Robust Digital Watermarking of Multimedia Objects

by

Gaurav Gupta,

Dissertation
Presented to
Department of Computing,
Macquarie University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Macquarie University

August 2008
Robust Digital Watermarking of Multimedia Objects

Committee:

Professor Josef Pieprzyk, Supervisor

Dr Hua Xiong Wang, Co-Supervisor
Contents

List of Tables v
List of Figures vii
List of Algorithms ix
Acknowledgments xiii
Abstract xv
Statement of Candidate xix
List of Publications xxi
Notations Used xxiii

Chapter 1 Introduction 1
1.1 Digital Watermarking ................................................. 1
1.2 Digital Fingerprinting .............................................. 3
1.3 Motivation .......................................................... 3
1.4 Contributions ..................................................... 4

Chapter 2 Background 7
2.1 Fundamental Mathematics ........................................... 7
2.2 Statistics ........................................................... 9
2.3 Cryptography ...................................................... 11
2.4 Hash Functions .................................................... 15
2.5 Natural Language Documents ..................................... 16
2.6 Software .......................................................... 21
## Contents

2.7 Databases ................................................................. 25

### Chapter 3  Overview of watermarking  27
3.1 Approaches to Watermarking ........................................ 30
3.2 Text and Natural Language Watermarking ..................... 32
3.3 Software Watermarking ............................................... 39
3.4 Database Watermarking ............................................... 56
3.5 Conclusion .............................................................. 73

### Chapter 4  Natural Language Watermarking  74
4.1 Current Scenario ...................................................... 75
4.2 Outline of Proposed Scheme ........................................ 76
4.3 Proposed Scheme .................................................... 78
4.4 Analysis ............................................................... 86
4.5 Experimental Results ............................................... 88
4.6 Conclusion ............................................................ 89

### Chapter 5  Software Watermarking  91
5.1 Description of Myles and Jun Watermarking Scheme .......... 94
5.2 Proposed Attack ..................................................... 97
5.3 Implementation Details and Results .............................. 100
5.4 Surviving the Debugging Attack .................................. 103
5.5 Analysis .............................................................. 106
5.6 Conclusion ............................................................ 106

### Chapter 6  Semi-blind and Reversible Database Watermarking  109
6.1 Introduction ........................................................... 109
6.2 Related Work and Agrawal-Kiernan Scheme .................... 110
6.3 Analysis of Agrawal-Kiernan Watermarking Scheme .......... 113
6.4 Modified Algorithms ............................................... 116
6.5 Analysis .............................................................. 117
6.6 Conclusion ............................................................ 124

### Chapter 7  Blind and Reversible Database Watermarking  125
7.1 Introduction ........................................................... 125
7.2 Model of Adversary .................................................. 129
7.3 Proposed Scheme ..................................................... 130
## Contents

7.4 Experimental Results ........................................ 131
7.5 Analysis ....................................................... 135
7.6 Conclusion ..................................................... 138

**Chapter 8 Conclusion and future research** 139

8.1 Thesis Summary ............................................... 139
8.2 Future Research Directions ................................. 142

**Bibliography** .................................................. 144

**Vita** ............................................................ 154
List of Tables

3.1 Comparative study of text watermarking schemes .................................. 40
3.2 Comparative study of software watermarking schemes .......................... 55
3.3 Meal table .................................................................................. 58
3.4 Combination table ........................................................................ 59
3.5 Version 1 of combination table ....................................................... 60
3.6 Version 2 of combination table ....................................................... 60
3.7 Original Table ............................................................................. 62
3.8 Watermarked with bit 1 ................................................................... 62
3.9 Watermarked with bit 0 ................................................................... 63
3.10 Foreign exchange rates ................................................................. 68
3.11 Foreign exchange rates (watermarked) ............................................ 68
3.12 Table with modified primary key ..................................................... 69
3.13 Table with binary representation of numerical values ....................... 71
3.14 Watermarked table with binary representation of numerical values .... 71
3.15 Owner identification possibilities ..................................................... 72
4.1 Natural language and text watermarking methods ............................... 76
4.2 Pseudo-randomization of watermarking sequence ............................. 80
4.3 Comparison of empirical results with theoretical values ....................... 81
4.4 Illustration of majority voting .......................................................... 86
4.5 Text modification with increasing watermark size ............................. 89
4.6 Text amplification with increasing watermark size ............................. 89
6.1 Original foreign exchange rates relation ........................................... 114
6.2 Watermarked foreign exchange rates relation .................................... 114
6.3 Probability of success for bit flipping attack ...................................... 119
List of Tables

6.4 Detecting watermarks in multi-party environment . . . . . . . . . . . . . . 121
List of Figures

3.1 Bishop’s crosier (Australia), 16th century 28
3.2 Watermarks in Australian currency bill 28
3.3 Watermarks in German currency bill 29
3.4 Watermark in Spanish document from 17th century 29
3.5 Magnified view of watermark from Figure 3.4 30
3.6 Inserting intermediate code without effecting output 42
3.7 $61 \times 73 = 3.6^4 + 2.6^3 + 3.6^2 + 4.6^1 + 1.6^0$ in Radix-6 encoding [29] 45
3.8 Planted Planar Cubic Tree [29] 45
3.9 Watermarks 010 and 111 resulting in the same watermarked graph 50
3.10 Launching an attack on second-LSB based watermarking 64
4.1 Generating a paragraph permutation using AES 79
4.2 Keys required to get a valid permutation using AES-128 82
5.1 Branch function modifying return addresses 93
5.2 Function set $F$ invoked using secret input parameter $key_{AM}$ 96
5.3 Fingerprint branch function modifies the return address itself 107
5.4 Calling instruction modifies address using key returned by fingerprint branch function 107
6.1 Owner identification 122
6.2 Multiple watermarking scenario - dotted lines denote distortion and solid lines denote watermarking 122
7.1 Effect of changing fraction of tuples marked on detection 134
7.2 Effect of changing percentage of marks that need to be detected to establish watermark presence 134
7.3 Effect of changing attack levels on detection . . . . . . . . . . . . . . 135
List of Algorithms

1. Euclid’s algorithm .................................................. 8
2. Euclid’s extended algorithm ..................................... 8
3. RSA key generation ................................................ 13
4. RSA encryption .................................................... 13
5. RSA decryption ..................................................... 13
6. RSA digital signature generation [68] ......................... 15
7. RSA digital signature verification [68] ......................... 15
8. Watermark insertion changing inter-word spacing ........... 34
11. QP watermark insertion [75, 76] ............................... 48
12. QP watermark extraction [75, 76] ............................. 49
13. QPS watermark insertion [70] ................................. 51
14. QPS watermark extraction [70] ............................... 52
15. Watermark insertion in numeric set ........................... 58
16. Uniform distribution attack ..................................... 64
19. Sentence sequence generation ................................. 80
20. Natural language watermark insertion ....................... 85
23. Reversible and semi-blind watermark insertion ............... 117
24. Reversible and semi-blind watermark detection ............. 118
25. Semi-blind owner identification ............................... 119
26. Reversible and blind watermark insertion ................... 132
List of Algorithms

27  Reversible and blind watermark detection .......................... 133
28  Blind owner identification .............................................. 137
To Gunjan for all her love and support. And my parents and Tina for being the wonderful people they are
In our life, we come across many people who inspire and motivate us, who help us become a better person and a better professional. I would like to take this opportunity to thank them for all they have done for me.

Firstly, I thank Josef for his tremendous support, not only for my research, but also for my academic and teaching interests. Thanks to Huaxiong as well for providing excellent guidance in the brief absence of my main supervisor. I appreciate the assistance provided by Daniel, Saurabh, Krystian, Vijaykrishnan, and Simon during various stages of my research. I thank Mohan for introducing me to the interesting topic of digital watermarking during my master’s degree and taking the time to supervise me for my master’s dissertation. I would also like to thank all my friends who have made a positive difference in my life - Gunjan, Ravi, Maya, Anjali, Jagrat, Colwin, Gautam, Urvi, Mohit, Reema, Meeta, Teju, Eric, Raghu, Radhika, Daniel, Menno, and Tanja. I thank Gunjan’s parents, Shekhar and Shobha, for their belief as well.

Thanks to Prof. Banerjee for bringing out the best in me during my undergraduate. He is the best teacher I have ever had and a huge inspiration for me. Very special thanks to Michelle for taking the time to read my thesis and giving her valuable feedback, it is really appreciated.

Most importantly, I thank my parents and my sister for being so kind, loving, and nurturing, despite the brat that I was. They always showed confidence in me and support and appreciated me for what I am.
I also want to acknowledge my late friend, Ashish, one of the nicest guy I have ever met, one who was the best at everything he did (and made us jealous in the process). I know he is in a better place; may his soul rest in peace.

The last part is the trickiest one; I want to acknowledge Gunjan’s support during all the seven years that we’ve been together and four years that we have been married (not that I am keeping a count!), but at the same time thanking her for all she has done makes her indirect contributions towards this thesis look so petty. I would just like to take a moment to appreciate how she appreciated my work, instilled confidence in me and applauded every little success I had in my research as if I had won an Olympic medal. So, far all that, and more, I love you Gunjan.
Robust Digital Watermarking of Multimedia Objects

Gaurav Gupta
Macquarie University, 2008

Supervisor: Professor Josef Pieprzyk

Digital watermarking has generated significant research and commercial interest in the past decade. The primary factors contributing to this surge are widespread use of the Internet with improved bandwidth and speed, regional copyright loopholes in terms of legislation; and seamless distribution of multimedia content due to peer-to-peer file-sharing applications.

Digital watermarking addresses the issue of establishing ownership over multimedia content through embedding a watermark inside the object. Ideally, this watermark should be detectable and/or extractable, survive attacks such as digital reproduction and content-specific manipulations such as re-sizing in the case of images, and be invisible to the end-user so that the quality of the content is not
Abstract
degraded significantly. During detection or extraction, the only requirements should be the secret key and the watermarked multimedia object, and not the original unmarked object or the watermark inserted. Watermarking scheme that facilitate this requirement are categorized as blind. In recent times, reversibility of watermark has also become an important criterion. This is due to the fact that reversible watermarking schemes can provided security against secondary watermarking attacks by using backtracking algorithms to identify the rightful owner. A watermarking scheme is said to be reversible if the original unmarked object can be regenerated from the watermarked copy and the secret key.

This research covers three multimedia content types: natural language documents, software, and databases; and discusses the current watermarking scenario, challenges, and our contribution to the field. We have designed and implemented a natural language watermarking scheme that uses the redundancies in natural languages. As a result, it is robust against general attacks against text watermarks. It offers additional strength to the scheme by localizing the attack to the modified section and using error correction codes to detect the watermark. Our first contribution in software watermarking is identification and exploitation of weaknesses in branch-based software watermarking scheme proposed in [71] and the software watermarking algorithm we present is an improvised version of the existing watermarking schemes from [71]. Our scheme survives automated debugging attacks against which the current schemes are vulnerable, and is also secure against other software-specific attacks. We have proposed two database watermarking schemes that are both reversible and therefore resilient against secondary watermarking attacks. The first of these database watermarking schemes is semi-blind and requires the bits modified during the insertion algorithm to detect the watermark. The second scheme is an upgraded version that is blind and therefore does not require anything except a secret key and the watermarked relation. The watermark has a 89% probability of survival even when almost half of the data is manipulated. The
Abstract

Watermarked data in this case is extremely useful from the users’ perspective, since query results are preserved (i.e., the watermarked data gives the same results for a query as the unmarked data).

The watermarking models we have proposed provide greater security against sophisticated attacks in different domains while providing sufficient watermark-carrying capacity at the same time. The false-positives are extremely low in all the models, thereby making accidental detection of watermark in a random object almost negligible. Reversibility has been facilitated in the later watermarking algorithms and is a solution to the secondary watermarking attacks. We shall address reversibility as a key issue in our future research, along with robustness, low false-positives and high capacity.
I certify that the work in this thesis entitled “Robust Digital Watermarking of Multimedia Objects” has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree to any other university or institution other than Macquarie University.

I also certify that the thesis is an original piece of research and it has been written by me. Any help and assistance that I have received in my research work and the preparation of the thesis itself have been appropriately acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature:

Gaurav Gupta - 40478890

Sydney, 08-August-2008
List of Publications


6. Gaurav Gupta and Josef Pieprzyk. Source Code Watermarking Based on
Notations Used

1. \{a_1, \ldots, a_n\}: set of \( n \) elements.
2. \( \mathcal{H}(x) \): hash of \( x \).
3. \( R \): relation
4. \( r \): tuple
5. \( A_i \): \( i^{th} \) attribute
6. \( r.A_i \): \( i^{th} \) attribute in tuple \( r \)
7. \( A^j_i \): \( j^{th} \) LSB of \( i^{th} \) attribute where LSB stands for least significant bit
8. \( r.A^j_i \): \( j^{th} \) LSB of \( i^{th} \) attribute in tuple \( r \)
9. \( r.P \): primary key of tuple \( r \)
10. \( \| \): concatenation
11. \( \mathcal{H}(\cdot) \): one-way hash function
12. \( R \xrightarrow{\text{inst}(p)} R_w \): relation \( R_w \) is the result of party \( p \) inserting its watermark in relation \( R \),
13. \( R_w \xrightarrow{\text{det}(p)} R \): original relation \( R \) is restored by the party \( p \) from the watermarked relation \( R_w \)
14. \( |x| \): size of \( x \) in bits
15. $\text{abs}(x)$: absolute value of $x$

16. $\lfloor x \rfloor$: greatest integer smaller than $x$ (floor function)

17. $\lceil x \rceil$: smallest integer greater than $x$ (ceiling function)

18. Distance for attribute $r.A_i$: $\delta_{r.A_i} = \min_{\tilde{r} \neq r} \{\text{abs}(r.A_i - \tilde{r}.A_i)\}$