Quantum Watermarking: A Review

Debnath Bhattacharyya[1], Pallabi Chakraborty[2],
Farkhod Alisherov[1], Tai-hoon Kim[1*]

[1]*Multimedia Engineering Department*
Hannam University
Daejeon, South Korea
debnath@sersc.com, sntdvl@yahoo.com, taihoonn@empal.com

[2]*Computer Science and Engineering department*
Heritage Institute of Technology
Kolkata, India.
pallabi2007@gmail.com

Abstract

Watermarking is the practice of imperceptibly altering a cover to embed a message about that cover. Watermarks are inseparable from the cover in which they are embedded. Unlike cryptography, watermarks can protect content even after they are decoded. Quantum watermarking is a new-born subfield of the young field of digital watermarking. In this paper, we review the proposed encoding decoding algorithm for quantum watermarking.

Keywords: *Security, quantum, data hiding, watermarking.*

1. Introduction

Biometrics are automated methods of recognizing a person based on a physiological or Watermarking is a process of embedding information into digital data in a secret and inconspicuous way. Today watermarking is widely used in applications of copyright protection, fingerprinting, copy protection, content authentication, data hiding, etc. We can classify watermarking in two general categories: spatial domain and frequency domain watermarking. In frequency domain watermarking, media is transformed from spatial to frequency domain, then some watermarking algorithm is applied, and finally watermarked data is transformed back to spatial domain. Additionally, for some media types, certain decoding and encoding operations can take place before and after watermarking algorithm is applied.

Watermarking applications:

A. Copyright protection– Most prominent application. Embed information about the owner to prevent others from claiming copyright. Require very high level of robustness.
B. Copy protection – Embed watermark to disallow unauthorized copying of the cover. For example, a compliant DVD player wills not playback or copy data that carry a "copy never" watermark.
C. Content Authentication – Embed a watermark to detect modifications to the cover. The watermark in this case has low robustness, "fragile".

*Corresponding Author

D. Transaction Tracking – Embed a watermark to convey information about the legal recipient of the cover. This is useful to monitor or trace back illegally produced copies of the cover. This is usually referred to as "fingerprinting".
E. Broadcast Monitoring – Embed a watermark in the cover and use automatic monitoring to verify whether cover was broadcasted as agreed.

2. Watermarking Encoding and Decoding Block Diagram

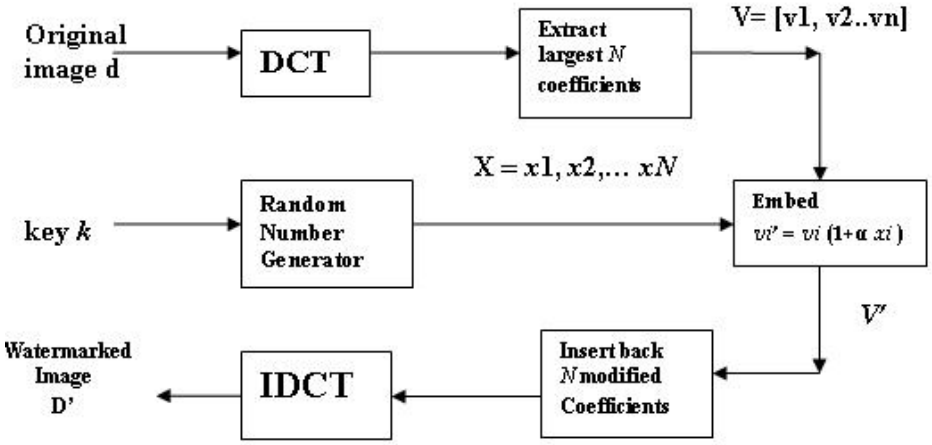


Figure 1. Watermarking Encoder.

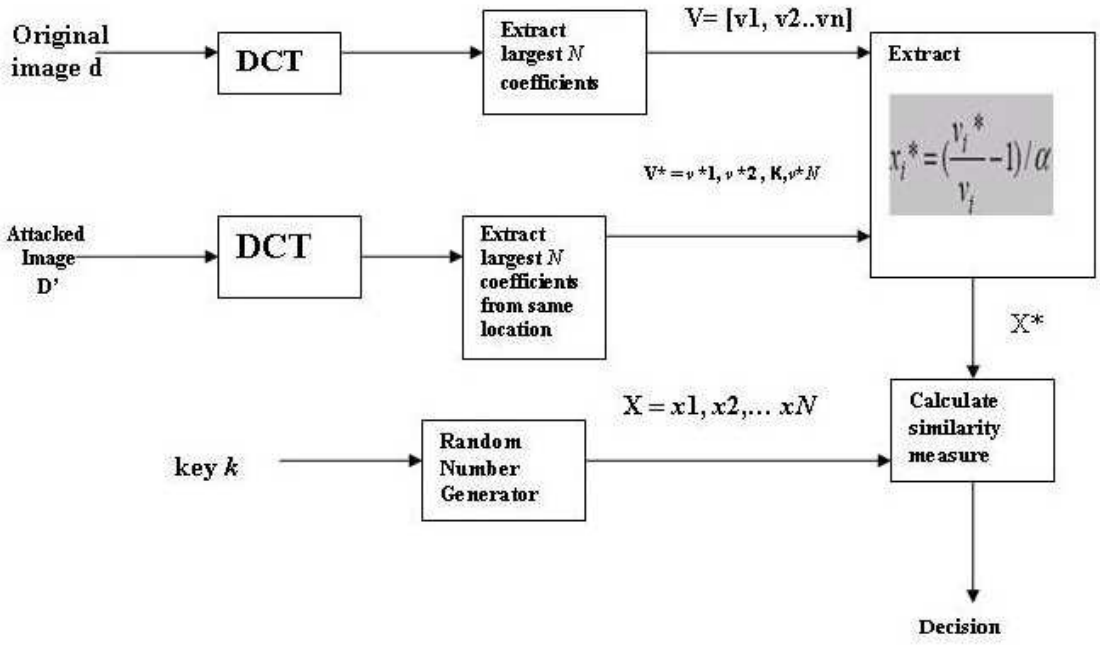
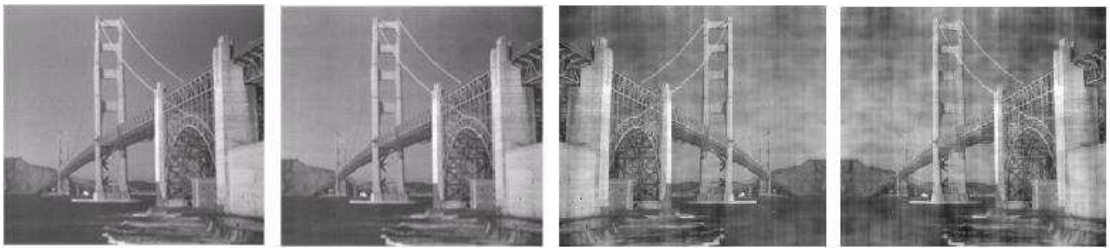


Figure 2. Watermarking Decoder.

Example:



Original α=0.1 α=0.4 α=0.6

Figure 3. Watermarking Encoding and Decoding.

3. Previous Works

A. Watermarking Algorithm for Fingerprinting Intelligence Images:

The rapid growth of digital multimedia technologies brings tremendous attention to the field of digital watermarking. One application for digital watermarking is fingerprinting. The owner or the distributor of the multimedia data can insert unique watermarks into copies for different customers or receivers, which will be helpful to identify the source of illegal copies. Fingerprinting can be used in an intelligence agency to trace the source of the leak [3].

B. Algorithms for audio watermarking and steganography:

Broadband communication networks and multimedia data available in a digital format opened many challenges and opportunities for innovation. Versatile and simple-to-use software and decreasing prices of digital devices have made it possible for consumers from all around the world to create and exchange multimedia data. Broadband Internet connections and near error-free transmission of data facilitate people to distribute large multimedia files and make identical digital copies of them. Perfect reproductions in digital domain have promoted the protection of intellectual ownership and the prevention of unauthorized tampering of multimedia data to become an important technological and research issue [4].

4. Author name(s) and affiliation(s)

3. Watermarking Schemes:

3.1. The Watermark Embedding Process:

3.1.1 The Watermark insertion process:

Figure. 4 shows the block diagram of the watermark insertion process. The input image is subjected to a four level discrete wavelet transform (DWT) decomposition using the Daubechies 8-tap filter. The wavelet coefficients of each subband are detected by Sobel edge detector. The wavelet coefficients classified into two groups with respect to a threshold value. Also, another group of coefficients is formulated containing the region around the edges. This is accomplished using a morphological dilation operation with a structuring element of 9×9 [2].

Comparing bioguard and paper[5], it seems bioguard palm vein technology provide advantages, such as :

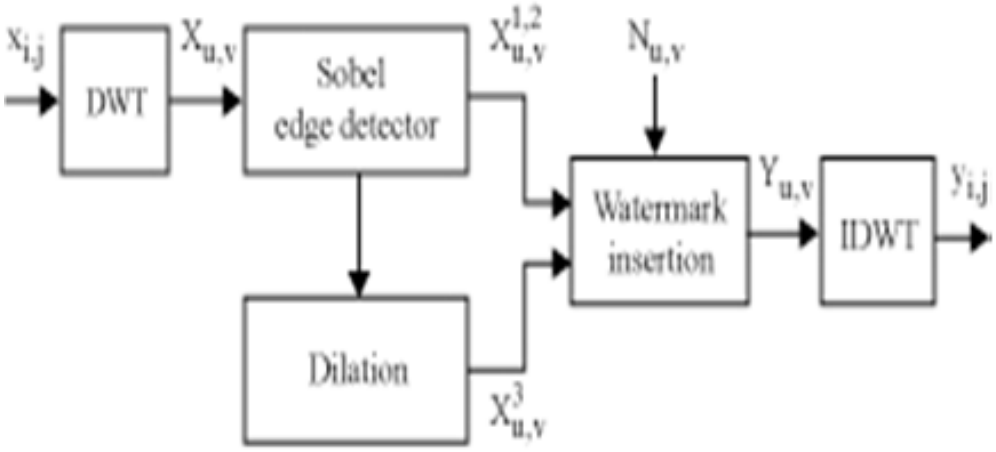


Figure 4: Block diagram of the watermark insertion process

The equation of the watermark insertion process is:

$$Y_{u,v} = (X^{1,2}_{u,v} + X^{3}_{u,v}) + (\alpha_l^{1,2} X^{1,2}_{u,v} + \alpha_l^{3} X^{3}_{u,v}) N_{u,v} \quad (1)$$

Where

$Y_{u,v}$ = the modified wavelet coefficients,

$X^{1,2}_{u,v}$ = the edge selected wavelet coefficients classified into two groups

$X^{3}_{u,v}$ = the coefficients around edges captured by dilation

$\alpha_l^{1,2}$, α_l^{3} = level dependent parameters controlling the watermark strength for the corresponding groups

$N_{u,v}$ = the watermark sequence which is represented by Gaussian noise of zero mean and unit variance.

The detail sub bands, where the watermark is inserted, contain edge information or high frequency coefficients. Consequently, adding the watermark to these coefficients makes the insertion invisible to the human visual system. Moreover, the insertion is scaled according to the decomposition level and the group that coefficients belong to. Finally, the watermarked image is attained by an inverse transform.

3.1.2 The Watermark Detection Process:

Watermark detection is performed by correlating the marked wavelet coefficients of the possibly attacked watermarked image, $\tilde{y}_{i,j}$.

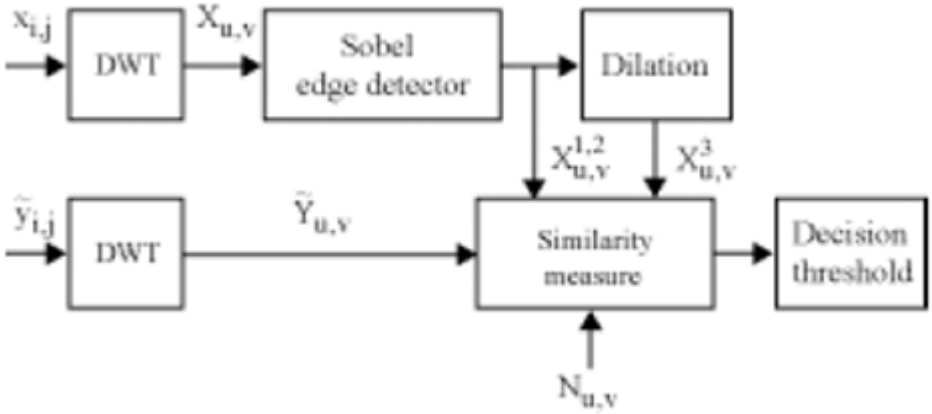


Figure 5: Block diagram of the watermark detection process

Watermark detection is a non-blind process using equation (2)

$$\rho = \frac{1}{MN} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} \tilde{Y}_{u,v} N_{u,v}, \qquad (2)$$

Where

$\tilde{Y}_{u,v}$ = the attacked watermarked coefficients, its provide the groups of the perceptually significant coefficients.

$N\ u, v$ = the watermark sequence.

The correlation factor is compared to a threshold value, which is

$$\rho \rangle T_w \quad true\,watermark$$
$$\rho \langle T_w \quad false\,watermark \qquad (3)$$

Where

$$T_w = 3.97\sqrt{2\sigma^2}. \qquad (4)$$

Variance σ *2* is defined as

$$\sigma^2 = \frac{1}{(MN)^2} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} \left(\tilde{Y}_{u,v}\right)^2. \qquad (5)$$

Where *M, N* are the dimensions of the input image [2].

3.2 A Quantum Watermarking Scheme:

P wrote a digital message. P wants to send that message to her friend Q. P trusts Q enough to send him this message; she wants to be sure that he will not try to claim its authorship. To accomplish this process, P will insert a watermark in her message that has the following properties:

• Imperceptibility– The modifications caused by watermark embedding should be below the perceptible threshold. Here it is not perceptible. Q will not notice the presence of the watermark.

• Robustness– The ability of the watermark to resist distortion introduced by standard or malicious data processing. It is nondestructable, unless the message is destroyed beyond use in the process.

• Security– A watermark is secure if knowing the algorithms for embedding and extracting does not help unauthorized party to detect or remove the watermark. It is uniquely verifiable by a secret that only Q has [1].

P has some quantum message M that she wants to watermark and changes it to M', which contains some watermarking qubits. All qubits $|\Phi i\rangle \in M$ are written in some basis j. To watermark M, P observes the qubits $|\Phi i\rangle$ where $i \in I$, where I is the set of bits in M that we will use for watermarking to M in a dissimilar basis k, producing M', the watermarked message. M' now contains the original qubits written in basis j and the watermarking qubits at $|\Phi' i\rangle \in M'$ where $i \in I$ written in basis k, where k is not equal to j .The watermark is created when M' is observed in the basis j (we denote this as $M' \circ j$). The watermarking qubits, which are written in basis k, will be observed in error of the intended value with a probability of error pe where I and k are the secrets.

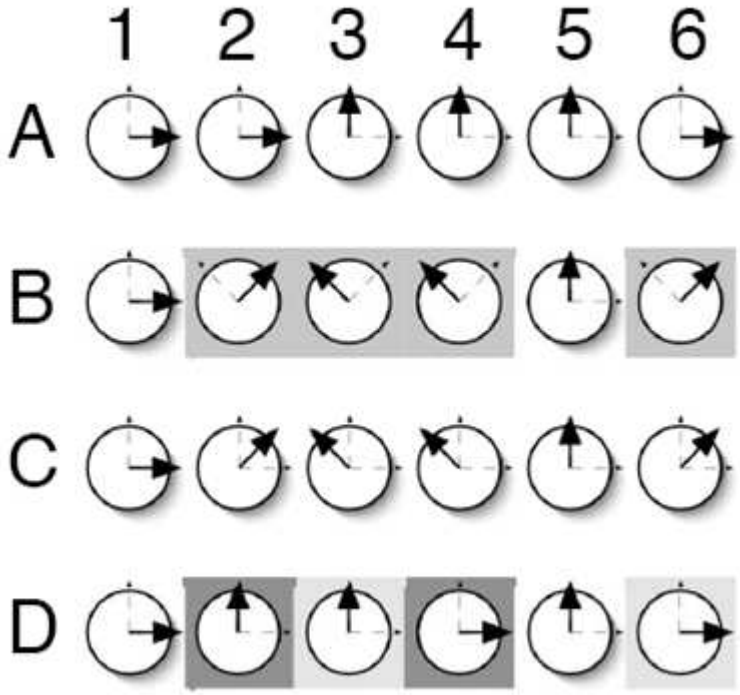
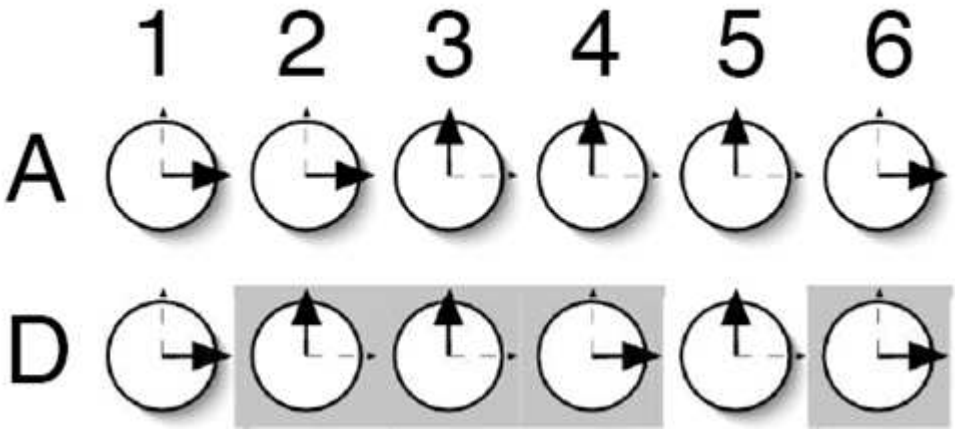


Figure 6: Watermarking process

Consider the example in Figure 6. In this diagram circles represent qubits; dashed lines represent basis states, and the current state of a qubit represented by solid lines. At first our message encoded as qubits in A. Then in B the grayed qubits (i.e. I = 2, 3, 4, 6) are rewritten in a different, secret basis by P. She then sends B to Q, who interprets the message as in C because he does not know which qubits are written in a different basis. When Q observes the message, he gets D with some of the watermarking qubits in error (the dark gray qubits) and some accurately (the light gray qubits) [1].

The Watermarking verification process:

The Figure 6, Figure 7 shows how P would verify that D is the same message as A with her watermark. Here P compares the two messages on the qubits in I and finds the relative frequency of error. P has verified that D is a watermarked A [1].



2 of 4 differ

Figure7: The watermark verification process

4. Results and discussions

The image quality of the watermark embedding process is performed by

$$PSNR = 10\log_{10}\left(\frac{255\times 255}{mse}\right)$$

Where

M, N = Dimensions of the input image

x = original image

y = watermarked image

But sometimes PSNR declines from the perceived subjective quality because the HVS does not correlate well with the mean square error. In this case we can use the weighted PSNR. The equation of weighted PSNR is:

$$wPSNR = 10\log_{10}\left(\frac{255\times 255}{wmse}\right)$$

Where wmse = weighted mean square error

$$wmse = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[\frac{x(i,j)-y(i,j)}{1+\mathrm{var}(i,j)}\right]^2$$

The performance measures are the invisibility of the inserted watermark and the robustness of the method against various types of attacks. The attacks employed for testing are common signal processing operations such as JPEG compression, median filtering, Gaussian noise and geometrical operations such as cropping and scaling. The objective quality of the watermarked copy is about 35 dB with a detector response of about ten times the detection threshold. It is obvious that the watermarked copy is α_1^3 stinguishable from the original image. The values of the watermark strength factor are properly tuned so that the watermarking sequence is completely invisible, with detector response just above the detection threshold (detection strength of about $0.2Tw$).

In quantum watermarking scheme based on the relative frequency of error in observing qubits in a dissimilar basis. P has a message made of qubits or a classical message that she converts to qubits. After inserting the watermarking qubits, she can either observe the message immediately and only send the classical version out, or leave the message in qubit form and let Q observe the qubits. Note that the watermark is not actually created until observation, so it is probably best for P to only send out a pre-observed version of the watermarked message to avoid the averaging attack.

When P visits Q's website and finds a message M', that she believes to be a copy of M. Since she watermarked M before sending it to Q, she can detect if M' is her watermarked M by comparing the bits that result from observing ai' Є M'◦ j and ai Є M ◦ j, where i Є I. If the relative frequency of error between ai' and ai is very nearly the expected probability of error of reading a qubit as if it were written in basis j when it was actually written in basis k, the message M' is probably M watermarked by P. In the figure 7, P compares the two messages on the qubits in I and finds the relative frequency of error. In this case, there are 2 errors in 4 bits, for a relative frequency of 0.5. Since we can assume from Figure 6 that probability of error pe = 0.5, Q has verified that D is a watermarked A.

5. Conclusion

The watermarking embedding process embeds the data on selected groups of wavelet coefficients of the input image. Two groups of coefficients are formed after detecting the edges using a Sobel edge detector and a threshold value. Another group is formulated by a morphological dilation operation applied on the edge coefficients. The selected coefficients reside on the detail subbands and describe the edges of the image or the region around them. But the quantum watermarking scheme based on the relative frequency of error when observing qubits in a dissimilar basis. Quantum watermarking scheme is the new field of watermarking technique.

6. References

[1]. G Gordon Worley III," Quantum Watermarking by Frequency of Error when Observing Qubits in Dissimilar Bases", submitted to quant-ph/0401041v2,pp 1-2.

[2]. John N. Ellinas," A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection," pp. 291-296.

[3]. Yiwei Wang, John F. Doherty and Robert E. Van Dyck, "A Watermarking Algorithm for Fingerprinting Intelligence Images", 2001 Conference on Information Sciences and Systems, The Johns Hopkins University, March 21–23, 2001,pp.1-5.

[4]. Nedeljko Cvejic, "Algorithms for audio watermarking and steganography", OULU 2004, pp.1-112.