數位浮水印技術發展現況:以數位典藏計畫為例

蕭人豪, 林欣慧, 林金龍, 林麗虹
中央研究院資訊科學研究所
{jenhao, augcat, eddy, monica }@iis.sinica.edu.tw

摘要

隨著電腦與網路的快速發展，數位資料得以不受時間與空間的限制藉由網路快速的傳播交換，隨之而來的是許多安全上的問題，例如智慧財產權的侵權問題。在數位化的世界中，複製資料是一件輕而易舉的事，但是未經授權的複製與散佈，對原創作者來說卻是一大打擊。目前數位典藏國家型科技計畫中，各典藏單位主要採用的數位智財保護機制為數位浮水印技術。數位浮水印是將代表數位智財擁有者的資料嵌入到數位多媒體資訊中未來若發生版權爭議時，則可以反向取出嵌入在數位多媒體中的數位浮水印，作為版權認證的依據。在此種以數位浮水印為保護核心的架構下，數位浮水印的有效性及強健性將是整個系統是否成功的關鍵因素。本文藉由數位典藏國家型科技計畫—技術研發分項計畫所舉辦的『2004 浮水印技術評比』競賽結果探討浮水印技術發展的現況，與其應用在保護數位典藏品上所能發揮的效果。

關鍵字：數位浮水印、數位版權管理、2004 浮水印技術評比

1. 前言

由於數位內容可以很輕易的利用電腦進行複製，再經由網路交換與散佈，本質上和傳統的出版業有著很大的差異，因此，數位內容 (Digital Content) 與智慧財產權在近幾年成為一個相當熱門的議題，數位內容的智財權保護也就格外的受到重視。尤其在『數位典藏國家型科技計畫』中擁有數量龐大且珍貴的數位典藏品，各內容典藏單位希冀透過各種保護機制防止數位典藏品被非法的複製及濫用。因此如何有效的保護數位典藏品成為各內容典藏單位相當重視的一個環節。其中，『數位浮水印技術』是目前各內容典藏單位主要用來保護數位典藏品的方法，典藏單位將代表數位智財擁有者的資料嵌入到數位多媒體資訊中，將來若發生版權爭議時，則以反向取出嵌入在數位多媒體中的數位浮水印，作為版權認證的依據。

在以數位浮水印為主要核心的數位內容保護架構下，其所能夠達到的保護效果將是整個系統能否成功的關鍵因素。為瞭解目前數位浮水印技術的發展現況，數位典藏國家型科技計畫—技術研發分項與中央研究院資訊所聯合主辦『2004 浮水印技術評比』，以瞭解目前國內數位浮水印技術之成熟度。在本論文即以『2004 浮水印技術評比』測試結果進行分析與探討，以瞭解當前浮水印技術所能達到的保護效果與瓶頸。

本論文結構說明如下。在第二節中將介紹最常被用來保護數位智財的技術—數位浮水印的基本原理；在第三節中，以『2004 浮水印技術評比』的結果來探討目前數位浮水印技術現況及其瓶頸；而目前最新的數位智財保護趨勢 - 數位版權管理 (Digital Right Management)，將在第四節進行檢視，並分析其可為數位智財帶來的保護效果；最後第五節為本文的結論。

2. 數位浮水印概述

2.1 數位浮水印基本定義

如前所述，將代表原創作者的資料或是一組特別的資訊嵌入到數位多媒體資訊中，未來若發生版權爭議時，希望透過此一技術，將嵌

入在數位多媒體中的認證資訊取出，作為版權認證的依據。這一種技術稱之為數位浮水印。當所嵌入之資料或資訊在視覺上是無法察覺的，稱為「隱性浮水印」(invisible watermarking)；若加入的資料是可察覺的，稱為「顯性浮水印」(visible watermarking)。一般而言，當提到數位浮水印技術時，絕大部分的情況所指的都是隱性浮水印。而數位浮水印在設計上常需考慮的因素如下：

(1) 透明度 (Transparency)：
浮水印植入影像後，不能影響原始影像在視覺上的品質，此為浮水印的基本要求。

(2) 安全性 (Security)：
所植入的浮水印必須具有不可偵測的特性。即使知道了浮水印的架構，使用者仍必須擁其對相應之秘鑰 (secrete key) 才可以取出浮水印。

(3) 明確性(Unambiguous)
所藏入之浮水印應該清楚確認版權所有人。

(4) 強健性 (Robustness)：
含有浮水印之影像在經過攻擊後，是否仍能存在於影像之中。

(5) 容量 (Capacity)：
在原始影像中，能加入最多不同的浮水印長度或個數。一個好的浮水印技術必須能使原始影像盡可能容納更多的資訊，但這個條件通常和透明度的要求背道而馳。

(6) 是否需要來源的比對 (Blindness)：
在抽取浮水印時，是否需要原始來源資料或相關資訊加以比對。

2.2 數位浮水印運作原理

假設數位內容的作者 A 握有一張數位影像 I’ 為了保護它，A 可以加入一個包含其著作權資訊的數位浮水印 w 到原始影像 I 中，產生一個受保的影像 I’：

$$I' = I + w$$

受保護的影像 I’ 可以開始流通，交予使用者使用。而當日後 A 發現一個可能侵犯其知財權(非法盜用)的可能侵權影像 I’’ 時，就可以計算 I 和 I’’ 之間的差異而取出浮水印 w’ ：

$$w' = I'' - I$$

若侵權影像 I’’ 的確是源自於受保護的影像 I’ (即 I’’ = I’)，則：

$$\begin{aligned} w' &= I'' - I \\ &= I' - I \\ &= w \end{aligned}$$

因此我們可以依據 w’ 與 w 的相似程度來判斷可能侵權影像 I’’ 是否就是遭到盜用的數位影像[7]。圖 1 以流程圖的方式顯示了完整的浮水嵌入與抽取流程。

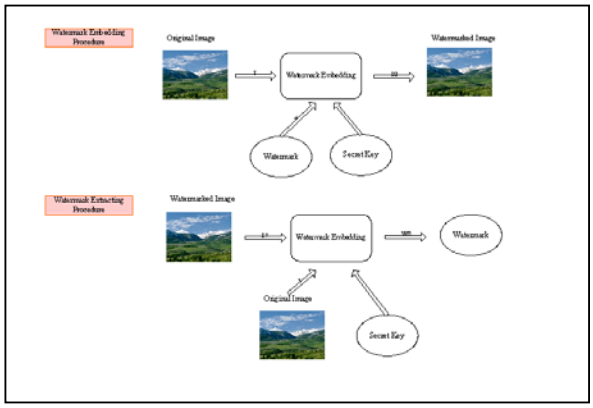

圖 1. 完整的浮水嵌入與抽取流程

2.3 數位浮水印應用分類

根據不同的需求，數位浮水印可以區分以下不同類別的應用[8]：

(1)版權保護(Copyright Protection)
版權保護是最常見的數位浮水印應用類型。為了可以辨識所有權者，在影像散佈之前事先加入一組可以代表所有權人資訊的數位浮水印到其中，以便於發生版權上的爭議時，可以用來驗明影像的所有權。

(2)驗證(Authentication)
數位浮水印也可以拿來當成數位資料真確性驗證及竄改偵測。在此種應用模式中，數位資料會被加入一組強韌性較低的脆弱浮水印(fragile watermark)。在進行數位資料的傳遞時，如果數位資料遭到第三者的截取並進行修改，則隱藏在其中的浮水印將因遭到破壞而無法抽取，也因此數位資料的接受方得以驗證資料之真確性，與查覺是否數位資料已遭到第三者的竄改。

(3)具鑑別性的特徵(Fingerprinting)
Fingerprints 意指為每一個數位物件加入一個獨一無二的識別碼，就像指紋一樣。為了追蹤使用者或購買者非法將產品轉賣或移做其它用途時，通常會在數位資料交給使用者之前，就在每個釋出的版本中放入一個獨一無二的浮水印，以供日後辨別。若日後發覺非法的產品時，就可取出數位浮水印，以查明是誰將數位資料做了非法的用途。

2.4 典型數位浮水印保護流程
學者 Carlos Serrao 與 Joaquim Marques[6] 曾針對數位影像提出一套完整的保護流程的概念模型 - DIGIPIPE。從最上游的數位影像的製作，到下游的數位影像散佈與交易，共可分為四個階段：

(1) 第一階段(Pre-Selection, Digitalization and Selection)
對實體影像進行數位化，並進行品質的控管。

(2) 第二階段(Retouching, Pre-Cataloguing and Tilling)
對前一階段所產出的數位影像進行最後的視覺校正，並記錄所有數位檔案的相關資訊（作者，出處，數位化時間等）。

(3) 第三階段(Registration and Watermark Insertion)
將完成數位化的影像註冊到資料庫中，並將相關版權資訊以數位浮水印型式嵌入到數位影像中。

(4)第四階段(CD-ROM production, Cataloguing, E-Commerce site publication and Tading)
加入浮水印保護的數位影像製作完成後，即可開始以各種不同的型態(儲存於 CD-ROM 中、利用網路傳輸等)進行資訊交換與交易行為。

DIGIPIPE 的模型是最基本的以數位浮水印保護數位影像的完整流程，也非常接近目前各典藏單位的浮水印嵌入流程。不過整個模型的智財權保護主要依賴數位浮水印，因此數位浮水印的抗攻擊性是否足夠將是整個模型的成敗關鍵！在下一節中，我們將以『2004 數位浮水印技術評比』競賽的測試結果來檢視目前浮水印技術的發展成熟度，並分析各項測試數據背後的意義。

3. 2004 數位浮水印技術評比

3.1 評比目的

在軟體開發的領域中，使用者的想法與技術開發者觀點常存有不少的差距，在數位浮水印核心軟體的研發上亦有著類似的問題。內容典藏單位所提出的需求與技術研發團隊所重視的研發方向大相逕庭，一方面是典藏單位不熟悉數位浮水印技術發展狀況與成熟度，另一方面則是技術研發團隊忽略使用者在使用上所在意的細節事項。為了減輕典藏單位與技術研發團隊之間所存在的鴻溝，數位典藏國家型科技計畫—技術研發分項計畫與中央研究院資訊科學研究所特舉辦『2004 數位浮水印技術評比』活動，目的在於廣邀浮水印技術相關研究人員與內容專家參與，彼此砌磋以促進浮水印技術之發展，並讓內容技術雙方了解浮水印技術發展狀況與應用之可行性，以提供數位典藏單位未來規劃浮水印技術整合之參考。

3.2 評比準則

浮水印核心之評比以下列四個項目做為評分依據[4]:

(1)影像品質(Visual Quality)

浮水印加入影像後，對影像品質所造成的影響。使用 PSNR 做為評分依據，定義如下：

$$PSNR(dB) = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

(2)浮水印強韌性(Robustness)

經過攻擊後，浮水印是否仍能存在於影像之中。在此使用 BER (bit-error rate) 值做為參考，定義如下：

BER = Number of Wrong Extracted Bits / Number of Original Watermark Bits

(3)浮水印嵌入及擷取時間

加入及擷取浮水印所需的時間是否合理。

(4)False Positive Test

測試浮水印核心程式進行浮水印抽取時，產生誤判的機率。

3.3 競賽環境與參數設定

(1)軟硬體環境

由於浮水印的嵌入及抽取會耗用大量的軟硬體資源，為了防止因記憶體不足而導致浮水印核心程式執行失敗，本次競賽採用裝載 1G DDR Ram 之雙 CPU 機器進行測試。相關軟硬體環境簡述如下：

軟硬體項目	配備內容
CPU	Pentium 4 Xeon 2.8G * 2
Memory	1G DDR Ram
OS	Windows 2000 Advanced Server

(2) 競賽測試影像

為針對不同的應用領域，測試影像分為一般彩色影像、大型彩色影像及二元黑白影像三個類別。其中大型彩色影像為大於 5000*5000 像素，且色彩深度大於 8 bits 之數位影像，此類別對應數位典藏計畫中之典藏級影像。一般彩色影像為小於 5000*5000 像素，且色彩深度大於 8 bits 之數位影像，此類別對應數位典藏計畫中之一般瀏覽級影像。二元黑白影像則為色彩深度為 1 bits 之數位影像，且小於 5000*5000 像素。

(3)浮水印攻擊項目

為了驗證浮水印之強韌性，競賽使用 Stirmark 4.0[9] 做為本次浮水印攻擊軟體，並採用表 1 所列之攻擊項目及相關參數[10]：

表 1. Stirmark 4.0 攻擊參數設定

編號	攻擊方式	Stirmark 參數設定
A1	AddNoise	Noise level 20、40、80 Level 愈高，則雜訊愈多
A2	JPEG	Quality level 20、10、5 Level 愈低，則壓縮比愈高
A3	MedianCut	filter size = 5、7、9
A4	ConvFilter	Gaussian filtering、Sharpening
A5	RemoveLines	frequency 5、10、15 frequency 愈高，則移除資訊愈多
A6	Cropping	ratio 15、30、50 ratio 愈低，則移除資訊愈多
A7	Rescale	ratio 25、50、150 當 ratio > 100 時，為放大效果 當 ratio < 100 時，為縮小效果
A8	Rotation	angles 20、45、90

3.4 評比結果與分析

由『2004 浮水印技術評比-技術報告』[3] 中可以發現，典藏單位在浮水印技術的基本需求及管理議題，如 key files 的管理等問題，目前的技術已經可以提出一套有效的解決方案，來符合典藏單位的需求。不過在浮水印嵌入技術及強韌性方面，則顯然還未能滿足典藏單位所期望的效果。

在浮水印嵌入技術方面，隱性浮水印嵌入技術、多元圖檔色彩嵌入、大型影像檔嵌入支援、批次處理嵌入與浮水印錯誤偵測率…等等問題，大部分都可以順利的在本次競賽中找到符合需求的技術，較大的問題在於，浮水印嵌入後對原始影像所造成的傷害高過於典藏單位所預期，原因之一是因為藝術工作者對於影像品質的要求較高，也因此各組參賽隊伍在人工視覺評分方面幾乎都未能取得高於正常視覺標準的成績，這將可能會是未來浮水印技術在實際應用上的一個障礙。

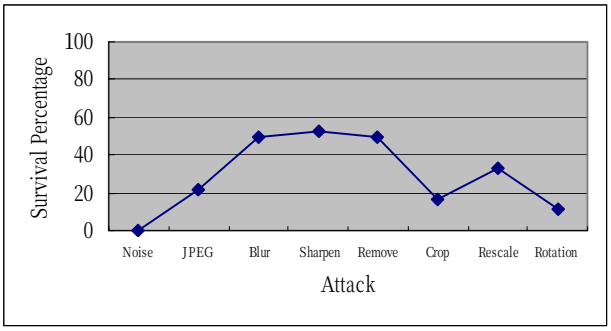

圖 2. 受攻擊後的浮水印存活率

目前浮水印技術發展與典藏單位需求落差最大的項目可說是在浮水印的強韌性方面。圖 2 顯示了在本次評比中，浮水印在不同種類攻擊下的存活率。X 軸表示各種不同的影像攻擊方式，Y 軸則代表所有嵌入浮水印的測試影像在遭受攻擊後，還可以順利取出取水印的比例。從圖中可發現，浮水印除了在一般影像處理類攻擊下有較高的存活率外，其餘的表現則明顯不理想。而關鍵點在於浮水印之強韌性為浮水印核心中最重要部分，也是典藏單位最重視的環節，如果一個受浮水印保護的數位內容可以經由簡單的影像組合攻擊而移除，那麼以浮水印來保護數位智財及宣告所有權人資訊的這一深層意義將蕩然無存。但以目前浮水印技術在實際應用面的成熟度觀之，數位浮水印技術目前似乎尚無法提供一個完整而穩健的數位智財保護環境。

事實上在目前網路高度開放環境中，若僅僅使用浮水印技術就要能對抗起所有的駭客或惡意第三者的攻擊的要求是過高的。這項事實不難從目前數位智財的保護趨勢得到驗證，目前在產業及學界的研究發展中，多較為朝向由數位內容製造的起始端即開始進行保護，包含其間的傳遞、使用存取與行為紀錄，強調完整流程的保護，與資訊安全相關技術的整合(包含加解密技術、使用者驗證、數位簽章及數位浮水印…等)，用以建構完整的數位智財保護環境。此一類型的整合架構，稱之為『數位版權管理系統』 (Digital Right Management，DRM)，本文將介紹此一技術，並分析它能為數位智財保護帶來的效果。

4.數位版權管理—DRM

4.1 DRM 定義

數位版權管理，Digital Rights Management，簡稱 DRM，國際數據資訊中心 IDC(Internet Data Center)之定義為[5]：結合硬體與軟體的存取機制，將數位內容設定存取權限，並與儲存媒體聯結，使得數位內容在其生命週期內—從產生到消失(如檔案被刪除或全世界都無法開啟使用的狀態下)，不管在其使用過程中是否有被複製到別處，仍然可以持續追蹤與管理數位內容之使用狀況。總而言之，在數位內容生命週期內，能提供完善保護數位內容、權利之管理技術，則稱為 DRM。

數位化內容產業包括實體面與權利面[1]，實體面指的是數位內容的部分，包括取得、加值等方面；而權利面即指著作權管理的部分。DRM 強調其能在數位生命週期內做到「事前防範」的安全管理，因此，DRM 可以說是結合了『數位物件保護技術』及『數位權利管理模型』以達到對數位內容保護的解決方案。

4.2 典型 DRM 模型

當 DRM 運作的過程中，通常會涉及到以下四個不同的實體[5]：內容提供者(Content Provider)、數位內容散佈者(Distributor)、交易與權限控管中心(Clearinghouse)與消費者(Consumer)。圖 3 描繪出了一個典型的 DRM 模型概念，而每個實體所代表的意義為：

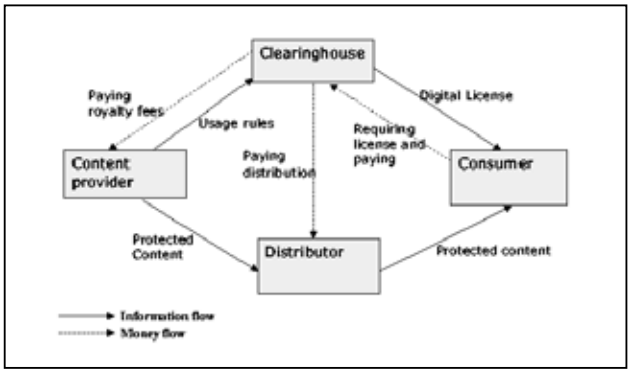

圖 3. 典型 DRM 模型

(1)內容提供者(Content Provider)

數位內容的提供者，擁有數位內容的權利。

(2)數位內容散佈者(Distributor)

數位內容散佈者為內容提供者和消費者之間的媒介，並擁有數位內容銷售或散佈的管道及通路。他們從內容提供者接收取數位內容後，再利用其通路交給消費者。

(3)交易與權限控管中心(Clearinghouse)

負責管控數位內容的權限與交易等事宜，並負責核發數位權限(digital rights)，所有消費者的相關執行權限與交易記錄都會被記錄在此。

(4)消費者(Consumer)

有意願取得及利用數位內容的末端使用者。

模型的運作流程如下。首先內容提供者利用加解密技術封裝原始的數位內容，並加入代表其所有權的浮水印及其願意開放的數位權限。封裝完成的數位內容將會傳遞給擁有通路的『數位內容散佈者』，而其相對應的數位權限則交由『交易與權限控管中心』進行保存。消費者可以透過數位內容散佈者取得經過封裝的數位內容，並向『交易與權限控管中心』要求相關授權，或進行數位權利之購買。『交易與權限控管中心』收到消費者的請求後，再依據其提出之要求審核其資格是否符合，確認後再給予其要求之數位權利。最後消費者則可以依據此數位權利所允許執行之項目，來解開封裝的數位內容，並進行利用。值得注意的是，消費者仍然可以任意的散佈從數位內容散佈者所下載的封裝數位內容，但是其它使用者將因沒有『交易與權限控管中心』所核發的數位權限，而無法對該數位內容進行應用。

5. 結論

『數位典藏國家型科技計畫』的意義不僅只侷限於狹義的將資料數位化，也更進一步扮演推廣與教育的角色，透過有系統的規劃與處理，將資訊呈現給大眾。期盼以更快速、便利的機制來吸引更多的大眾，使社會大眾瞭解中華文化的博大精深。但在資料數位化或資訊傳播的過程中，卻也延伸出許多的問題，例如智慧財產權的保護、數位典藏品在網路上傳遞可能遭到竊取與典藏資料庫的非法存取…等等問題，種種的攻擊方式都需要依賴於健全的安全機制來加以預防與偵測。

不過單憑數位浮水印技術以求達到數位智財的保護是消極且不周全的，在網路與駭客同樣發達的今天，或許我們可以說，數位浮水印是一種『防君子不防小人』的技術 。倘若要求數位浮水印對於目前成千上百種影像攻擊方式都具有強韌性是過於苛求的！關於這個事實我們也不難在這次的浮水印技術評比中得到佐證，參賽團隊的浮水印演算法通常只會對某些攻擊項目具高存活率，而非如我們所想像中般可以抵禦所有的攻擊。

數位浮水印的最大作用或許是在於它的嚇阻作用，而非眾所想像的『無論流通在外的數位內容遭遇到何種攻擊或修改，只要發生版權爭議時，可以將嵌入在數位多媒體中的認證資訊取出，作為版權認證的依據。』數位浮水印技術之所以『防君子』，是因為有動機竊取數位內容的使用者並無法確定數位內容中的浮水印是否已經因為遭受攻擊而被移除(數位浮水印假設使用者並無法得到偵測浮水印是否存在的核心程式)，因此與其冒險違法使用數位智財，還不如安份守已。當然此一論點對於具有高超技術能力的駭客可能是不成立的，他們可能可以攻破整個數位浮水印的設計架構，甚至在把原始浮水印移除後，反向加入代表自己的浮水印，如此一來豬羊變色，駭客反客為主，也因此說數位浮水印『不防小人』。若從另一個角度思考，當數位智財發生版權爭議時才進行補救，這個想法本身對於智財權的保護就已經顯得消極了。所謂『積極的預防勝過事後的補救』在數位智財的保護將同樣是最高指導原則。如果我們在數位智財的製作、生產、分佈與流通的過程中，每一個環節都曾留心注意，不予有心人士可趁之機，則數位智財才能真正稱為所謂的得到保護。

6.誌謝

[1] 行政院國家科學委員會，數位典藏國家型科技計畫-技術研發分項計畫，NSC93-2422-H-001-0003

[2] 行政院國家科學委員會，數位典藏國家型科技計畫-技術研發分項計畫-典藏系統，建置與相關技術研發計畫，NSC 93-2422-H-001-0004

[3] 數位典藏技術發展組(DAAL)

[4] 中央研究院資訊科學研究所電腦系統與通訊實驗室

7. 參考文獻

[1] 陳映后，何佳欣，黃崇瑋，”數位圖書館與 DRM”，數位內容創意加值研討會，論文集 II，2003 年 11 月，頁 17-25

[2] 楊大廣主講、林雅玲整理。”數位權利管理的市場趨勢及技術展望”，智慧財產權管理季刊 35 期，民 91 年 12 月，頁 6-7

[3] 蕭人豪,“2004 浮水印技術評比-技術報告”，中央研究院資訊科學研究所年度報告,民國 93 年 3 月

[4] M. Kutter and F. A. P. Petitcolas, “A fair benchmark for image watermarking systems”, Electronic Imaging '99. Security and Watermarking of Multimedia Contents, vol. 3657, Sans Jose, CA, USA, 25~27 January 1999. The International Society for Optical Engineering.

[5] Qiong Liu, Reihaneh Safavi-Naini, Nicholas Paul Sheppard, “Digital rights management for content distribution”, Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003 - Volume 2

[6] Serrao, C.; Marques, J.; “DIGIPIPE-A Pipeline methodology for Digital Image Production And Protection”, Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium on VIPromCom , 16-19 June 2002, Pages:411 – 416

[7] Sin-Joo Lee; Sung-Hwan Jung, “A survey of watermarking techniques applied to multimedia”, Industrial Electronics, 2001. Proceedings. ISIE 2001. IEEE International Symposium on , Volume: 1 , 12-16 June 2001, Pages:272 - 277 vol.1

[8] Stefan Katzenbeisser, Fabien A.P. Petitcolas, Information hiding techniques for steganography and digital watermarking, Boston : Artech House, 2000

[9] stirmark benchmark 4.0, http://www.petitcolas.net/fabien/watermarking/stirmark/

[10] Voloshynovskiy, S.; Pereira, S.; Pun, T.; Eggers, J.J.; Su, J.K.; “Attacks on digital watermarks: classification, estimation based attacks, and benchmarks”, Communications Magazine, IEEE , Volume: 39 , Issue: 8 , Aug. 2001, Pages:118 - 126