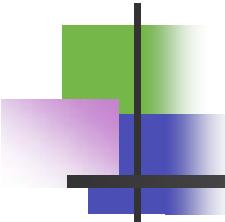


Computer Forensics with Steganography in Evidence Investigations



DOP Shiu-Jeng WANG / 王旭正

- 
- 中央警察大學 資訊管理系
 - 中華民國資訊安全學會 (www.ccisa.org.tw, 理事 (2000-2012)
 - 中華民國資訊安全學會 副理事長 (www.ccisa.org.tw, 2012-)
 - Visiting Scholars at FSU and UF in USA, 2002, 2004, 2010.
 - Academic tour for International Project Inspection at CMU in USA, 2007
 - Columnists of Domestic Information-tech Magazines, <http://www.netadmin.com.tw/>
網路通訊/iThome/網管人雜誌, 2002-2006, 2007-至今
 - Director of ICCL, <http://hera.im.cpu.edu.tw>
(Information Cryptology and Construction Lab.)
 - sjwang@mail.cpu.edu.tw, <http://www.wretch.cc/blog/icclsjwang>

Outline

- Security
- Steganography
- ICCL-FROG
- Forensics and Evidence
- Research works
- --- **Forensics in Steganography Evidence Investigations**
- Conclusions



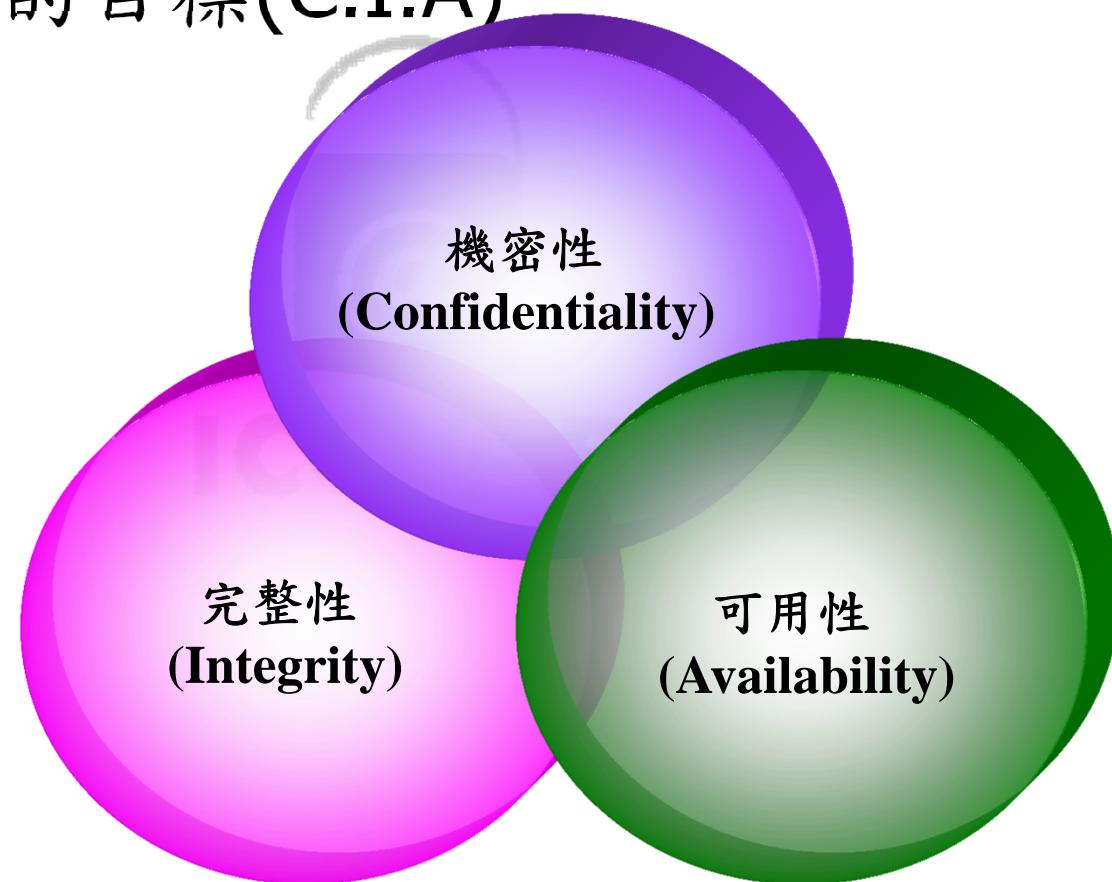
ICCL@B

C'est La Via

- HAKUNA MATATA
- Information/Network Security
- Authentication and Forensics
- Computer/Network Forensics

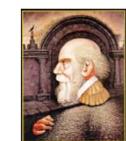
C.I.A.

■ 資訊安全的目標(C.I.A)

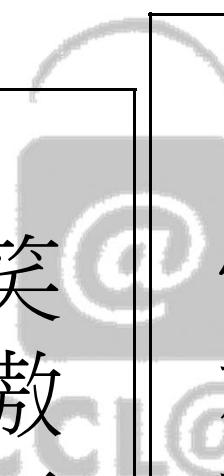




大自然中 瞒天過海的偽裝術



偽裝法



捨身比武搏妹笑
縱是孤苦一生傲
學琴定情濱於江
曲諧常笑傲江湖

性狂難羈武通神
亦師亦友身旁鶻
棄私斬奸人稱俠
情堅逾石得仙侶

偽裝法

- 拆字詩是利用漢字的特點，將字拆開後寫成的詩句，要得到隱藏的訊息，就必須仔細體會，將詩詞中的漢字組合起來，才能得到所要表達的意旨。

鵝飛鳥去永不回，
良字去頭雙人陪，
雙木非林心相隨，
您若無心各自飛。

偽裝法

- 拆字詩是利用漢字的特點，將字拆開後寫成的詩句，要得到隱藏的訊息，就必須仔細體會，將詩詞中的漢字組合起來，才能得到所要表達的意旨。

鵝飛鳥去永不回，
良字去頭雙人陪，
雙木非林心相隨，
您若無心各自飛。

語譯：我很想你

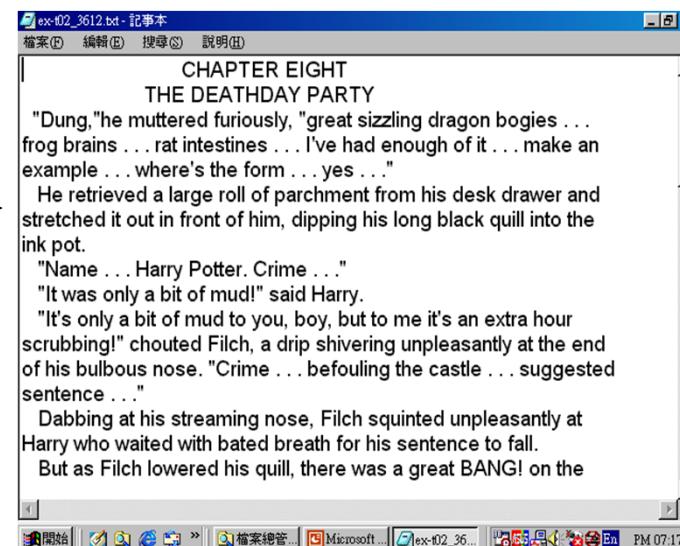
資料嵌入



掩護圖
(秘密隱藏
前)

掩護圖 / 偽裝圖 (128x128pixel)

嵌入小說 「哈利波特(Harry Potter)」
部分的內涵

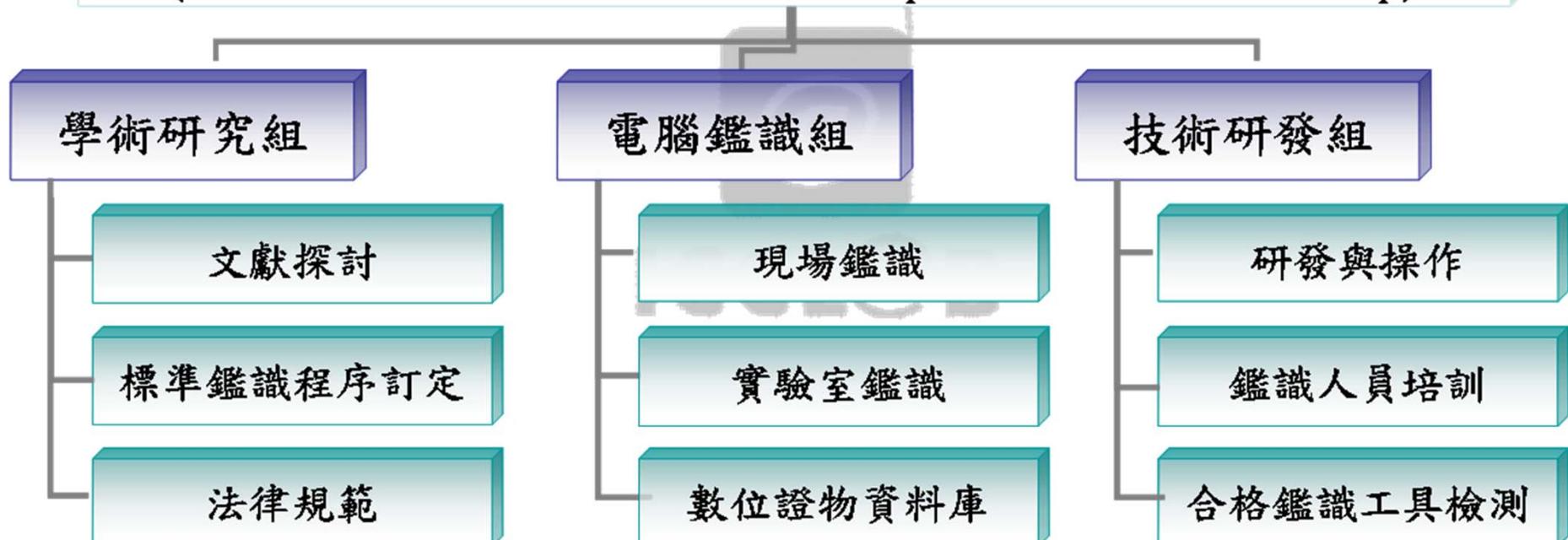


偽裝圖
(秘密隱藏後)

MY FROG and the FROG with you

ICCL數位鑑識實驗室FROG

(ICCL-Forensic Research & Development Task Force Group)



Cyber Crime

- 電腦犯罪日漸嚴重(調查報告)
 - 調查報告美國在西元兩千年因電腦犯罪所產生的財產損失即增加43%，由 \$US265 million 增加為 \$US378 million (FBI案件統計)
 - 美國85% 的企業及政府機構曾偵測到計算機系統遭到入侵
- 資料來源:<http://www.smh.com.au/icon/0105/02/news4.html>.

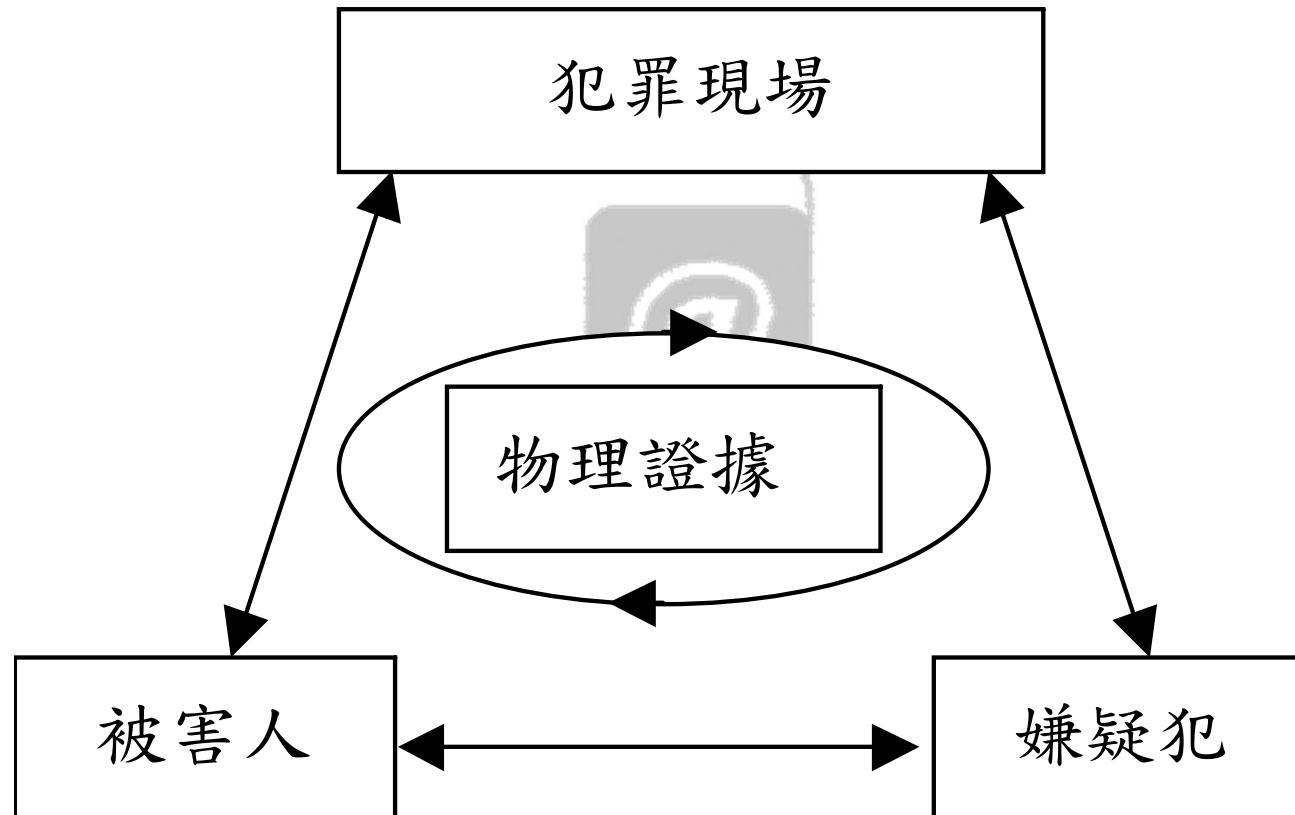
鑑識科學(Forensic Science)

■ 定義

- 運用科學於執法
- 科學：化學，生物學，物理學，地理學，...
- 目標：確定犯罪現場及相關證物之證據能力



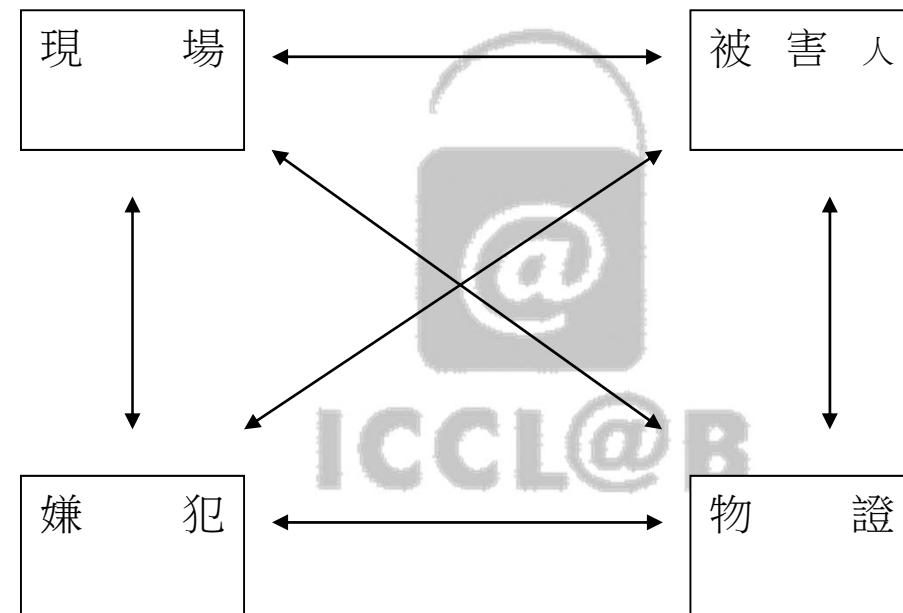
鑑識科學 (Locard's Exchange Principle)



Implications

- 多方面偵查，**勿勿下結論**：除數位證據之外，仍需訪問受害人、目擊證人、以及檢視相關之**物理證據**。
- 探討**犯罪者之行為特質**，可據以作為推論犯罪模式
 - 犯罪地點及型態
 - 接近及控制被害者之方式
 - 犯罪者之作為、不作為、及反應。
- 探討**被害者之特質**
ICCL@B
 - 可藉以了解犯罪者，及其與被害者之關係。
 - 網路跡證與被害者之關係。
 - 可藉以推測受害者之類型並提出警告。
 - 犯罪者之**冒險因素**及被害者之**危險因素**。

犯罪現場的立即偵查



四相面間連接方式基本原則

Computer Forensics

(Warren, G. Kruse ii and Jay G. Heiser, 2002, *Computer Forensics – Incident Response Essentials*, Addison Wesley)

■ 定義：

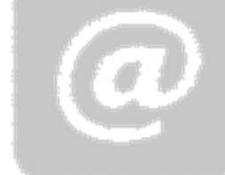
- 以周延的方法及程序**保存, 識別, 抽取, 記載, 及解讀**電腦媒體證據與分析其成因之科學

■ 方法與基本原則：

- 在不改變或破壞證物的情況下**取得原始證物**
- **證明**所抽取的證物來自扣押的證物
- 在不改變證物的情況下**進行分析**

證物之抽取

- 從電腦系統抽取證物
 - 是否即刻關機或斷絕網路連線需視情況而定
 - 從運行中的系統抽取證物
- 證物處理:
 - 證物鏈之管理
 - 採證
 - 證物之識別
 - 證物之運輸
 - 證物之保存
 - 偵查活動之記載



ICCL@B

證物之分析

- 將原證物完整拷貝兩份
 - 包含正常檔案, 刪除檔案, 及硬碟之其他部分
- 重複鑑定證物



ICCL@B

Example to digital information

- 通連紀錄
- 交易紀錄(如提款、購物、轉帳等等)
- 電子郵件備份
- 網路連線紀錄
- BBS 備份
- 機密文件



ICCL@B

數位證物鑑識之目的

- 確認嫌犯
- 起訴犯罪者
- 保護無辜
- 了解犯罪行為與動機



數位證據與物理證據之比較

- 為物理證據之一種
- 易於複製與修改
- 不易證實其來源及完整性
- 無法直接被人類所感知、理解的內容



ICCL@B

數位證據與犯罪重建

- 重建被刪除、破壞、隱藏或加密之資料。
 - 利用特殊工具。
 - 利用公用程式。
 - 破解密碼(猜解密碼)。
- 推論犯罪事實 (5W1H)
 - 何事(What)
 - 何人(Who)
 - 何時(When)
 - 何地(Where)
 - 如何(How)
 - 為何(Why)



ICCL@B

檔案系統證物之蒐集

- 正常檔案：搜尋，文件分析，…
- 加密檔案：密碼分析與破解，…
- 已刪除檔案
- 剩餘空間(slack space)之資料



ICCL@B

討論

- 數位證據的偵防所必須遵循的**程序與原則**，為因應泛網路犯罪的行為亦不斷的提出。
- 現行刑法中有明訂規範的賭博、詐欺等泛網路犯罪，司法與執法機關在追查泛網路犯罪行為上，已開始利用**新興工具對數位證據**進行分析
- 利用六何(**5W1H**)要件作為分析條件，以求獲取相關電腦網路證據，並以發生案例作說明，希冀能對未來的數位證據蒐證工作有所助益。
- 法律並非打擊犯罪的唯一手段，**正確的網路倫理及使用方式**才是**抗泛網路犯罪**的重要概觀。

- Security
- Steganography
- ICCL-FROG
- Forensics and Evidence
- Research works
- **--- Forensics in Steganography Evidence Investigations**
- Conclusions



ICCL@B

Research works

- 相關研究背景
- 證據管理鏈完整性保護系統
 - 疊合性資訊嵌入機制研究
- 結論



Integrity Evidence for Chain of Custody in Signature Payload Embedding Systems

- 數位資料能很快地透過資訊系統有效管理並經由網路快速交換，而數位相片也不例外。當多數人擁有同一份數位相片時，為了證明誰才擁有數位相片的所有權，通常所有權人會在公開數位相片之前先在相片中加入能證明自己身份的標籤、符號或文字，以宣告相片的版權所有。

簡介(續)

- 簽章機制所代表的意義為所有權的宣示與得具不可竄改性。在數位媒體的簽章機制一般以浮水印的嵌入與鑑定加以實現。數位浮水印的設計依使用的需求可分為強韌性(Robust)浮水印、脆弱性(Fragile)浮水印及半脆弱性(Semi-fragile)浮水印。

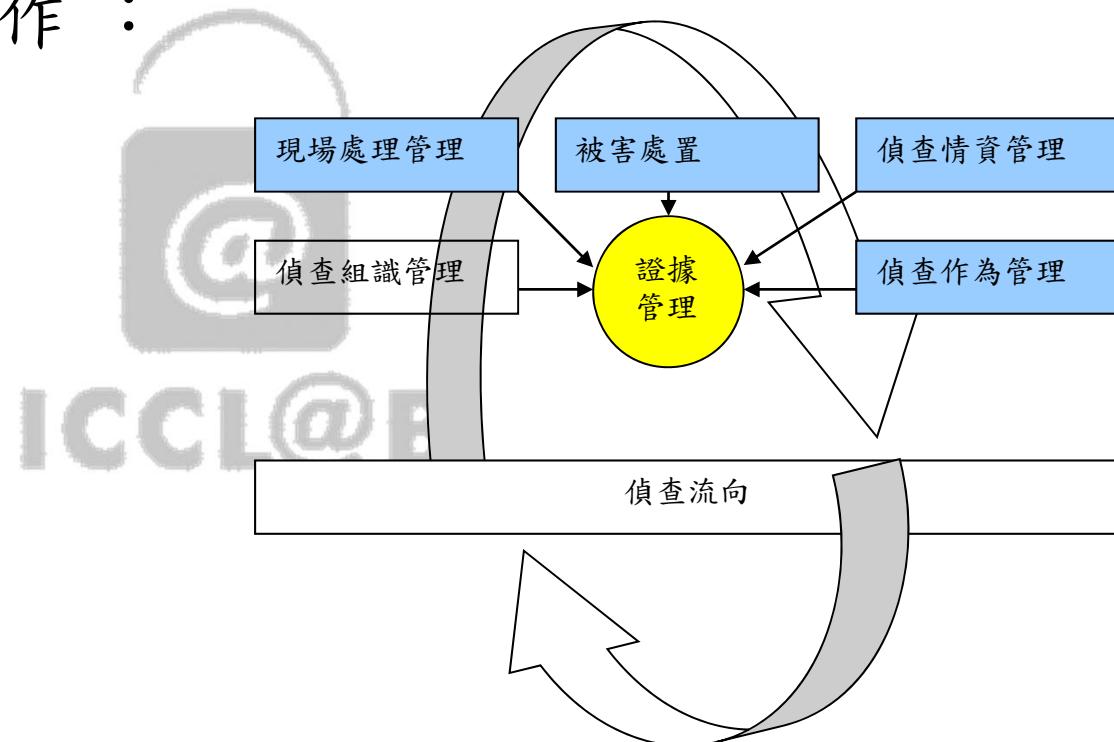
簡介(續)

- 證據(數位證據)在證據管理裡具有兩項特質
 - 一者為偵查工作上可能影響案件偵辦方向
 - 一者則是作為呈予法庭供法官審定並具案件關連的說服能力
- 不論蒐集到的數位證據定位為何，其**完整性**皆須受到**保護**。

簡介(續)

犯罪偵查的四項工作：

- 現場處理管理、
- 被害處置、
- 偵查情資管理、
- 偵查作為管理



簡介(續)

- 對於各類案件自始至終貫穿全案則是「**證物管理**」，也因此顯示出衍生所需的數位證據蒐集與鑑識在證據管理的重要性
- 證據管理鏈：證物鏈承辦人員所有權的順序如下：
現場採證人員→證據管理人員→偵查人員(或專案小組)→鑑識人員→偵查人員(或專案小組)→檢察官→法官。
- 證據管理鏈的重點
 - 證據與擁有者的關係
 - 證據本身的完整關係

簡介(續)

- 一個具有完整性的證據管理鏈，除了證物本身的物理性質不被破壞外，從證據的產生到法庭上其與各個擁有者間應具有連續不間斷的支配關係。



ICCL@B

相關的研究背景

■ 影像在數位證據管理鏈的證據完整性

- 刑事偵查上有所謂的「毒樹毒果實理論」，其意指非法律程序「毒樹」取得的證據「毒果實」是不能做為證據的。然而從另一個角度而言，當證據管理過程當中出現瑕疵時，也就是毒樹的一個型態。
- 數位證據管理鏈的關係起自數位證據在被搜索、扣押、保管、鑑識，最後到了法庭上為法官審理案件的重要證據關連依據。
- 「證據能力」是指具有可以成為證據資料的資格
- 「證明力」則是證據能夠證明事實的程度
- 若證據已非有毒的果實，但其色、香、味條件程度能否形成法官強大的心證，則可稱為證據力。

相關的研究背景（續）

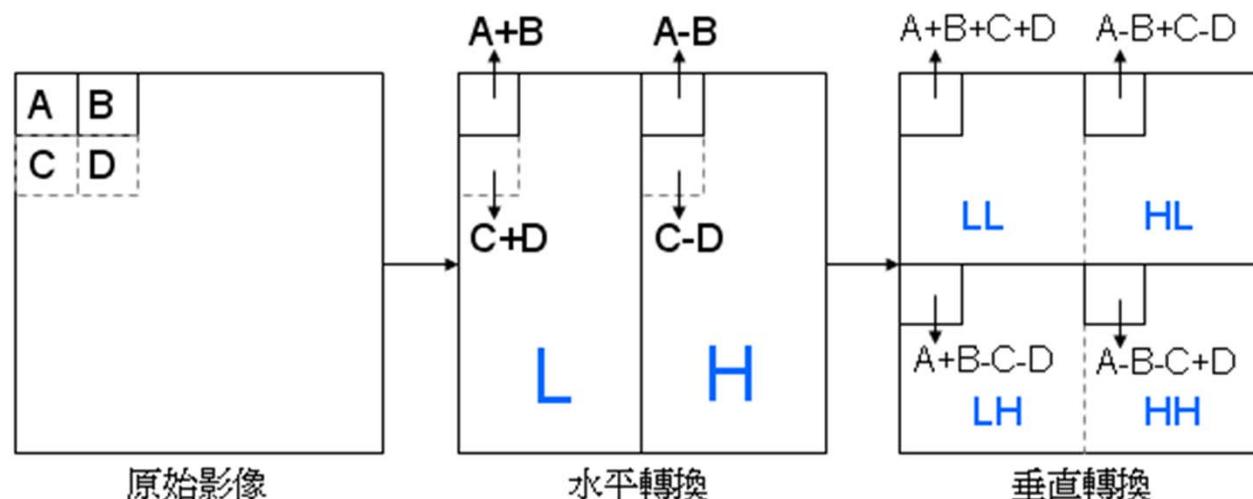
- 本研究為疊合性資訊嵌入系統，並以Wang-Yang-Scheme，與KH -Scheme 的研究背景進行數位媒體在證據管理鏈的完整性研究。



ICCL@B

離散小波轉換

- 在離散小波轉換的領域裡有不同的濾波用來將空間域的訊號轉換成為頻率域的訊號，包括有 Haar Wavelet、Daubechies 與 Gaussian 等
- 下圖為 Haar 離散小波轉換範例：



Wang-Yang-Scheme

- Wang-Yang-Scheme是以區塊特徵為主，透過模數運算的特性，將浮水印位元嵌入並萃取，是屬於盲(blind)的強韌型浮水印。
- 嵌入/萃取資訊的量化方式如下表所示：

浮水印位元	原始像素值	修改後像素值
$W(i)=0$	$b(x,y) \geq 0$	$b(x,y)' = b(x,y) + \Delta_0$
	$b(x,y) < 0$	$b(x,y)' = b(x,y) - \Delta_0$
$W(i)=1$	$b(x,y) \geq 0$	$b(x,y)' = b(x,y) + \Delta_1$
	$b(x,y) < 0$	$b(x,y)' = b(x,y) - \Delta_1$

區塊餘數	萃取浮水印位元 $W(i)$
$R' \geq \lfloor T/2 \rfloor$	1
$R' < \lfloor T/2 \rfloor$	0

KH Scheme

- 一種以離散小波轉換為基礎的浮水印鑑定機制，藉由所取出的浮水印可以檢驗影像所有權，並且具有偵測影像竄改位置的功能，稱之為 KH-Scheme，可以用來嵌入脆弱型的浮水印。
- 嵌入資訊的量化方式如下所示：
 - $Q(C_i) = \lfloor C_i/d \rfloor \bmod 2$, $d = \delta \times 2^L$
 - $Q(\cdot)$: 量化函數
 - C_i : 像素值
 - d : 強度參數
- 下表為 $d=2$ ($\delta=1$ 、 $L=1$)，值從 -2 到 6 之量化表

C_i	-2	-1	0	1	2	3	4	5	6
$Q(C_i)$	1	1	0	0	1	1	0	0	1

證據管理鏈完整性保護系統

■ 疊合性資訊嵌入機制研究

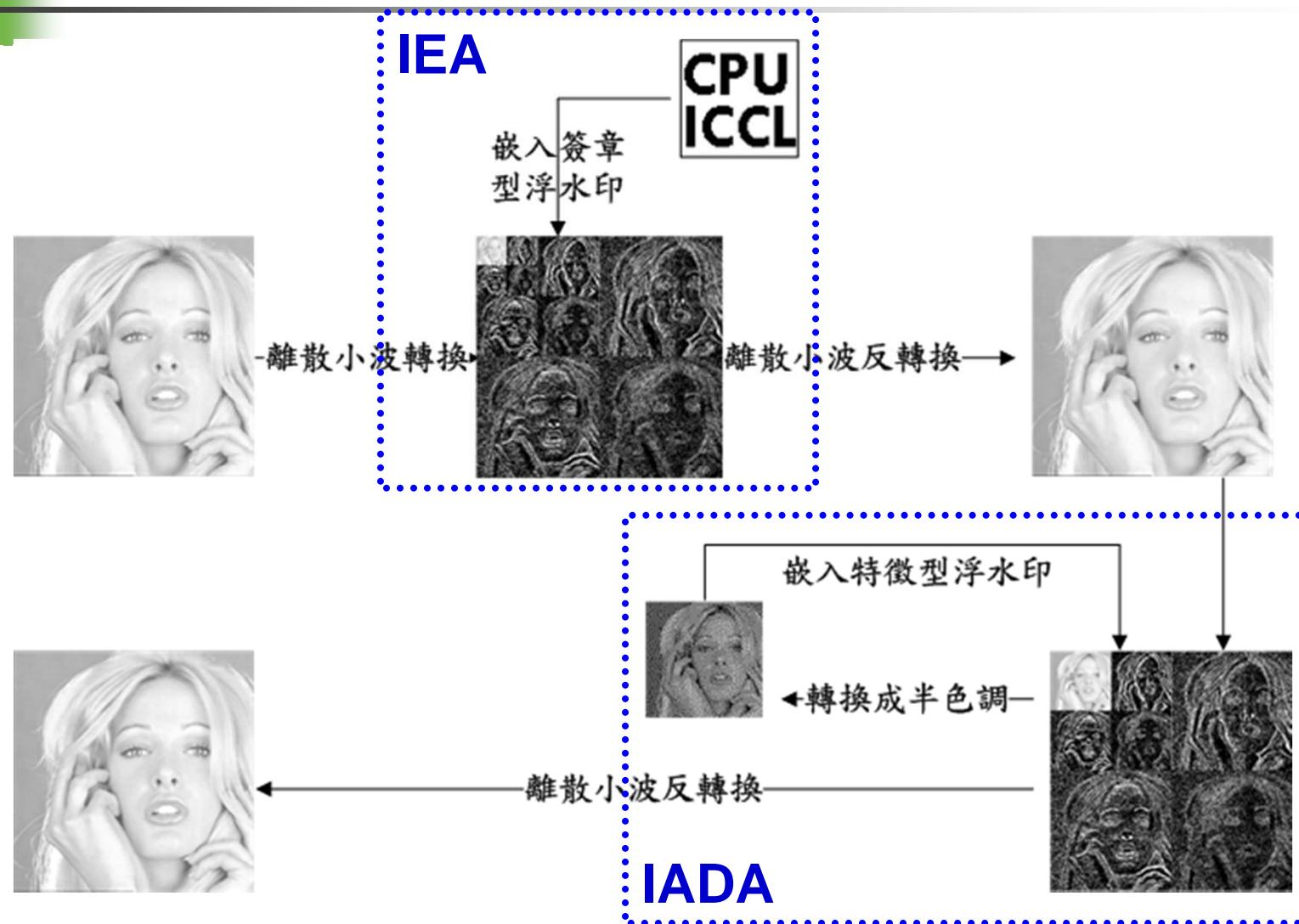
- 證據管理除了須要證據本身的物理性質的完整性外，更須完善保護在案件搜索、偵查、移送等過程中，**相關承辦人的簽章與證物結內含特徵資訊的不可竄改性**。
- 對於**證物鏈**承辦人員所有權的順序如下：現場採證人員→證據管理人員→偵查人員(或專案小組)→鑑識人員→偵查人員(或專案小組)→檢察官→法官。

疊合性資訊鑑定與偵測機制(續)



- 疊合性資訊嵌入系統以Wang-Yang-Scheme與KH-Scheme為基礎並以證據管理鏈的簽章鑑定與竄改偵測為訴求，提出嵌入保護資訊以達到二項保護需求的演算法：
- 資訊嵌入演算法(Information Embedding Algorithm，*IEA*)
- 資訊鑑定與偵測演算法(Information Authentication and Detection Algorithm，*IADA*)。

疊合性資訊鑑定與偵測機制



討論與分析

- 評估工具：PSNR、NC
- 實驗母圖 512×512 、簽章型浮水印 64×64 、特徵型浮水印 128×128
- 嵌入結果如下

母圖	Baboon	Airplane
PSNR	42.304	42.063

母圖	Baboon		Airplane	
	NC1	NC2	NC1	NC2
25%切割攻擊	0.7452	0.7695	0.7445	0.7503
50%切割攻擊	0.5038	0.5027	0.5005	0.4948
像素值隨機修改	0.9943	0.9950	0.9932	0.9947

實驗結果

攻擊型態	簽章型浮水印鑑定	特徵型浮水印鑑定 (差異度比較結果)
25%切割		
50%柵欄式切割		
像素隨機修改		

結論

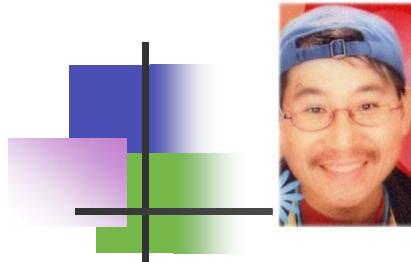
- 完善的證據管理及**保護機制**，對於在電腦/
網路犯罪的案件調查具有關鍵性地位，可成
為法官採信的依據並影響審理的結果。因此
，建立受信任的**證據管理鏈**，將提高數位證
據在法庭上被採信的程度。

結論（續）

- 在本文中，我們提出一基於強韌型與脆弱型浮水印的原理實現保護證據管理鏈過程中的**數位媒體證據**。在我們的系統中，能完全滿足數位證據管理鏈的二項需求，即同時建立能具備**簽章的鑑定性質與內容完整特徵偵測**。
- 在本文的研究中所提出的兩演算法分別為**IEA**與**IADA**可清晰鑑定所有權人的嵌入浮水印得以確立簽章的正確來源，並進一步可以得知數位影像是否經過竄改，藉以建立數位證據完整性。因此。我們的疊合型資訊嵌入系統確實符合現行**證據管理鏈完整性保護系統**裡對於數位證據蒐集與鑑識的需求，實現管理鏈過程中的合法性。

References

- 王旭正, 林祝興 and ICCL(資訊密碼暨資料建構實驗室), 數位科技安全與鑑識-高科技犯罪預防與數位證據偵蒐, 博碩文化出版社, ISBN: 978-986-201-196-6, Feb. 2009.
- 王旭正, 柯永瀚, and ICCL(資訊密碼暨資料建構實驗室), 電腦鑑識與數位證據-資安技術、科技犯罪的預防、鑑定與現場重建, 博碩文化出版社, ISBN: 978-986-201-004-4, June, 2007.
- 王旭正, 柯建萱, and ICCL(資訊密碼暨資料建構實驗室), 資訊媒體安全- 偽裝學與數位浮水印, 博碩文化出版社, ISBN: 978-957-527-980-6, July, 2007.
- 王旭正, 高大宇, and ICCL-資訊密碼暨資料建構實驗室, 資訊安全與鑑識科學, 博碩文化出版社, Jan., 2007.
- 王旭正, 柯宏叡, and ICCL-資訊密碼暨資料建構實驗室, 秘密通訊與網路安全, 博碩文化出版社, March, 2006.
- 王旭正 (資訊密碼暨資料建構實驗室), “資訊安全鑑識程序建立與有效證據萃取作業(XXXIII) 一直擊Unix/Linux系統入侵Using the Power of TCT鑑識,” 網管人雜誌, <http://www.netadmin.com.tw/>, 城邦文化電腦雜誌系列, to appear in April, 2009.
- 王旭正 (資訊密碼暨資料建構實驗室), “資訊安全鑑識程序建立與有效證據萃取作業(XXXII) 一即時通訊媚力vs. 數位鑑識魅力,” 網管人雜誌, <http://www.netadmin.com.tw/>, 城邦文化電腦雜誌系列, to appear in March, 2009.
- 王旭正 (資訊密碼暨資料建構實驗室), “資訊安全鑑識程序建立與有效證據萃取作業(XXXI) 一新USB介面: U-Key於資安與鑑識應用,” 網管人雜誌, <http://www.netadmin.com.tw/>, 城邦文化電腦雜誌系列, Feb., 2009.
- 王旭正 (資訊密碼暨資料建構實驗室), “資訊安全鑑識程序建立與有效證據萃取作業(XXX) 一以小搏大: 遠端鑑識的閃靈工具-Helix 2.0,” 網管人雜誌, <http://www.netadmin.com.tw/>, 城邦文化電腦雜誌系列, Jan, 2009.
- 王旭正 (資訊密碼暨資料建構實驗室), “資訊安全鑑識程序建立與有效證據萃取作業(IXXX) 一數位證據縱橫談：抽絲剝繭之藕斷絲連,” 網管人雜誌, <http://www.netadmin.com.tw/>, 城邦文化電腦雜誌系列, Dec., 2008.
- S.J. Wang and D.Y. Kao, "The IP Address and Time in Cyber-crime Investigation," Policing: An International Journal of Police Strategies & Management, accepted in Feb. 2009. (SCI).
- S.J. Wang, D.Y. Kao, and Frank F.Y. Huang, "Procedure Guidance on Internet Forensics Coping with Copyright Arguments of Client-Server-based P2P Models," International Journal Computer Standards & Interfaces, on-line, 2008. (SCI)
- S.J. Wang, "Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crime," International Journal Computer Standards & Interfaces, Vol. 29, Jan. 2007. (SCI)
- S.J. Wang and D.Y. Kao, "Internet Forensics on the Basis of Evidence Gathering with Peep Attacks," International Journal Computer Standards & Interfaces, Vol. 29, pp. 423-429, 2007. (SCI)
- S.J. Wang, H.J. Ke, J.H. Huang, and C.L. Chan, "Hash Cracking and Aftereffect on Authentication Procedures in Cyberspace," IEEE Transactions on Aerospace and Electronic Systems, Jan. 2007. (SCI)



- **Dr. Professor Shiuh-Jeng WANG**
- PhD. National Taiwan University, Taiwan, 1996
- Full Professor, Central Police University, Dept. of Information Management
- Director Information Crypto and Construction Lab
- Chair of ICCL-FROG (Forensic Research development task force Group)
- Vice-President, Chinese Cryptography Information Security Association (www.ccisa.org.tw)

- Chairs of IEEE-CS/LNCS Proceedings, Internat'l confs.
<http://www.sercsc.org/SH08/> <http://www.ftrg.org/MPIS2009>
<http://ncs2009.ntpu.edu.tw/CI/CI.htm> <http://www.ftrg.org/futuretech2010>
<https://sites.google.com/site/uicuipm2012/> IEEE-sponsored,
<http://www.ftrai.org/music2012>
- Editor-in-Chief AT JITAS (<http://jitas.im.cpu.edu.tw>)
- SCI-Journals, Guest-editors,-
 - IEEE J-SAC, <http://www.comsoc.org/livepubs/sac/index.html>
http://hera.im.cpu.edu.tw/sjw_2006/meeting_report/IEEE-GUEST-EDITORIAL-0808-2011-.pdf
 - Journal of Internet Technology (JIT)
<http://jit.ndhu.edu.tw/callforpaper/April-2011-SI-JIT.pdf>
 - The Computer Journal, <http://comjnl.oxfordjournals.org/>
 - Springer Telecommunication Systems
<http://www.springer.com/business/business+information+systems/journal/11235>
 - The Journal of Supercomputing,
<http://www.springer.com/computer/swe/journal/11227> (Springer)
 - Peer-to-Peer Networking and Applications,
<http://www.editorialmanager.com/ppna/> (Springer)