

ICC AB

博碩文化



資訊媒體安全

偽裝學與數位浮水印



王旭正、柯建萱

ICCL資訊密碼暨建構實驗室 著

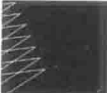
資訊媒體安全

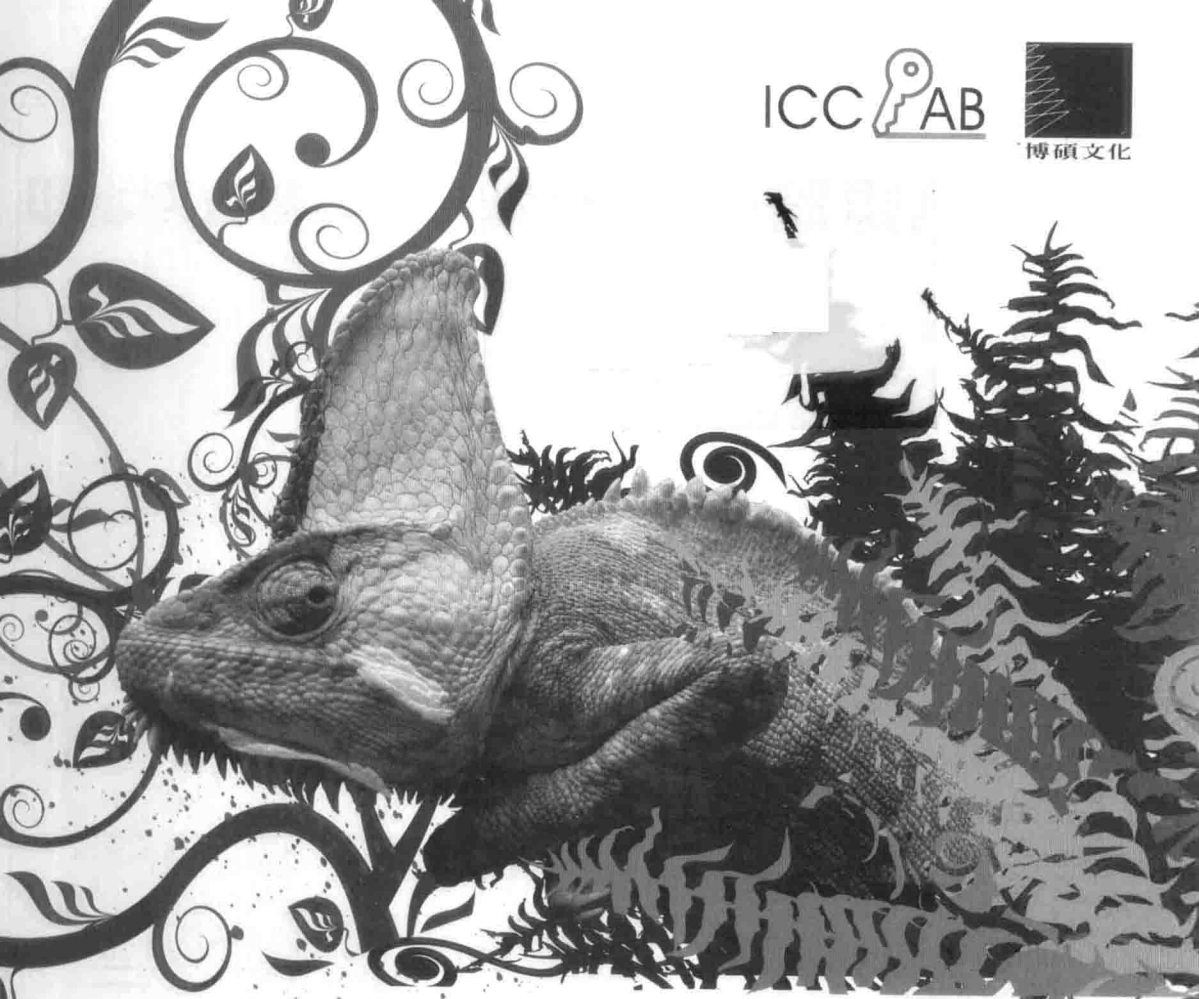
偽裝學霸數位浮水印



CC BY-NC-SA
此作品係根據 CC BY-NC-SA 授權

ICC  AB


博碩文化



資訊媒體安全

偽裝學與數位浮水印



王旭正、柯建萱

ICCL資訊密碼暨建構實驗室 著

資訊媒體安全—偽裝學與數位浮水印

作者：王旭正、柯建瑩、ICCL 資訊密碼暨建構實驗室

發行人：林麗芬

出版：博碩文化股份有限公司

台北縣汐止市新台五路一段 112 號 10 樓 A 棟

TEL：(02)2696-2869 · FAX：(02)2696-2867

郵撥帳號：17484299

律師顧問：劉陽明

出版日期：西元 2007 年八月初版

ISBN-13：978-986-201-021-1

博碩書號：CNE0006

建議售價 NT \$560 元

資訊媒體安全：偽裝學與數位浮水印 / 王旭正、
柯建瑩、ICCL 資訊密碼暨建構實驗室作。-- 初
版。-- 臺北縣汐止市：博碩文化，2007[民96]
面：公分
ISBN 978-986-201-021-1 (平裝)
1. 資訊安全 2. 電腦犯罪 3. 證據(法律)
312.976 96011602

本書如有破損或裝訂錯誤，請寄回本公司更換

Printed in Taiwan

著作權聲明

本書著作權為王旭正、柯建瑩、ICCL 資訊密碼暨建構實驗室所有，並受國際著作權法保護，未經授權任意拷貝、引用、翻印，均屬違法。

商標聲明

本書中所引用之商標、產品名稱分屬各公司所有，本書引用純屬介紹之用，並無任何侵害之意。

有限擔保責任聲明

雖然作者與出版社已全力編輯與製作本書，唯不擔保本書及其所附媒體無任何瑕疵；亦不為使用本書而引起之衍生利益損失或意外損毀之損失擔保責任。即使本公司先前已被告知前述損毀之發生。本公司依本書所負之責任，僅限於台端對本書所付之實際價款。

作者序

本書《資訊媒體安全—偽裝學與數位浮水印》(*Information Multimedia Security: Steganography and Watermarking*)為資訊安全的多媒體應用安全。本書的資料並非僅自於近代的高科技資訊產物，而是傳承自我們前輩在生活／工作／情感所醞釀／融合下所呈現的科學與智慧精華。事實上，古往今來有許多的創作者將偽裝技巧運用在與文辭字意與視覺感官中。這些運用包括利用文字隱藏玄機或者圖像感官變化，讓人得費心思解出答案。多媒體的資訊安全，在學術研究上通稱為「資訊隱藏」(Information Hiding)此種形式與文字的資訊安全最大的差別在於前者的“Seeing the Unseen”與“Seeing Is Not Believing”。這是種有趣的形容，也充滿著想像的情境。對於如此神秘又富有色彩的一門舊瓶新裝的科學，既維持文明的氣息又增添科技新貴的氣派，怎能不令人砰然心動呢！進而欲在此領域中放手一博。在創作者勾畫出一個美麗世界後，所有人皆因此沈浸這樣的如詩夢幻般的想像世界，背後的神秘，卻依然泰然完好，毫無洩漏的隱憂。她的魅力，是否您亦感受到了呢？是的，這就是這本書的來由，引領您一窺其中的奧妙。神秘面紗的揭開，不是僅爲了想探索裡面的真相；更重要的是，該如何讓她的色彩與美在適當的時候能帶來更具保障的資訊安全效果。這樣的消長，當然也成就她在科學研究者心中的地位，並在近年來的網路多媒體世界裡所予以高度重視與追求了。

承襲ICCL (Information Crypto & Construction Lab.)的傳統，所有的努力皆來自一個計畫的策動者與實踐／貫徹目標的工作者，這即是一個前瞻

性的系統／組織發展的模式。過程裡許多的人員該是感謝，然太多無法全數入鏡，太少地僅用「謝天」(God Knows It)兩個中文字或者「愛大家」(Love Each Other)三個中文字也著實無法表達真實的感動。就以柯宏叡、林建一、林宜萱的「柯建萱」在本書封面頁的編撰來表達對這些代表ICCL成員的努力下的「謝天」與「愛大家」。藉此永刻留在書名上，而不只是內頁裡一般的文字而已。

本書《資訊媒體安全—偽裝學與數位浮水印》的技術可以視為是數位時代的奇門遁甲。網路際網路發展時至今日，人類許多的智慧與智識不斷的累積，從傳統的文書保存至今日數位格式的儲存。訊息傳達的方式也從面對面的溝通，變成了面對螢幕的視訊會議。數位資訊快速累積，訊息被竊取／聽的風險也快速提高。這樣情況也就使得資訊媒體安全的需求令人不得不正視之。

資訊媒體安全的領域廣大，在本書的撰寫中，Semester Fall in 2006，我開課於研究所課程中所使用的兩本用書：Information Hiding: Steganography and Watermarking-Attacks and Countermeasures (Authored by N.F. Johnson, Z. Duric, and S. Jajodia)與Information Techniques for Steganography and Digital Watermarking (Authored by S. Katzenbeisser and F.A.P. Pertitcolas)，在與修習研究生們的討論與報告中給了ICCL諸多的靈感，再匯整ICCL這些年研發能量的期刊論文/研究資料終得此書的主要資料參考來源之一。正應驗學術研究／討論無古今／無國界／無前後／無止

作者序

境的金玉良言，盡在「虛」、「痴」與「心」。我從課程中的個人研讀、教學與學生的互動，教學相長，收穫著實匪淺。此時亦想到Aug. 2006到韓國的研討會參訪行程中於國立濟州大學Campus看到的標語「學而不疑知快活」、「免教虛作百年人」，似乎可為此種學習心作最貼切的詮釋。

本書著重於「偽裝學」、「視覺系統安全」、「數位浮水印」與「資訊隱藏應用於數位鑑識」的議題，主要是近年來國際上對於智財權在數位網路世界上屢屢受到侵害及網路秘密訊息傳遞的議題受到大家的矚目。本書藉由介紹傳統文字與藝術訊息隱藏的概念引入四大主軸：偽裝學、視覺系統安全、浮水印技術、與資訊隱藏應用於數位鑑識。藉此迎合國際資訊科技發展在資訊媒體安全的趨勢。

沒有一群專業工作者，當然也就成就不了一個既定目標的工程。從心得交換／討論中，我將我的 ICCL 研究人員分成三個研究層次，分別為基礎研究 (Fundamental Study)、主要研究 (Major Study) 與卓越研究 (Power Study)。這些成員提供了我諸多的資安／數理邏輯思考的研究空間想像。這群研究人員包括了過去式下雖已單飛但仍念念不忘的「老鳥」(Senior Guys)，現在式下正要畢業的「菜鳥」(Junior Guys)，未來式裡準備嗷嗷待哺／魔鬼訓練的「新鮮人」(Fresh Members)。所有的 ICCL Members 皆為 Lab 的永續經營盡最大的努力並留下難以抹滅的「菜鳥」回憶。

努力的背後，Family絕對是最重要的支柱，In Particular for Rebecca/G.Y./G.R.，my wife, my kids, my loves with them。最後吾人以經常對ICCL/

生活的期許(禪語)與讀者分享，並盼此書得以為科技發展／研究之文獻做粗淺整理，以為此相關領域的參酌。

「學習 as well as 忘」

「研究 as well as 痴」

「做事 as well as 心」

「生活 as well as 混」

「情感 as well as 容」

「成就 as well as 慟」



ICCL@B

ICCL-資訊密碼暨建構實驗室

<http://hera.im.cpu.edu.tw>

<http://163.25.10.166>

王旭正

Late Jan. 2007

Visit at Carnegie Mellon University (CMU)

Pittsburgh, Pennsylvania, USA

Preface

The present book on Information Multimedia Security- Steganography and Watermarking discusses the security of multimedia applications in information security. The data in the present book is derived not only from high technology information assets in the present era, but is also drawn from the scientific and intellectual essence manifested from the growth and fusion of the life, work and emotions of our predecessors. In reality, there have been many authors over the passage of history who have used steganography techniques with regards to the meaning of words and the “look and feel”. These applications include the concealment of words and the alteration of the “look and feel” of an image, such that it would take a considerable amount of effort to solve the puzzle. The information security related to multimedia has been referred to as “Information Hiding” within the field of academic research. The main difference between this form of expression

and the information security relating to text (studied in cryptography) is that the former involves “Seeing the Unseen” while the latter involves “Seeing Is Not Believing”. This is an interesting way of putting it, and it is also full of imagination. With regards to such a mysterious and interesting science that has manifested the repackaging of an old concept, which not only preserves the cultural distinctive but also adds on the valuable notions of science and technology, it is easy for a person to be fascinated with the topic. It is hoped that an attempt can be made to make inroads in this field, and to outline the beautiful world of the authors. Everyone is therefore immersed in this dream-like world of imagination, with the desire to see the concealed secret remain intact and complete, without any fear of being divulged. Can you feel its charm? This is truly the original motivation for this book, to guide you into the secrets that lie within the art. In unveiling the mask that covers up the mystery, it is not only

about exploring the truth that lies within, but more importantly, it is also about enabling its color and beauty to achieve higher levels of information security at the same time. Such development has naturally established the position of the present field in the eyes of academic researchers, and in recent years it has also been a hot topic of interest in the online multimedia industry.

Following the perspective culture of ICCL (Information Crypto & Construction Lab.), all the efforts come from a systematic plan for the project and workers that executes the plans and sets goals to be achieved. It is a farsighted system and model of organizational development. Many people need to be thanked in this entire process. There are too many people to be listed here, and simply using “God knows it” or “Love each other” would be insufficient to express the full extent of the appreciations. It therefore remains to list out the “K-J-S” from H.J. KE, J.Y. LIN,

and I.S. LIN on the cover page of the book to express the idea of “God knows it” and “Love each other” towards the hard work of the ICCL staff. This would always be deeply ingrained in the title of the book, and not just a matter of the general words found within the internal pages of the book.

The present book on Information Multimedia Security- Steganography and Watermarking can be considered as an invaluable guide to protection in the present digital age. Over the course of the development of the internet, the accumulation of the knowledge and wisdom of humanity has moved from the traditional documentary form of storage to the present digital formats of storage. The transmission of information has also shifted from a face-to-face communication to face-to-screen online video conferences. With the rapid accumulation of digital information, the risk of such information being stolen or

Preface

eavesdropped upon is also increasing rapidly. Such a scenario has made it inevitable that people would pay attention to information multimedia security.

The realm of Information Multimedia Security is extensive, while the present book has focused on the topics of “Steganography”, “Visual Security”, “Digital Watermarking” and “Applications of Information Hiding in Digital Forensics”, mainly because of the increased attention in recent years towards the successive instances of intellectual property right infringements on the internet and the transmission of confidential information over the internet. The present book explores four major areas through introducing the concept of information hiding in traditional writings and art: Steganography, Visual Security, Watermarking Technology, and Applications of Information Hiding in Digital Forensics. Through the aforesaid, it is hoped to be able

to move along with the trends in information multimedia security in the development of information technology in the international arena.

This book is akin to a progress plan for an engineering project. A completed plan/project results not from a single mind but from a group of specialized workers, and all the colleagues from ICCL, young and old, worked together to complete this work. This book belongs to all of those hard workers. From discussions and exchange of ideas, I divided my researchers in my ICCL into three research levels: Fundamental Study, Major Study, and Power Study. These groups provided me with many research ideas regarding information security and mathematical and logical deliberation. The researchers included the Senior Guys, past graduates who left but never forgotten; the Junior Guys, current students preparing to graduate; and Fresh Members, future graduates ready to learn and

train. All ICCL members worked hard on the continual operation of the lab and were left with unforgettable memories.

Family is absolutely the most important pillar of support behind hard work, in particular Rebecca, G.Y., G.R., my wife, and my children – my love is with all of them. Finally, I would like to share with readers my expectations of ICCL/Life. I hope this book can be used as a preliminary attempt for the literature of technology development/research, and a reference for related fields.

“Think why you are here”

“Find where you are interested in here”

“Marry whom you look for here”

“Get what you want to have here”

“Honor here when you own something special with knowledge”



ICCL –Information Cryptology and
Construction Lab.

<http://hera.im.cpu.edu.tw>

<http://163.25.10.166>

A handwritten signature in black ink, appearing to read 'Shiuh-Jeng Wang'.

Shiuh-Jeng Wang




~窺探數位媒體世界的奇門盾甲~

緣起

《資訊媒體安全—偽裝學與數位浮水印》的緣起各有其歷史背景與意義。偽裝學發展的歷史意義代表著古人的智慧，透過生活中簡單的事物去傳達更深一層的意義而不被發現為其精髓。而數位浮水印的技術則是傳統智慧創作躍上網路平台後，創作者權利的申張。20世紀末的電腦革命帶給人類生活莫大的便利，不變的是秘密通訊的基本人權，這象徵著偽裝學同樣有其存在於數位世界的必要性；至於人類智慧不斷的創新、發明，從原本的生活的巧思到電腦世界的數位音樂及軟體創作，則給了數位浮水印存在的意義。

網際網路的興起拉近了人與人之間訊息溝通的距離。以時間成本的角度而言，往昔寄出一封情書到情人手中至少花費數日光陰，而今日透過電子郵件在短短幾秒鐘內，一封封的郵件已經自動的送達收件人手中。在目前的網路通訊架構上，透過各式各樣的訊息交換軟體(如電子郵件、論壇、即時通訊等)，好朋友間無時無刻都進行著訊息的傳送與接收。對於有心保護通訊內容的人們除了利用加密軟體或機制，應用不同的偽裝技術亦為現代秘密通訊一時之選。

而在P2P技術帶動下，網路社群(論壇)等如雨後春筍的不斷成立，不幸卻導致今日侵害智慧財產權的猖獗，創作人的智財權保護每況愈下；非法的創作音樂分享、電影、應用軟體幾乎在網路上四處流竄。眾所皆知，水可載亦可覆舟。資訊科技的趨勢使得網路的四通八達，帶來便利，但也造成今日新興的犯罪型態及被害權益。如何保護秘密通訊的自由以及建立數位智慧產權的保護傘，正可謂「障眼法」的偽裝學及現代浮水印技術最有存在價值的意義與目




的。在這樣的需求下，此本書的來由亦因應而生。本書著重於「偽裝學」、「視覺系統安全」、「數位浮水印」與「資訊隱藏應用於數位鑑識」的議題，主要是藉由對於偽裝學、視覺系統安全、浮水印技術、與資訊隱藏應用於數位鑑識的認識，才能建立數位世界的新秩序，也能讓你我的通訊能更有機密，而智慧的創作更受保護。

架構

本書共有12章。第一章裡藉由文字與藝術的另類解讀開始對於偽裝學發展的歷史背景做介紹，透過簡單的中西文學及藝術在偽裝學領域的歷史，引領大家進入資訊隱藏的世界，給讀者引入中古世紀至近代世界各國偽裝技術實際發生的範例串連出偽裝學的歷史。而第二章的現代偽裝學的發展則介紹現代偽裝學基本原理及分類，並進一步對數位影像上進行資料隱藏的方法與技術的比較，提供大家對於現代偽裝學的技術有基本的認識；接著第三章探討偽裝學在進入數位時代後出現的技術與研究並操作現代偽裝技術發展出來的偽裝工具；第四章，我們進一步探討在偽裝學領域的主流—視覺密碼學，介紹視覺密碼的源起及基礎、黑白、彩色視覺密碼學的原理；第五章深入瞭解視覺密碼在資訊隱藏及身份認證領域之應用。

針對「浮水印技術」在本部份中我們規劃了數位浮水印的研究發展，由第六章介紹浮水印系統的基礎概念、特徵及相關研究的分類(Categories)。第七章探討數位浮水印系統的評估工具(Evaluation Tools)及瞭解各種影像處理的攻擊方式；接著第八章介紹將浮水印系統結合到網路系統後，應用於版權保護的相關問題；第九章則介紹視覺密碼在浮水印領域之應用，嘗試運用視覺安全來提升浮水印之竄改偵測與所有權鑑別的效果。




本書後半階段以「資訊隱藏應用於數位鑑識」為核心，探討新興的網路犯罪在偽裝學及浮水印保護版權的技術下與數位鑑識的相關議題。首先第十章先就對數位證物與數位鑑識作基本的解說，資訊媒體安全搭配數位鑑識技術，將成為多媒體犯罪的預防赫嚇阻效果；接著第十一章探討偽裝學在數位鑑識之應用，在數位鑑識工作中，偽裝與浮水印技術所扮演的角色。最後在第十二章探討數位媒體(如照片)在浮水印機制下的數位證據能力問題及其他相關議題，希冀能建立完善的證據管理及保護機制，對於在電腦／網路犯罪的案件調查具有關鍵性地位，可成為法官採信的依據並影響審理的結果。



對象

對於本書的編排，適合大專／科技技術學院／大學與一般大學的理工科系／研究所的學生教材上課使用。在偽裝學與數位浮水印的技術研究領域裡，已累積了前人的智慧，正所謂「前人種樹，後人乘涼」，在法制社會的今日，我們宜善加應用以保護人們的權益並求更進一步的創新！



Early Feb. 2007
ICCL-資訊密碼暨建構實驗室
Information Cryptology and Construction Lab.
<http://hera.im.cpu.edu.tw>, <http://163.25.10.166>

目錄

01 文學與藝術的世界

- 1.1 何謂資訊隱藏與偽裝學 2
- 1.2 西方世界的偽裝史 4
- 1.3 中國文學的隱藏藝術 7
- 1.4 影像的資訊隱藏藝術—另類視覺欺騙 18
- 1.5 結語 20

02 現代偽裝學的發展

- 2.1 偽裝系統的分類與原則 26
- 2.2 數位影像的資料型態 35
- 2.3 資訊隱藏的原則 40
- 2.4 偽裝分析的技術介紹 44
- 2.5 結語 56

03 偽裝學工具應用

- 3.1 傳統的偽裝工具 60
- 3.2 偽裝技術的工具 73
- 3.3 抵抗攻擊的分析與討論 79
- 3.4 結語 81

04 視覺安全的原理與基礎

- 4.1 視覺安全簡介 84
- 4.2 視覺安全演算法 111
- 4.3 視覺安全之像素擴張 118

目錄

4.4	視覺安全之欺騙與預防	129
4.5	結語	132
05	視覺安全應用	
5.1	身份認證	136
5.2	資訊隱藏與秘密分享機制	146
5.3	視覺安全與基因演算法	166
5.4	視覺安全與自然圖片	174
5.5	結語	180
06	數位浮水印概論	
6.1	數位浮水印的概念	185
6.2	數位浮水印的特性	187
6.3	數位浮水印的分類	200
6.4	JPEG影像壓縮技術	207
6.5	結語	217
07	浮水印的評估工具及影像攻擊	
7.1	浮水印技術的評估標準	220
7.2	浮水印的影像攻擊方式	224
7.3	自動化的攻擊工具	235
7.4	浮水印的強韌性實驗	237
7.5	結語	250