灰階色差視覺密碼於 DICOM 醫療影像之加密與浮水印的研究

A Study of Encryption and Watermarking for DICOM Medical Images Based on Grey-Level Chromatic Visual Cryptography

曾明性[1]、何英治[1]、林明毅[2]

[1]中山醫學大學資訊管理學系、[2]國立暨南國際大學資訊工程研究所碩士生

[1]mht@csmu.edu.tw、[2]dalelin007@hotmail.com

摘要

由於醫療資訊學的快速發展，許多醫學影像已數位化，而數位化之醫學影像除便於儲存及傳輸外，更有助於醫生做診療。然而將未保護的醫療影像直接於網路上傳輸，極容易被擷取利用，而侵害病患的隱私權、或侵犯影像原作者的著作權。基於視覺密碼的原理，本文研究目的為開發可適用於 DICOM 3.0 灰階醫療影像之色差視覺加密技術與數位浮水印製作技術，以增加醫療影像於網路傳輸的安全性，當有著作權侵害時，可將浮水印取出驗證以證明醫療影像之原作者為誰。實做結果顯示，本研究提出以灰階色差視覺加密法製作 DICOM 灰階醫療影像之加密與浮水印技術，確可為保護隱私權與智慧財產權提供另一種簡易、直接且強韌有效的方法。

關鍵字：醫療影像、視覺密碼、色差視覺加密技術、數位浮水印。

Abstract

The medical-informatics vigorously develops now, many medical images have been digitalized, which are not only convenient to be saved and transferred but more helpful for doctors to diagnose. It is easy to result in the privacy invasion and copyright infringement if non-protection medical images transmit in the network directly. Based on visual cryptography, the objective of this study is to develop encryption and digital watermarking technologies for DICOM 3.0 grey-level medical images using the chromatism visual encryption method. The result reveals that the proposed technologies are simple, direct and robust to protect the privacy and copyright of DICOM grey-level medical images when they are transferred in the Internet.

Key words: medical images, visual cryptography, chromatism visual encryption, digital watermarking

壹、緒論

一、研究動機

從嵌入數位浮水印後的媒體外觀可區分為兩種技術，第一種是可見數位浮水印，也就是於表現版權之媒體上顯現隱約可見的浮水印，如圖 1 所示可以隱約從圖形中看見「LENA」字樣，其缺點是破壞原有影像的品質，只能用肉眼辨識，無法使用程式自動化偵測，但使用者看見浮水印也就不敢隨意非法使用，主要具有嚇阻的作用。第二種是不可見數位浮水印，嵌入浮水印的媒體與原未嵌入時無法從外觀上看出有何差別，如圖 2 所示，將浮水印隱藏在媒體的不顯眼處，優點是對媒體品質的破壞降低，符合了浮水印的隱蔽性，當發生著作權爭議時，將浮水印取出以保障原著作者的權益。

圖 1 可見浮水印範例

圖 2 不可見浮水印範例

綜觀現今的浮水印技術[4-5]，大致存在以下四個缺點：

(1) 部分演算法在取出浮水印時，需要原圖的協助。

(2) 所有演算法在加入浮水印時，皆會破壞到原圖。

(3) 不同浮水印技術，嵌入的浮水印資料量皆有其限制。

(4) 若不慎流失了原圖，所有演算法即無任何保護可言。

今日由於網際網路與電腦產業的快速發展，醫院內外均使用網路環境進行醫療影像之傳輸交換，因此，為了能確保病患的醫療影像在傳輸時不易直接外洩、並改善上述四項現有浮水印技術的缺點，本文應用視覺密碼的理論，提出一種新的灰階醫療影像加密方法與浮水印製作技術，可對原醫療影像無任何破壞，具有加密功用，並可將浮水印抽象的加入。

二、文獻回顧

一個良好的浮水印應具有下列特性：

(1) 隱蔽性(imperceptibility)：媒體加入浮水印之後，在視覺、聽覺上必須難以查覺，並應減少對欲嵌入媒體品質的破壞。

(2) 強韌性(robust)：將浮水印嵌入隱藏媒體後，經過壓縮、變形、模糊、旋轉、分割、馬賽克等或其他數位訊號處理程序後，仍然可以取出原先嵌入的浮水印並可進行判讀，或者至少浮水印在被破壞時，原始影像已經嚴重失真。

(3) 不可偵測性(undetectable)：加入浮水印須無法被偵測出位置，避免遭到有心人士剪裁移除。

(4) 不易移除(non-removable)：擷取者不易移除浮水印資訊，或者降低浮水印相關的資訊。

(5) 明確性(unambiguous)：取出的浮水印必須能明確的證明所有者，在遭到攻擊後還能準確的取出浮水印，不會有模擬兩可的情況。

(6) 安全性(security)：未經授權者即使知道浮水印加入的程序也無法移除浮水印。

浮水印的嵌入方法分為兩種，第一種使用空間域，另一種使用頻率域，以空間域製作浮水印其方法簡易，但容易遭到攻擊而破壞浮水印，目前製作浮水印大都使用頻率域，需要經過複雜的運算嵌入及取出，並對原圖的資料加以破壞，如要減少對原圖資料的破壞以提昇浮水印的製作效能，則須將欲嵌入的浮水印大小逐次減半，但過小的浮水印恐將難以辨識。

以往要將資訊加解密必須透過複雜的數學運算才可行，若在一個無法負荷繁複的計算需求的環境下，視覺密碼提供一有效之加解密的解決方法。視覺密碼最早由 Naor and Shamir[7]在 1994 年於國際密碼研究學會中提出的黑白視覺密碼學，其方法是產生 n 張無任何意義的投影片，其中只要 t 張投影片重疊起來，即可讀出機密影像，只有一張是無法取得機密影像的，但傳送時擷取者只要能取得所有的分享影像，即可以視覺系統進行解密。

Rijmen and Preneel[9]於 1996 年提出一個彩色視覺密碼的做法，其原理是將每個像素分割成四個附屬像素，包括了紅、綠、藍、白，這些附屬像素可以是隨意排列順序，並能得到 24 種可能的組合，其認為兩張分享影像重疊後就有 24^2 種組合，但 Yang[6]提出修正，認為其只有 17 種不同的組合。

侯永昌與周智倫[1]提出以視覺密碼為基礎，使用灰階圖形當作原圖、單色圖形當作浮水印，其浮水印為原圖大小的 $\frac{1}{4}$，Share1 以四宮格為單位與浮水印比較產生 Share2，Share1 與 Share2 疊合後產生出 75%的黑當作白色與 100%的黑當作黑色，再以正規化關聯分析 NC 值輔助視覺系統判斷。

貳、研究方法

一、DICOM 格式簡介

DICOM 是由 ACR-NEMA 所制定，其目的在於使醫療影像可以在不同系統間傳輸交換，目前為止 DICOM 已修訂至 3.0 版。DICOM 檔案結構分成兩大部分(圖 3)，分別為檔頭(Header)與資料集合(Data Set)，使用標準 DICOM 格式在檔頭部份是可以省略的。其檔頭又分為 Preamble 與 Prefix 兩部分，Preamble 存放協助其他應用軟體讀取影像的資訊，通常不使用，長度為 128 Bytes，Prefix 則固定存放 DICOM 四個字元。

Data Set 是由一群 Data Element(圖 4)所組成，Data Element 可分為 Data Element with explicit VR(圖 5,6)與 Data Element with implicit VR(圖 7)兩類，而 Data Element with explicit VR 又細分為兩種，其詳細結構如下所示，在此需注意的是，同一個 DICOM 檔案不可同時擁有 Data Element with explicit VR 與 Data Element with implicit VR 這兩種 Data Element。

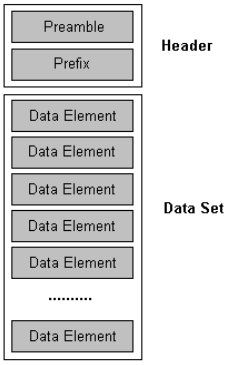

圖 3 DICOM 檔案結構[8]

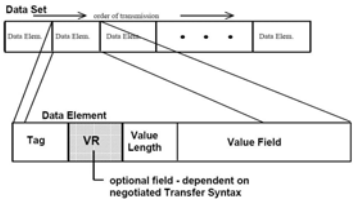

圖 4 Data Set and Data Element Structures

Tag		VR		Value Length	Value
Group Number (16-bit unsigned integer)	Element Number (16-bit unsigned integer)	VR (2 byte character string) of "OB", "OW", "OF", "SQ", "UT" or "UN"	Reserved (2 bytes) set to a value of 0000H	32-bit unsigned integer	Even number of bytes containing the Data Element Value(s) encoded according to the VR and negotiated Transfer Syntax. Delimited with Sequence Delimitation Item if of Undefined Length.
2 bytes	2 bytes	2 bytes	2 bytes	4 bytes	'Value Length' bytes if of Explicit Length

圖 5 包含 OB, OW, OF, SQ, UT, UN 的 Data Element with explicit VR

Tag		VR	Value Length	Value
Group Number (16-bit unsigned integer)	Element Number (16-bit unsigned integer)	VR (2 byte character string)	(16-bit unsigned integer)	Even number of bytes containing the Data Element Value(s) encoded according to the VR and negotiated Transfer Syntax.
2 bytes	2 bytes	2 bytes	2 bytes	'Value Length' bytes

圖 6 其他 Data Element with explicit VR

Tag		Value Length	Value
Group Number (16-bit unsigned integer)	Element Number (16-bit unsigned integer)	32-bit unsigned integer	Even number of bytes containing the Data Elements Value encoded according to the VR specified in PS 3.6 and the negotiated Transfer Syntax. Delimited with Sequence Delimitation Item if of Undefined Length.
2 bytes	2 bytes	4 bytes	'Value Length' bytes or Undefined Length

圖 7 Data Element with implicit VR

二、灰階色差視覺密碼

傳統密碼學皆須藉由繁複的數學運算來確保資訊的加密與解密，而視覺密碼不需複雜的運算即可將需要加密的影像拆成數張雜亂無章的分享影像，解密時止需將分享影像疊在一起，在利用人類的視覺系統即可分辨出解密影像。在安全性方面，竊密者也不可能在雜亂無章的分享影像上找到任何蛛絲馬跡[2-3,6-7]。

本文應用視覺密碼的理念，提出一個不需擴展處理且適用於灰階 DICOM 影像之新的加密方法：灰階色差視覺加密法。本演算法可表如下式所示：

$$\begin{cases} S_{1\ ij}^{R} = Random(a), 0 \le S_{1\ ij}^{R} \le 255, S_{1\ ij}^{R} \in N \\ S_{2\ ij}^{R} = S^{R}{}_{ij} - S_{1\ ij}^{R} \\ 1 \le i \le X, 1 \le j \le Y \end{cases} \quad (1)$$

其中 X、Y 為圖形大小，a 為亂數種子，S_{ij} 代表機密影像每個像素的灰階值，S_{1ij} 代表 Share1 每個像素的灰階值，S_{2ij} 代表 Share2 每個像素的灰階值。值得一提本演算法可直接延伸應用於全彩格式之任何影像上。

以一張 436×436 大小的灰階胸腔影像為例，每個像素(pixel)之灰階值 0~255，若原機密影像某像素之灰階值 S = 255，首先分享影像一之 S1 值係由亂數種子(seed)產生一隨機數值如 S1 = 100，分享影像二即 S2 = S - S1 = 155。由於分享影像一每個像素均使用不同亂數產生，故能有效的將機密影像中的色彩圖徵完全打散，使擷取者無法從單一影像中取得有關機密影像的輪廓，而分享影像二是由分享影像一和機密影像所共同產生，它具備了分享影像一的優點並且保留了還原時所需的資訊，能使用重疊的方式進行解密，其被破解的可能性為 $\frac{1}{256^{m\times n}}$，$m\times n$ 表機密影像的解析度。

在原始圖形使用色差視覺加密法，可以使原始機密影像每個像素的灰階值分散於兩張分享影像上，即可達到加密作用。在進行解密時，可以只要將分享影像直接重疊後靠人類的視覺系統進行解讀，以得到原始的機密影像。其詳細做法如下：

圖 8 顯示一張 436×436 大小的灰階胸腔影像機密影像，經過公式(1)的簡易演算後，即可獲得與機密影像相同大小的已加密之分享一影像 (圖 9) 與分享二影像(圖 10)。在進行解密還原影像時，只需將兩張分享影像重疊即可得到原機密影像的資訊。張真誠等人[5]指出，若使用環境是在電子網路上，則視覺密碼就不會有對不準兩張分享影像的問題，本文提出之色差視覺加密法解密後其所得到的機密影像資訊將會與原機密影像完全相同(圖 11)。

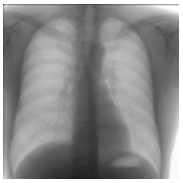

圖 8 機密影像 (436×436)

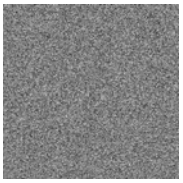

圖 9 分享一 (436×436)

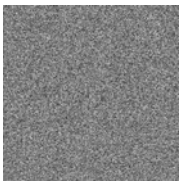

圖 10 分享二 (436×436)

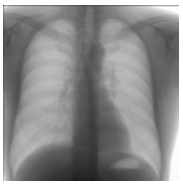

圖 11 還原機密影像 (436×436)

本文發展之灰階色差視覺加密法與前人需仰賴計算複雜度之加密法比較，本法更適用於計算資源負荷已重但儲存資源相當閒置之資訊環境上。

三、製作浮水印之演算法

輸入：一張灰階 DICOM 圖形，大小為 $W_1\times H_1$。

一張灰階的浮水印，大小為 $W_1\times H_1$。

輸出：Share2，大小為 $W_1\times H_1$。

其製作浮水印的詳細做法與演算法(公式 2)如下：

(1) 取出原圖(圖 13)各像素最高位元，架構成最高位元平面(BitPlane 7)，如圖 12 所示，以一個初始亂數碼自動產生一系列的虛擬隨機值重組最高位元平面，此為 Share1(圖 15)，此步驟是為了消除後續產生之 Share1 與 Share2 外觀上擁有原圖輪廓的情況。

(2) 使用灰階色差加密法，參考 Share1 與浮水印(圖 14)產生 Share2(圖 16)，Share1 可捨棄，Share2 與初始亂數碼則由原作者保存。

$$\begin{cases} S_{1ij} = P_{ij} \wedge 128 + a_{ij}, 0 \le a_{ij} \le 255, a_{ij} \in N \\ S_{2ij} = S_{1ij} - W_{ij} \\ 1 \le i \le X, 1 \le j \le Y \end{cases} \quad (2)$$

其中 X、Y 為圖形大小，a_{ij} 為隨機增加各像素值，S_{1ij} 代表 Share1 每個像素的灰階值，S_{2ij} 代表 Share2 每個像素的灰階值，P_{ij} 代表機密影像每個像素的灰階值，W_{ij} 代表浮水印圖形每個像素的灰階值，符號Λ代表 and 的邏輯運算。

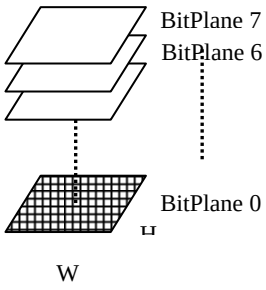

圖 12 位元平面圖

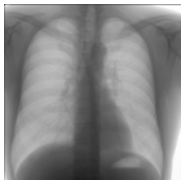

圖 13 灰階 DICOM 圖形 (436×436)

圖 14 浮水印原圖 (436×436)

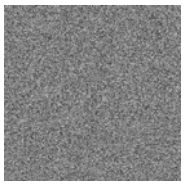

圖 15 Share1 (436×436)

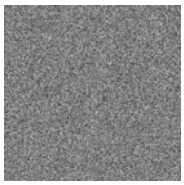

圖 16 Share2 (436×436)

五、取出浮水印之演算法

輸入：欲驗證之圖形與作者擁有之分享二圖形。

輸出：由 Share1*與 Share2 重疊後得到之浮水印。

其取出浮水印的詳細做法與演算法(公式 3)如下：

(1) 取出欲驗證之圖形各像素之最高位元，架構成最高位元平面，並以作者保有之初始亂數碼重組最高位元平面，此為 Share1*(圖 17)。

(2) 將 Share1*與 Share2(圖 18)重疊，即可取出初步之浮水印。

(3) 為去除原圖被攻擊後，還原之浮水印所產生的雜點，本文提出浮水印濾波器，對取出的浮水印以四宮格為單位，依據表 2 之規則替換此四宮格，如圖 19。

表 2 浮水印濾波器模型

Share1* + Share2	濾波後	說明
		白色
		白色權重大於黑色權重
		黑白權重一樣
		黑色權重大於白色權重
		黑色
		當非黑白色權重大於黑白色時，維持上次狀態

$$\begin{cases} S^{*}_{1\,ij} = V_{ij} \wedge 128 + a_{ij}, 0 \le a_{ij} \le 255, a_{ij} \in N \\ W^{*}_{ij} = S^{*}_{1\,ij} + S_{2ij} \\ 1 \le i \le X, 1 \le j \le Y \end{cases} \quad (3)$$

其中 X、Y 為圖形大小，a_{ij} 為隨機增加各像素值，$S^{*}_{1\,ij}$ 代表 Share1*每個像素的灰階值，S_{2ij} 代表 Share2 每個像素的灰階值，V_{ij} 代表驗證影像每個像素的灰階值，W^{*}_{ij} 代表取出之浮水印圖形每個像素的灰階值。

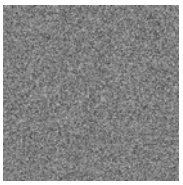

圖 17 Share1 (436×436)*

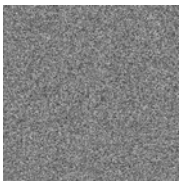

圖 18 Share2 (436×436)

圖 19 還原浮水印(436×436 *) (NC=1.0)*

六、使用正規化關聯(NC)分析

為了衡量取出的浮水印與原浮水印圖形的相似程度，利用 NC 值來評估還原後的黑白浮水印與原黑白浮水印的相似度。此值介於 0 與 1 之間，基本上，NC 值愈大，表示取出的浮水印與原浮水印的相似度愈高，反之愈低。NC 值的定義如公式(4)所示：

$$NC = \frac{\sum_{i=1}^{X}\sum_{j=1}^{Y} W^*_{ij}}{\sum_{i=1}^{X}\sum_{j=1}^{Y} W_{ij}} \qquad (4)$$

其中 X、Y 為圖形大小，W_{ij} 為原浮水印的總像素數目，W^*_{ij} 為還原浮水印的像素與原浮水印的像素相同數目，即像素相同之比例。

參、結果與討論

本文使用 Borland C++ Builder 6 作為程式開發軟體，首先以 436×436 大小的灰階胸腔影像當作機密影像製作分享影像，以增加傳輸安全性。繼之，以『中山醫學大學』灰階圖形當作浮水印來源，從胸腔影像中製作出數位浮水印之分享影像，可供原作者以後驗證之用。為了證實本研究所提之浮水印技術的確具有非常強韌之抗破壞效果，本文設計了一系列影像處理攻擊實驗：包括馬賽克、剪裁、變形、加入雜點、JPEG 壓縮、右旋一度、模糊化等七種破壞攻擊實驗，將遭攻擊後的數位影像進行數位浮水印的取回探討，本文並利用 NC 值來評估取出後的浮水印與原浮水印之相似程度的參考標準。

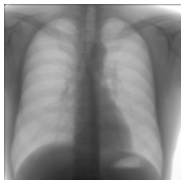

圖 20(a) 馬賽克攻擊

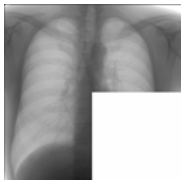

圖 21(a) 剪裁攻擊

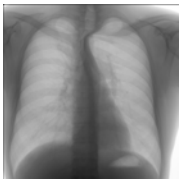

圖 22(a) 變形攻擊

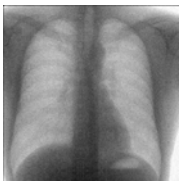

圖 23(a) 加入雜點攻擊

圖 24(a) JPEG 壓縮攻擊

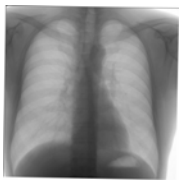

圖 25(a) 右旋一度攻擊

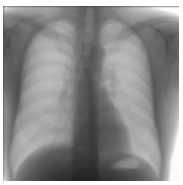

圖 26(a) 模糊攻擊

圖 20(b) 馬賽克攻擊後取出之浮水印(NC=0.9900)

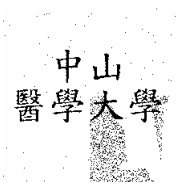

圖 21(b) 剪裁攻擊後取出之浮水印 (NC=0.9666)

圖 22(b) 變形攻擊後取出之浮水印 (NC=0.9886)

圖 23(b) 加入雜點後取出之浮水印(NC=0.9872)

圖 24(b) JPEG 壓縮後取出之浮水印(NC=0.9708)

圖 25(b) 右旋一度攻擊後取出之浮水印(NC=0.9854)

圖 26(b) 模糊攻擊後取出之浮水印(NC=0.9901)

圖 20~圖 26 之七種攻擊實做結果顯示，包含馬賽克、剪裁、變形、加入雜點、JPEG 壓縮、右旋一度、模糊等行為，取出數位浮水印的 NC 值皆高達 0.9666 ~ 0.9901 之間，成效相當優越。

另值得一提，在不做任何影像處理，直接由測試影像(如圖 13)中萃取出浮水印，如圖 19 所示。比較原始浮水印(如圖 14)及萃取出的浮水印(如圖 19)可發現所萃取出的浮水印是清晰可辨，而 NC 值＝1.0 可說明此兩張浮水印是完全相同的。在整個浮水印之製作與取出過程，對原醫療影像皆無任何破壞處理。

肆、結論

本研究利用灰階色差視覺密碼技術，首先開發適用於 DICOM 3.0 灰階醫療影像之加密保護技術，繼之提出了一種新的視覺密碼浮水印製作技術。

在加密技術方面，本研究提出 DICOM 灰階醫療影像之色差視覺加密法，各分享影像可有效的保留機密影像的訊息，被破解的機率僅為 $\frac{1}{256^{m\times n}}$，實驗結果顯示，本法不但擁有良好的隱藏性，並且本法不需擴展處理可降低在傳輸時的資料負荷，而且還原影像完全不失真等優越性。

在數位浮水印技術方面，本法比現今的浮水印技術更具以下優勢：(1) 本浮水印技術在取出浮水印時，不需要原圖的協助。(2) 本浮水印技術在加入浮水印時，完全不會破壞到原圖。(3)本浮水印技術所嵌入的浮水印資料量並無受到任何限制。(4) 本浮水印技術若不慎流失了原圖，依然具有完整的浮水印保護措施。(5) 本浮水印技術不需複雜的運算，具簡易直接的特性。在經過七種攻擊實驗，結果顯示本文之浮水印技術，可為 DICOM 灰階醫療影像之著作權保護提供另一簡易、直接且強韌有效的方法。

參考文獻

1、 侯永昌、周智倫，民91，”應用視覺密碼原理之浮水印技術”，第十三屆國際資訊管理學術研討會。

2、 侯永昌、林芳助、張兆源，民89，”以半色調技術製作彩色視覺密碼”，第十期資管評論。

3、 侯永昌、林芳助、張兆源，民88，”一種256色機密影像分享的新技術”，第九期資管評論。

4、 張真誠、黃國峰、陳同孝，2003，”電子影像技術”，台北：旗標出版股份有限公司。

5、 陳同孝、張真誠、黃國峰，2003，”數位影像處理技術”，台北：旗標出版股份有限公司。

6、 Ching-Nung Yang, “A Note on Efficient Color Visual Encryption”, Journal of Information Science and Engineefing, Vol. 18, 2002,pp.367- 372

7、 Naor. M. and A. Shamir, “Visual Cryptography”, Advances in Cryptol-ogy: Eurpocrypt’94, Springer-Verlag, Berlin, 1995, pp.1-12.

8、 NEMA Standards Publication PS3.x, “Digital Imaging and Communications in Medicine(DICOM) Part 5: Data Structures and Encoding”, National Electrical Manufactures Association, 1300 N Street, Rosslyn Virginia 22209 USA, 2003

9、 Rijmen, V. and B. Preneel, “Efficient Color Visual Encryption for Shared Colors of Benetton” Presented at urocrypto’96 Rump Session Available as http://www.iacr.org/confere

nces/ec96/rump/preneel.ps