thus, the distortion caused by the channel is:

$$E[D] = \|n\| = \|y \quad s\| \qquad (4)$$

For a robust watermarking system, the distortion n could be from both common signal manipulations (such as format conversion) and intentional attacks by adversaries. Therefore, it is very difficult to completely characterize the distortion channel [9]. However, the objective of an adversary is not only to destroy the embedded watermark but also to reclaim the ownership of the documents. Thus, the attacks are constrained by certain criteria (e.g., image's visual quality).

The distortion bound can be defined as the range of degradation caused by the possible attacks, while the quality of the attacked signal still satisfies the defined criteria. However, the distortion bound is difficult to calculate exactly. The first reason is that it is difficult to define a general subjective or objective quality measurement method to assess all the multimedia documents to be protected. Thus,
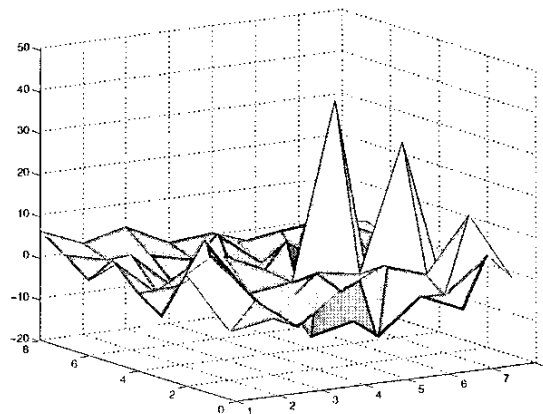

Fig. 1. DCT coefficient difference after JPEG 30 compression.

the strength of attacks could be very different because of the different quality measurement methods. Furthermore, at the stage of embedding, the distortion channel is unknown. The attack could be a single manipulation, combination of many manipulations (e.g., the digital-analogue-digital conversion), or even a totally new attack to the embedder. However, the distortion bound can be estimated and used during watermark embedding after we investigate how the common attacks degrade the watermarked signal. An 8x8 Discrete Cosine Transform (DCT) is chosen in our experiments. For simplicity, a randomly-selected 8x8 block B_{ij} ($1 \leq i,j \leq 8$) of LENA is used for demonstration. Fig. 1 illustrates the difference matrix of frequency coefficients between the cover image subblock B_{ij} and the distorted subblock $\widehat{B_{ij}}$. JPEG compression with a quality factor of 30 is used here as an attack. In Fig.1, it can be easily observed that the distortion of most frequency components caused by JPEG 30 is approximately within a range of 10.

A simple method to estimate the distortion bound T_d is to calculate the mean of the difference between B_{ij} and $\widehat{B_{ij}}$, weighted by a strength factor α.

$$T_d = \frac{\alpha}{N^2} \sum_{m=n=1}^{N} \left| B_{mn} \quad \widehat{B_{mn}} \right| \qquad (5)$$

3. TQSS: TWO-LEVEL QUANTIZATION BASED SPREAD-SPECTRUM

In this section, we introduce the watermark embedding and retrieval algorithms. A general framework of the proposed watermarking method is depicted in Fig. 2.

In this framework, before embedding, a two-level quantizer $Q(.)$ is performed to x. The encoder embeds the watermark bits $m : \{1, \quad 1\}$ based on the prior knowledge about
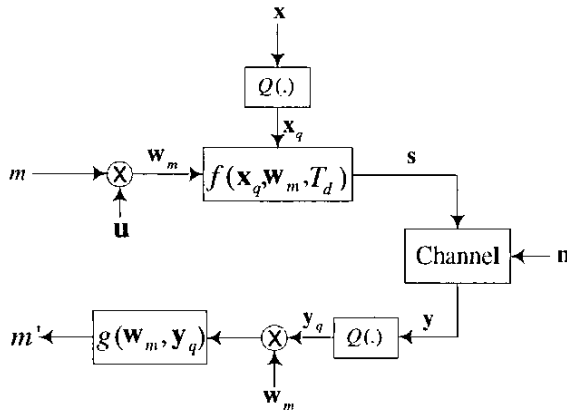
Fig. 2. A framework of the TQSS watermarking technique

the weighted distortion bound T_d. The watermark decoder employs the two-level quantizer again to retrieve the watermark m' from the possible signal-bearing vector y.

3.1. Watermark embedding

Prior to embedding, the watermark bits m are expanded by using a spreading sequence $u : \{1, \ 1\}$, which is produced by a pseudo-random number (PRN) generator. After spreading, according to the watermark bit to be 1 or -1, we obtain a corresponding sequence w_1 or $w_{\ 1}$ as follows.

$$\mathbf{w}_m = m\mathbf{u} \tag{6}$$

The entire watermark embedding process is divided into two passes, polarity modulation and amplitude modulation.

Polarity Modulation In pass 1, x first goes through the two-level quantizer $Q(.)$, and then a binary sequence $\mathbf{x}_q$ is generated. We can always find a $\mathbf{x}_q^*$, which satisfies,

$$\langle \mathbf{w}_m, \mathbf{x}_q^* \rangle \geq T_s \tag{7}$$

where $\langle . \rangle$ denotes the inner product and T_s denotes an appropriate positive threshold. The inner product is defined as follows.

$$\langle \mathbf{a}, \mathbf{b} \rangle = \frac{1}{N} \sum_{i=0}^{N\ 1} a_i b_i \tag{8}$$

where $\mathbf{a}, \mathbf{b}$ are vectors with length of N, and a_i, b_i are elements of $\mathbf{a}, \mathbf{b}$, respectively.

To find $\mathbf{x}_q^*$, we define a polarity modulation function, which is used to toggle values in the binary sequence $\mathbf{x}_q$. If the inner product between $\mathbf{w}$ and $\mathbf{x}_q$ is less than T_s, we toggle one bit in $\mathbf{x}_q$, then compute the inner product again,

until the inner product value is greater than or equal to the pre-defined threshold T_s.

Amplitude Modulation In the second pass, the amplitude modulation is performed as follows.

$$s_i = \begin{cases} x_{qi}^* \ T_d & \text{if } |x_i^*| \leq T_d \\ x_i^* & \text{else.} \end{cases} \tag{9}$$

where s_i denotes the modified transform coefficient, x_i^* denotes the polarity modulated coefficients and x_{qi}^* is the output of the two-level quantized x_i^*. As described in the Equation 9, only the frequency coefficients whose amplitudes are smaller than the distortion bound T_d are modified, and those coefficients with higher amplitude are remain intact.

3.2. Watermark decoding

For watermark decoding, we first locate the watermarked coefficients and perform a two-level quantizer to find the polarity sequence $\mathbf{y}_q$. The pseudo-random sequence $\mathbf{u}$ is reproduced by using the seed from the secret key.

A minimum distance (MD) detector is then performed to decide the watermark bits.

$$m' = \arg \min_{m=1, \ 1} \left(dist(\mathbf{w}_m, \mathbf{y}_q) \right) \tag{10}$$

where m' denotes the extracted watermark bit and $dist(.)$ denotes the Hamming distance function.

4. SIMULATION RESULTS

In our experiments, we employed an 8x8 DCT transform and pseudo-randomly selected subblocks for embedding. The LENA image was used for testing. We compared our proposed TQSS with TSS and ISS methods. We fixed the amount of embedded watermark bits and modified the embedding strength to obtain the same perceptual quality of the watermarked images. Fig. 3 and Fig. 4 illustrate the performance comparisons under JPEG compression and additive Gaussian white noise (AWGN), respectively. Table 1 shows the simulation results under more attacks. It can be observed that when the attack-induced noise becomes dominant in the watermarked signal, ISS achieves similar robustness to TSS. However, in TQSS, as long as most of the polarities of the transform coefficients remain unchanged, the watermark can be always correctly decoded.

In this paper, we restrict our attention to the non-geometric attacks and assume that the watermark detector is always synchronized. Some geometric attacks, such as scaling is also included in our experiments, but we assume the size of the cover signal is available for the decoder and thus the size of the inspected image is restored prior to watermark detection.
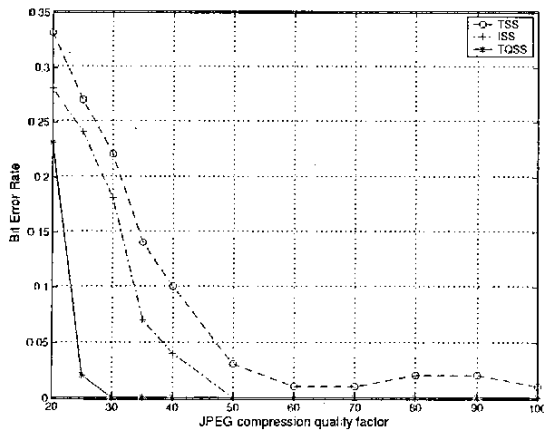
Fig. 3. Performance comparison under lossy compression

Fig. 4. Performance comparison under AGWN

Attack	TSS	ISS	TQSS
Gaussian filtering	0.03	0	0
Sharpening	0	0.01	0
Median filtering			
Wiener filtering	0.11	0.03	0
Scaling(40%)	0.21	0.16	0
Scaling(35%)	0.25	0.20	0.06
JPEG70+AWGN(10dB)	0.08	0.05	0.03
JPEG70+Median filtering	0.15	0.10	0
JPEG70+Scaling(60%)	0.35	0.30	0.12
Print-and-scan[1]	0.30	0.21	0.15

Table 1. Bit error rates under more attacks.

5. CONCLUSION

We introduced a new robust watermarking algorithm known as two-level quantization based spread-spectrum (TQSS). In TQSS, the watermark bits were essentially embedded into the polarities of the frequency components of the cover signal. When compared with other well-known SS-based watermarking techniques, our proposed method was found to achieve a significant improvement under a variety of attacks, such as lossy compression, additive Gaussian white noise, scaling, filtering and print-and-scan process.

6. REFERENCES

[1] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," in *Proc. SPIE*, 1995, vol. 2420.

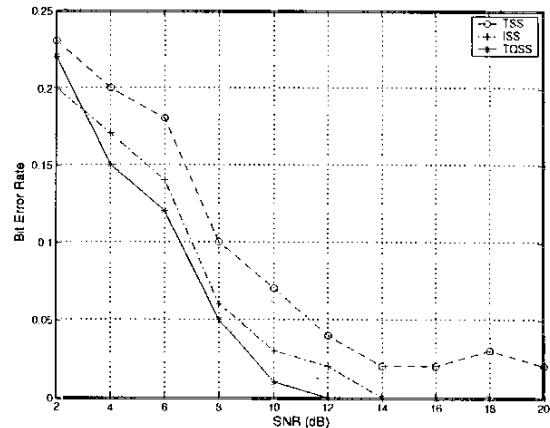[2] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digi-

tal watermarking and information embedding," *IEEE Trans. Information Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[3] H. S. Malvar and D. A. F. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. Signal Processing*, vol. 51, no. 4, pp. 898–905, 2003.

[4] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[5] F. Hartung and B. Girod, "Fast public-key watermarking of compressed video," in *International Conference on Image Processing (ICIP'97)*, Santa Barbara, California, U.S.A., 1997, vol. I, pp. 528–531.

[6] M. George, J.-V. Chouinard, and N. Georganas, "Digital watermarking of images and video using direct sequence spread spectrum techniques," in *Proceedings of 1999 IEEE Canadian Conference on Electrical and Computer Engineering*, 1999, vol. 1, pp. 116–121.

[7] S. Cheng, H. Yu, and Z. Xiong, "Enhanced spread spectrum watermarking of mpeg-2 aac," in *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2002, vol. 4, pp. 3728–3731.

[8] H.V. Poor, *An Introduction to Signal Detection and Estimation*, New York: Springer-Verlag, 1994.

[9] J.J. Eggers and B.Girod, "Quantization effects on digital watermarks," *Signal Processing*, vol. 81, no. 2, pp. 239–263, 2001.

[1]The printer and scanner used in our experiments are HP LaserJet 5000GN and CanoScan1220U respectively.