資訊媒體安全- 偽裝學與數位浮水印

Information Multimedia Security

---Steganography and Watermarking---

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，不是僅為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盾甲。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/無止境的金玉良言，盡在「痴」、「心」與「虛」。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相關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)與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：

「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」。

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。

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

Jan. 2007

Information Multimedia Security

---- Steganography and Watermarking----

FORWORDS

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 yes 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. **K**E, 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 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:

*"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".*

I hope this book can be used as a preliminary attempt for the literature of technology development/research, and a reference for related fields.

(ICCL –Information Cryptology and Construction Lab.)
http://hera.im.cpu.edu.tw
http://163.25.10.166

Shiuh-Jeng Wang
Late Jan. 2007
Visit at CMU, Pittsburgh
Pennsylvania, USA