Digital Watermarking with Side Information

I.Al-Houshi and M.A.Ambroze

School of Computing, Communications and Electronics, University of Plymouth

Abstract

The intent of this research is to improve the efficiency of digital watermarking techniques through applying side information principles in them, and to build an application for digital watermarking trying to prove that side information techniques are sufficient (theoretically) to defeat the noise caused by cover objects, then to prove that result practically through experiments by applying image samples to the developed application, to increase the ability to detect the hidden messages.

Keywords

Digital Watermarking, Side Information, Cover Object, Encoding, Embedding, Detection, Informed, Blind, Orthogonal Keys, Effectiveness, Robustness, Fidelity.

1 Introduction and motivations

The increasing of interest in digital watermarking is most likely due to the increasing of concern and interest in copyright protection and content authentication, verification, and tracking. The growing of Internet and the increasing of its usability make it excellent system for distributing digital media; Internet system is inexpensive and instant method to support digital media access, on the other hand, the risk of piracy is increasing with the growing of internet services and systems. Cryptographic techniques and principles are very efficient method to maintain secure transmission in addition to provide security for distributed messages and media before the decryption step, thus it will be easy to illegally distribute digital media soon after decrypting it. This limitation of cryptography explains the strong need for an alternative solutions and techniques which can protect the contents even after decrypting them. Digital watermarking has the ability to maintain the security during normal usage, decryption, encryption, or even compression and file format changes due to the fact that digital watermarking techniques place information within the content of digital media, this information is dependent to the content and sometimes, its existence is hidden as well (Lu, 2005).

Watermarking is using general standards and principles of communication systems such as noise averaging, spread spectrum communications, in addition to message encoding and embedding. Most of these principles and techniques ignore the fact that the noise caused by the cover work is known to the sender/encoder (Petrovic *et al.*, 2004), so it is more efficient to exploit this information to defeat the noise caused by the cover work. Techniques and algorithms which neglect the information about the noise caused by the cover work decrease the effectiveness of watermarking (effectiveness is one of the main properties should be considered when designing

watermarking algorithms, and it is related to the probability of immediate detection after embedding step (Muharemagic *et al.*, 2001)). This project is to investigate the background of spread spectrum communication techniques to improve these techniques by designing a system able to use the knowledge and information obtained from the original cover work, this process called side information techniques (Ambroze, 2007).

This research starts from building theoretical background about the main digital watermarking techniques in addition to the properties of these techniques which should be considered in the assessment of digital watermarking applications, covering the weaknesses of assumptions leaded to the algorithms and techniques of simple digital watermarking, then presenting side information theoretical approaches and principles as a better solution to address and solve the problems related to the assumptions done in these techniques and algorithms; Most of these principles and techniques were gathered from latest resources and articles published in the field of digital watermarking in general and side information techniques in particular. The second step is to design and draw the road map of building the tools and resources for running the experiments; this includes choosing the framework of programming, explaining the flow charts of our algorithms and application. The follower part of this research is reviewing the findings and results obtained from applying the developed techniques, in addition to comparing the results obtained from simple watermarking techniques with the results obtained from side information techniques before and after applying some attacks to these techniques to check similarities and differences between theory and application. Finally, this research is going to result in many conclusions about the achieved points of this project, in addition to presenting some recommendations and assumptions for the proposed future work.

2 Theoretical analysis

This section is to start by discussing the spatial domain approaches which are the core and most important case in watermarking systems (since they are used in both spatial and frequency domain techniques), then it is to move to cover the frequency domain issues taking in consideration the benefits and results obtained from spatial domain discussion.

The first technique to present is Least Significant Bit (LSB) Technique, where the message bits are included directly to the cover object without serious modification, for example, it is easy to add one bit message to one byte cover object without significant modification, so, human eye will not be able to distinguish and notice the differences between the watermarked object and cover object itself (this preserves the fidelity property of watermarking, in addition to 100% of effectiveness), this technique is using side information principles as it applies the changes only to the least significant parts of the cover object. The problem in this technique is the fact that this technique is not capable to resist any type of attacks or noise (Petrovic *et al.*, 2004).

The second approach in spatial domain is based on correlation function and embedding weight principles (considering $\mathbf{c_0}$ as the cover object, $\mathbf{w_r}$ as watermarking

key, $\mathbf{w_m}$ as the encoded message pattern, $\boldsymbol{\alpha}$ as the weight of embedded pattern, $\mathbf{w_a}$ as the weighted embedded pattern). Using the latest considerations:

$$w_m = w_r \text{ if message} == 1 \text{ else } w_m = -w_r \quad \textbf{(1)}$$

$$w_a = \alpha . w_m \quad \textbf{(2)}$$

$$c_w = c_o + w_a \quad \textbf{(3)}$$

$\mathbf{c_w}$ is the watermarked object, in this approach, the weight of embedded pattern should be static, moreover, cover object is considered to have Gaussian distribution in the frequency domain so the correlation between watermarking key and cover object could be neglected (correlation function properties) so:

$$corr(c_w, w_r) = \sum(c_o . w_r) + \alpha . \sum(w_m . w_r) \approx \mp\alpha . \sum(w_r . w_r) \quad \textbf{(4)}$$

The previous formula shows that a decision of having hidden might be taken when having correlation value (between watermarked object and watermarking key) greater (in absolute value) than the size of watermarking key multiplied by the embedding weight. This is the core principles of first approach which neglects any information about cover object, this assumption led to lower effectiveness and fidelity values.

The third approach benefits from cover object information so no approximations were considered in formula (4), in this case, side information about the cover object is used to determine the value of adaptive embedding weight (Cox *et al.*, 2002):

$$\alpha = \frac{\tau - \sum(c_o . w_r)}{\sum(w_r . w_r)} \quad \textbf{(5)}$$

Where τ is the threshold or detection value (the decision of having hidden bits within the watermarked object is taken according this value). Adaptive embedding weight technique does not increase the ability of watermark to resist attacks and noise; on the other hand it increases the fidelity (SNR) of watermarked object in addition to having 100% effectiveness (Eggers *et al.*, 2002).

The other proposed solution in this research to increase the fidelity of watermarked object is to use orthogonal keys set, then to apply one key from this set according to its correlation value with the cover object (choosing the key which maintain the highest value to result in the minimum embedding weight). In this research, Hadamard orthogonal keys algorithm was applied to generate the needed orthogonal keys (Bella *et al.*, 2005).

All of previous techniques do not take in consideration the robustness/security property of watermarking, so moving to frequency domain is a better approach to solve noise/attacks problem due to the fact that most of attacks and noise types have special characteristics in frequency domain rather than spatial domain (DCT is one of frequency domain techniques). Applying spatial domain techniques to mid-

frequencies band samples limits the effect of high frequencies attack (such as edge removal attacks), and maintain the quality of watermarked object since this technique is not using low frequencies samples (human eye is sensitive to low frequencies changes) (Cummins *et al.*, 2004).

Finally, this research is to apply integrated solution benefits from all previous techniques and principles to prove that many improvements could be achieved in digital watermarking techniques by integrating one or more of digital watermarking techniques which are using side information.

3 Implementing the algorithms

Previously mentioned algorithms and techniques were implemented using MATLAB framework, gray scale images were considered as cover objects, where black/white images were considered as messages. The flowcharts of implemented algorithms are presented in this section as an explanation of the performed work. This research developed the code produced by (Shoemaker, 2002) to comply with the improvements of proposed approaches.

3.1 LSB

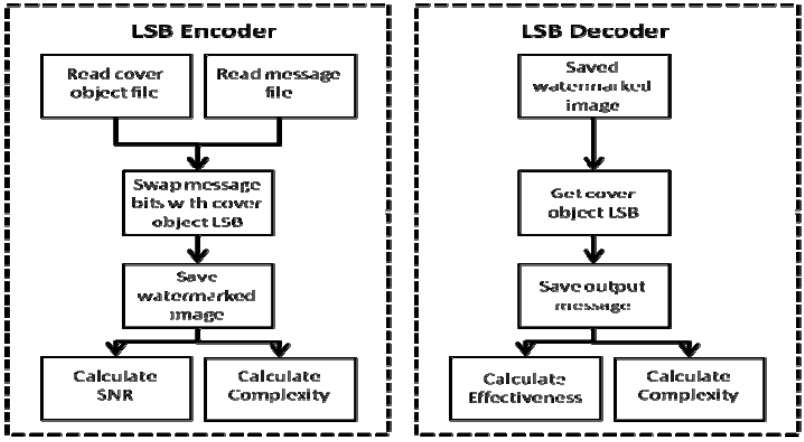

Figure 1: LSB technique flowchart (Sender/Receiver)

3.2 Static embedding weight

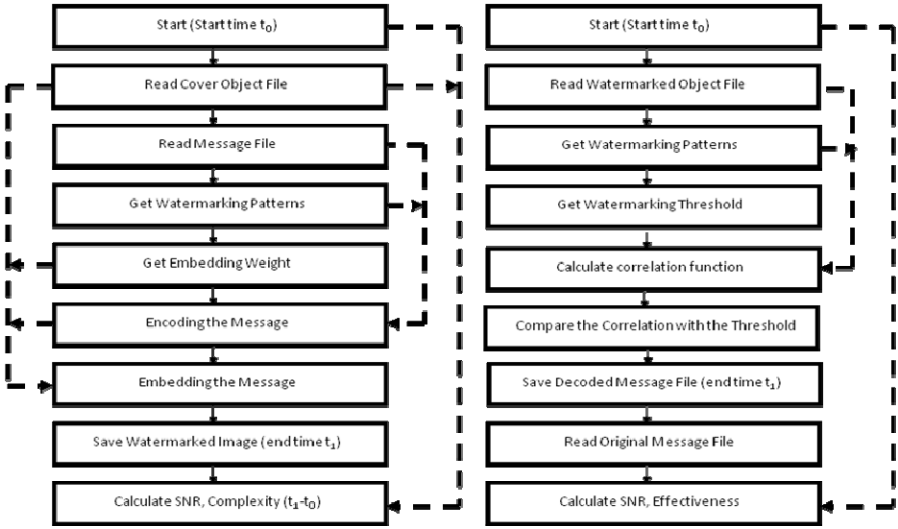

Figure 2: Static embedding weight technique (Sender/Receiver)

3.3 Hadamard orthogonal keys generator

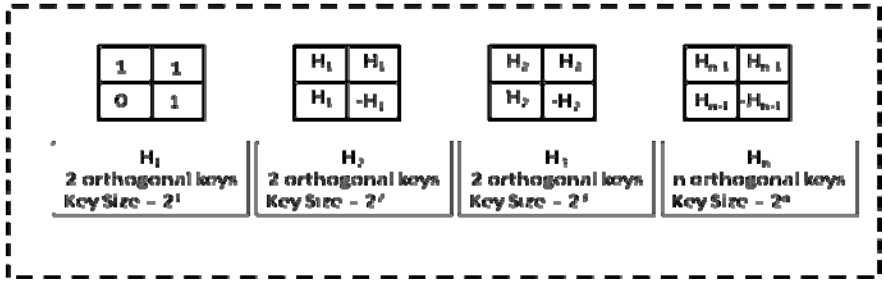

Figure 3: Hadamard orthogonal keys generator algorithm

3.4 Adaptive embedding weight

The flowchart of this technique is the same as static embedding weight technique, taking in consideration that embedding weight should be calculated according to the proposed threshold before embedding the message in the cover object.

3.5 DCT

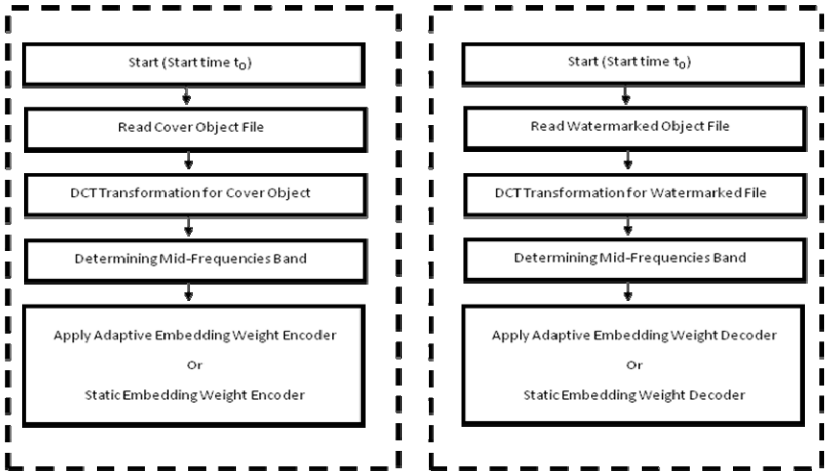

Figure 4: DCT technique (Sender/Receiver)

4 Experimental results and discussion

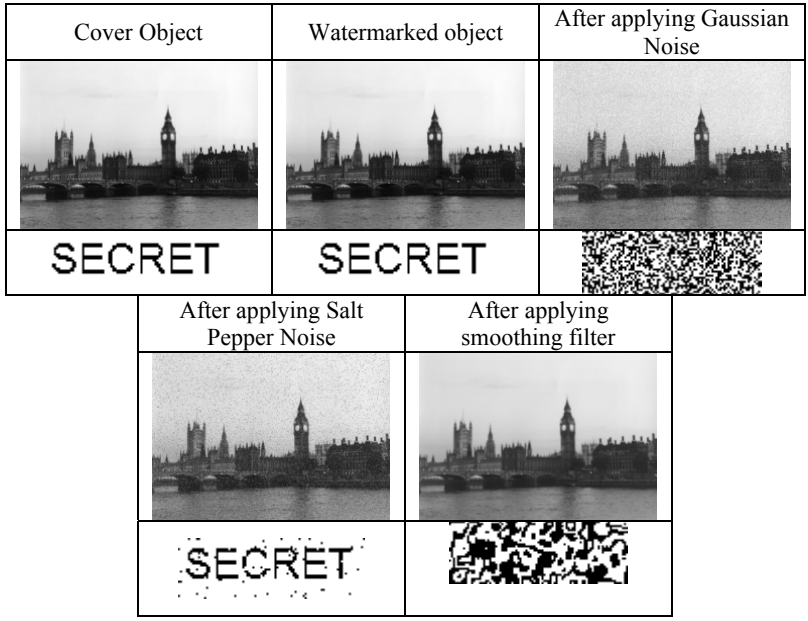

Figure 5: Example of applied LSB technique (Attacks/Noise)

The same samples were applied to all techniques in order to maintain the same conditions for all experiments. In these experiments cover object file was gray scale image (the size of cover object samples is 1600x1200 pixels), while the message file considered to be black and white image file (the size of message was 93x33 pixels where every pixel in these message is only 1 bit). As expected from the theoretical

part, applying LSB as digital watermarking technique was efficient according to the high values of fidelity (SNR~47.9 dB), effectiveness properties, while the probability of retrieving message bits after applying different types of attacks and noise was very low (53.5% when applying Gaussian noise, 49.5% when applying smoothing filter).

Static embedding weight is not better than LSB, since higher embedding weight maintains the effectiveness of watermarking while it decreases the fidelity of watermarked image, and lower embedding weight maintains the fidelity of watermarked image but it decreases the effectiveness of watermarking (when applying embedding weight=1, the results were SNR~44.9 dB, security~65.3% when applying Gaussian noise, and security~52.7% when applying smoothing filter)

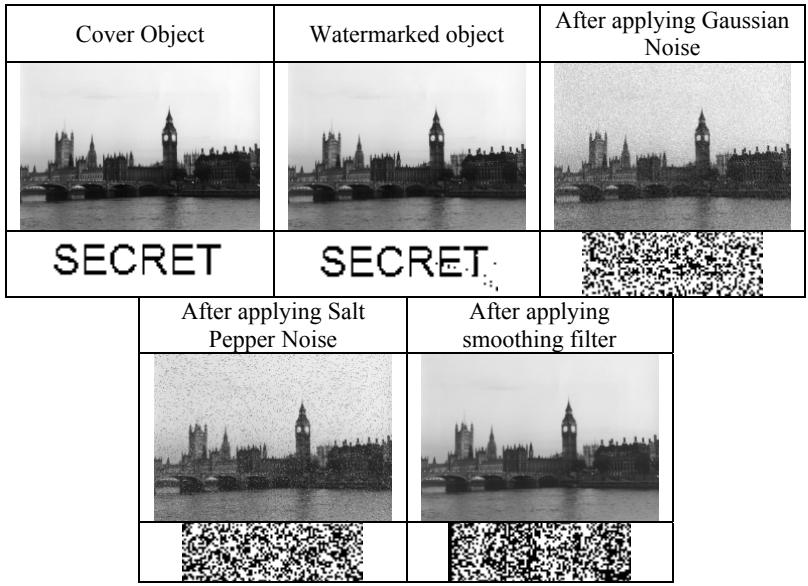

Figure 6: Example of applied static EWT (weight=1)

Adaptive embedding weight is a special case of static embedding weight technique, when the weight is adaptive to comply with the properties of cover object; adaptive EWT moves the samples of cover objects from the un-watermarked space to detectable watermarking space, to make sure that all watermarked samples can be detected (there are few errors related to the round-off and truncating errors). Adaptive EWT increases the value of effectiveness and security properties for the same signal to noise ratio or fidelity property value, this technique is making sure of applying static EWT in more efficient approach benefiting from the side information about the cover object (when applying threshold=0.1, the results were SNR~45 dB, security~79% when applying Gaussian noise, and security~61.8% when applying smoothing filter)

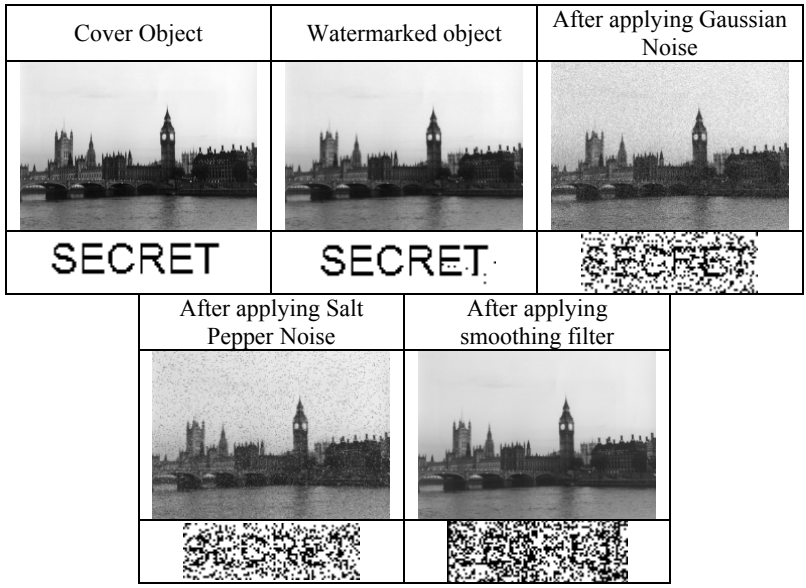

Figure 7: Example of applied Adaptive EWT (threshold=0.1)

DCT technique is using side information of cover object in frequency domains; by applying DCT in mid-frequencies band, high-frequencies band attacks will be defeated, in addition to increasing the fidelity of watermarked objects due to the fact that human eye is more sensitive to low frequency modifications. The results obtained from applying DCT using static EWT (embedding weight=1) were (SNR~56.3 dB, security~50.3% when applying Gaussian noise, and security~87.7% when applying smoothing filter).

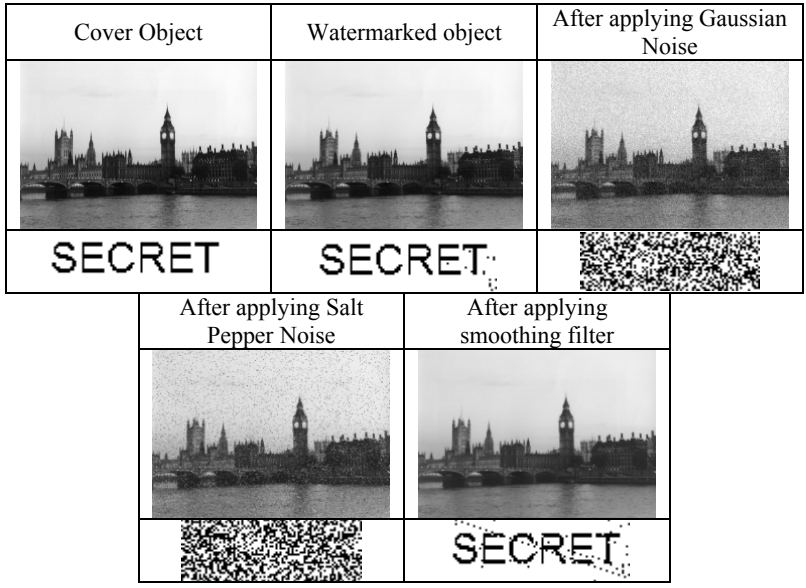

Figure 8: Example of applied DCT using SEWT (weight=1)

In the last experiment, DCT were applied using adaptive embedding weight technique (to increase effectiveness and fidelity) in addition to Hadamard orthogonal keys (to increase fidelity as well). The results obtained from this integrated technique was not surprising comparing them to theoretical principles which were applied in this integrated solution. This technique increases the fidelity and effectiveness (AEWT and Hadamard) and increases the security property value (DCT). For example, when applying this technique using 16 orthogonal keys and threshold=0.1 the results were (SNR~64 dB, security~80.1% when applying Gaussian noise, security~88.1% when applying smoothing filter, in addition to effectiveness~99.8%).

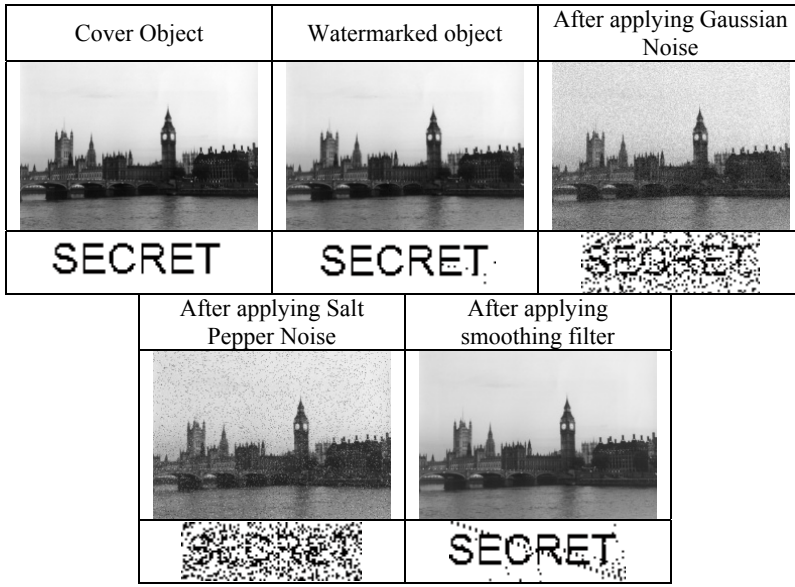

Figure 9: Example of applied DCT using AEWT and Hadamard (threshold=0.1)

5 Conclusion

Watermarking Technique	Pros	Cons
LSB	Simple, 100% effectiveness, reasonable fidelity (SNR)	Unable to resist noise and other types of attacks
Static EWT	Simple, more secure than LSB	Less than 100% effectiveness, fidelity is related to EW
Adaptive EWT (Side Information)	~100% effectiveness, reasonable fidelity, secure	More complicated than SEWT
Hadamard (Side Information)	Better fidelity, ~100% effectiveness	More complicated than SEWT
DCT (Side Information)	Better fidelity, high effectiveness, more secure	complicated
Integrated Technique (Side Information)	~100% effectiveness, higher fidelity value, as secure as DCT	The most complicated technique

Table 1: Pros and Cons of applied digital watermarking techniques

Using Side Information techniques is very efficient solution to benefit from the gathered information about the cover object. This is the best way to converse from the optimum principle proposed by (Costa, 1983) who made an assumption that blind detectors could perform as efficient as informed detectors. This project developed an integrated technique through maximizing digital watermarking properties to converse from the optimum solution, so, further improvements could be performed by applying further techniques and principles, and researches.

Table 1 shows the techniques implemented and tested in this research in addition to the pros and cons of each technique.

6 Future work

There are many points to be considered in future work, the first point is related to taking more properties in consideration when testing the performance of digital watermarking techniques (such as data payload property which is the size of message could be hidden in the cover object), the second point is applying other types of attacks to check the ability of watermarking techniques to resist them (such as synchronization attacks). The last point is to errors in retrieved message, further error analysis should be considered in addition to apply some types of error correction code to improve the security of digital watermarking.

7 References

Ambroze, M. A. (2007). Project Proposal for MSc Information Systems Security. University of Plymouth.

Bella, T.; Olshevsky, V.; Sakhnovich, L. (2005). Equivalence of Hadamard matrices and Pseudo-Noise Matrices. New York: IEEE Publications.

Costa, M. (1983). Writing on Dirty Paper. IEEE Transactions on Information Theory (pp. 439-441). New York, USA: IEEE.

Edin Muharemagic, B. F. (2001). Multimedia Security: Watermarking Techniques. Florida, USA: Florida Atlantic University.

Ingemar J. Cox, M. L. (2002). Digital Watermarking. London, UK: Morgan Kaufmann.

Joachim J. and Eggers, R. B. (2002). DigitalWatermarking facing Attacks by Amplitude Scaling and Additive White Noise. ITG Conference on Source and Channel Coding. Berlin, Germany: ITG Conference on Source and Channel Coding.

Jonathan Cummins, P. D. (2004). STeganography and Digital Watermarking. Arizona, USA: Arizona State University.

Lu, C.-S. (2005). Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property. London, UK: IDEA Group Inc.

Rade Petrovic, B. T. (2004). Digital Watermarking Security Considerations. San Diego, USA: The University of San Diego.

Shoemaker, C. (2002). Hidden Bits: A Survey of Techniques for Digital Watermarking. Independent Study.