以資訊隱藏技術作臉部影像在網路上傳輸之安全保護

吳大鈞[1,3]、李俊昇[1]、蔡文祥[2]
[1]國立高雄第一科技大學 電腦與通訊工程系
[2]國立交通大學 資訊工程學系
[3]dcwu@ccms.nkfust.edu.tw

摘要

在電子商務的應用中，以人臉佐證身份之技術日益普遍。網路購物時，即時攝取的買方臉部影像在網路上傳輸，駭客有可能會攔截、竄改影像或保留所攔截臉部影像日後再假冒交易。本論文完成三種臉部影像在網路上傳輸之不同安全保護機制，可供不同應用選擇合適的方式以保護所傳輸之臉部影像。

前兩種方法屬直接傳送影像之應用。第一種方法是以資訊隱藏技術在人臉以外的影像區域嵌入交易明細、時戳及影像之防偽訊號等資訊。當伺服器端接收到所傳送之影像時，可以由所擷取出之隱藏資訊得知交易明細，且可判斷影像之真確性及合理性。本論文提出依所隱藏資料量與臉部影像之DCT係數對影像之JPEG量化表做適應性調整之技術，以降低嵌入資訊時所造成之影像品質破壞。第二種方法是對JPEG臉部影像之DCT係數進行壓縮，在壓縮後所騰出空間嵌入欲隱藏之交易明細、時戳及防偽訊號等資訊。本方法可產生如同加密般的雜訊影像供傳送到伺服器端，因為無法直接辨識臉部原貌，所以更可達到安全傳輸之目的。本方法並可無失真地還原回未嵌入資訊前之原始臉部影像。

第三種方法屬傳送臉部特徵值之應用。本方法將特徵值、時戳、驗證真確訊號之位元資料結合，並以亂數打亂其位元次序。最後以伺服器端之公鑰進行加密後再傳送。伺服器端可用私鑰順利反向重建回原資料，並查驗其真偽及時間之合理性。

關鍵詞：臉部影像、資訊保護、資訊隱藏、資訊驗證。

Abstract

The techniques for identity recognition by using human face have become more popular in the applications of e-commerce. When a customer shops online, buyer's face image taken by a camera in real time. However, when the face image is transmitted on the network, it might be intercepted by a hacker, and modified or reserved for later use in fake transactions. In this paper, we have accomplished three distinct methods for security protection of online transmitted face images, which may be selected for different applications.

The first two methods transmit the face image directly on the network. The first method adopts information hiding techniques to embed information of the e-commerce transaction, time stamps, and authentication signals into the face image excluding its facial region. When the server receives a transmitted face image, it can then extract not only the information of the transaction but also judge the reasonableness and truthfulness of the image. In this paper, we adopt an adaptive JPEG quantization table which decided by the embedded data size and the DCT coefficients of the face image in order to decrease the influence of image quality caused by the embedding steps. The second method compresses the DCT coefficients of the JPEG face image. After compressing, we can obtain space for embedding information of the e-commerce transaction, time stamps, and authentication signals. This method produces a noise like image which is then transmitted to the server. Because the face is not exposed during

the transmission process, this method can achieve additional degree of security. At the receiver end, the original face can be reconstructed by a reversible process.

The third method is for the applications of transmitting biofeatures of the face image. The features are first mixed with the time stamp and the authentication signal of the face image, then randomized in order, and finally encrypted with a public key of server before being transmitted to the receiver. The server at the receiver end then reconstructs the original data in a reverse order with a private key, and checks the truthfulness and reasonableness of the result.

Keywords: face images, data protection, information hiding, data authentication.

壹、研究背景及目的

隨著網路普及與科技進步，越來越多資訊在網路上快速傳播。網站購物[1]是快速崛起之新穎商業模式，其交易金額與日俱增。傳統的個人密碼，已難以確保認證之安全性。反之，利用生物特徵如臉部特徵、指紋、掌紋、聲音與虹膜[2]等，由於具有個人獨特性、難以複製，成為解決安全認證問題之一新途徑。以人臉辨識技術[3-6]結合密碼，因可記錄臉面以提供伺服器查核之用，可更確保上網交易之安全性。駭客或密碼偷竊者因無法通過人臉驗證，便無法進行網上假冒交易。

一般來說，人臉辨識技術主要是利用人的臉部特徵作為識別身份的生物認證技術。人臉影像是透過數位相機或網路相機擷取，將所攝取之臉部影像，與人臉資料庫中之臉部資料樣本比對，以確認身份。網路購物交易時，買方所攝取臉部影像尚需經過網路傳輸至賣方或公正認證中心以進行身份確認，所傳送之資料有可能是所攝取之臉部影像或是由臉部影像中抽取之臉部特徵值，如輪廓、眼、鼻、嘴等。接收方再將所收到之資料與人臉資料庫中之資料進行比對，以即時確認身份。當買方臉部影像或特徵值在網路上傳輸時，駭客有可能會攔截竄改資料或保留所攔截相關資料，以供日後進行假冒交易使用。

本論文已完成開發三種臉部影像在網路上傳輸之不同安全保護機制，可供在不同應用情境下保護所傳輸之影像或特徵值之用。本論文以資訊隱藏技術[7-12]在臉部影像中嵌入交易資訊、時戳(time stamp)及驗證訊號。當伺服器端收到所傳送之資料時可以判斷資料有無被竄改，即驗證真確性。並且比對所擷取出之時戳與接收到資料之時間間隔之合理性，以查驗是否有假冒交易之可能。

第一種方法是在所攝取的臉部影像中嵌入交易資訊、時戳、人臉座標相關資訊及驗證訊號，再傳送至伺服器以供查驗。當伺服器端接收到所傳送之影像時，不但可以判斷影像及交易資訊之真確性，且由所擷取出之時戳可判斷其合理性。人臉是識別身份之重要依據，本方法將欲隱藏資訊嵌入於人臉以外之影像區域，以免破壞人臉部份之影像品質。第二種方法是將所攝取之買家影像打亂成如加密般的雜訊影像，再傳送至伺服器以供查驗。本方法對影像之 DCT 係數值進行無失真壓縮，並利用壓縮後所剩餘的空間嵌入交易資訊、時戳及相關驗證訊號。本方法除了能驗證臉部影像真偽及時間合理性外，因為在傳送時無法一窺臉部原貌，所以更具安全性。本方法可無失真地還原回原始臉部。第三種方法是對所攝取的買家影像直接進行臉部特徵抽取，將臉部特徵值、交易資訊、時戳及驗證訊號之位元資料結合，以伺服器端之公鑰進行加密後再傳送。伺服器端可用私鑰順利反向重建回原始資料，並查驗其真偽及時間之合理性。

本論文所採用之嵌入技術與 JPEG 影像格式習習相關，所以在第貳節中介紹 JPEG 影像壓縮之部份原理及相關資訊隱藏技術，在第參節中將探討所提出之以資訊隱藏技術傳送臉部影像之安全保護技術，第肆節將說明所提出以資訊隱藏技術傳送雜訊影像之安全保護技術，第伍節將介紹傳送影像特徵值之安全保護技術。本論文之實驗結果及討論

將在第陸節中呈現。

貳、JPEG 影像壓縮原理及相關資訊隱藏技術

2.1 JPEG 影像壓縮原理簡介

JPEG[13]是一種靜態影像壓縮方法，屬有損壓縮(lossy compression)，也就是影像經編、解碼後與原影像會有差異。因其差異難以肉眼觀察且壓縮效果良好，因此被廣為使用。圖 1 為 JPEG 壓縮流程，包括離散餘弦轉換(Discrete Cosine Transform; DCT)、量化(quantization)及熵編碼(entropy coding)。

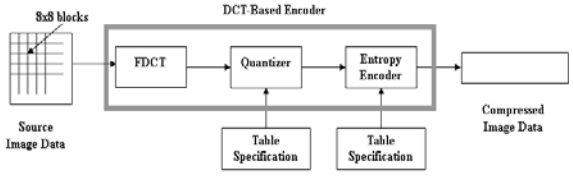

圖 1：JPEG 影像檔壓縮流程。

將影像資料分割成 8×8 的區塊，各區塊經 DCT 轉換後產生 64 個 DCT 係數，包括一個 DC 係數及 63 個 AC 係數。接下來進行量化，其目的是使係數值變小，更利後續的編碼動作。量化的過程是將所有 DCT 係數與一個 64 個量化值的量化表做一對一相對應的除法運算，除完後將商數四捨五入取整數。DC 係數使用脈差調變編碼(Differential Pulse Code Modulation；DPCM)及霍夫曼編碼(Huffman coding)。DPCM 主要是將目前區塊的 DC 值減去前一個區塊的 DC 值。AC 係數則以 zigzag 順序，使用長度變動編碼(Run Length coding)及霍夫曼編碼。Zigzag 掃瞄是將區塊的 AC 係數轉成一維係數陣列，再做長度變動編碼，以<Run, Level>形式呈現。Run 表示在一維陣列中，在非零元素之前所出現零的個數。Level 表示該非零元素之值。此一維陣列中最後一個非零元素後面的係數都是零，記錄成<EOB>，EOB 為 End Of Block 之意。

2.2 資訊隱藏簡介

在影像中隱藏資訊，可用來達到資訊安全保護或秘密通訊的目的。以下針對不同應用列出相關說明:

(1) 版權保護：此類應用係隱藏與版權資訊有關的訊號，如序號、擁有者名稱等，以分辨出影像提供者及授權者資訊。版權資訊很重要，即使影像被很嚴重破壞或被裁剪掉一大部分，仍希望能保有完整之資訊，所以這類應用所隱藏的訊號一般稱為強韌浮水印(robust watermarks)。一般所謂的數位浮水印[14][15](digital watermarks)即指此類應用之浮水印訊號。

(2) 註解資訊隱藏：此類應用隱藏與影像有關的資訊，如標題、簡短說明、時戳等，以讓影像能夾帶與其相關的資訊，避免在傳輸過程或資料移轉時流失資訊或誤植。

(3) 完整性驗證：此類應用之目的是建立驗證影像有無被竄改(tamper-proofing)的機制。任何影像的修改都能藉此機制偵測出。此類應用所隱藏於影像之訊號一般稱為易碎浮水印(fragile watermarks)。

2.3 嵌入技術簡介

在影像中嵌入資訊之技術可分成兩大類：空間域(spatial domain)之技術及頻率域(frequency domain)之技術。在空間域嵌入資訊之技術，一般是以修改或調整影像之像素值來達到資訊嵌入之目的。最廣為人知的為最低位元嵌入技術(least significant bit embedding)。頻率域之嵌入技術，包括離散小波轉換(Discrete Wavelet Transform; DWT)[16]、離散傅立葉轉換(Discrete Fourier Transform; DFT)[16]、離散餘弦轉換(DCT)[16]之嵌入技術等。這些類技術一般是以修改或調整適當的頻率係來達到資訊嵌入的目的。Upham提出JPEG影像之隱藏技術[17]，將訊息嵌入在AC係數之LSB中；Westfeld提出了運用矩陣編碼(matrix encoding)的技術[7]，有效的減少對影像的修改量，以提升

嵌入之效率；張真誠等人[8]將標準量化表之部份量化值改為1，將資訊嵌入在影像區塊之中頻位置，以降低嵌入資訊時對影像所造成的破壞。

在影像中嵌入資訊會造成遮蔽影像(cover-image)品質的破壞，倘若沒有特別設計，所造成的失真是沒有辦法還原的。然而，在一些如天文、醫學、軍事等特定的應用，在擷取出所嵌入資訊時也要能無失真的還原遮蔽影像是有其必要性，因此無失真資訊隱藏(lossless data hiding)也成為近年熱門的研究[18]。

參、以資訊隱藏技術傳送臉部影像之安全保護技術

本論文所提之第一種方法是直接傳送人眼可辨識之買家影像至伺服器以供查驗。在所傳送影像中，人臉是用來識別身份之重要依據，本方法將欲隱藏資訊嵌入於人臉以外之影像區塊，以免破壞人臉部份之影像品質。

本嵌入技術直接對 JPEG 影像之量化 DCT 係數運作。若攝取之影像格式為 JPEG 檔，則對 JPEG 影像檔做熵解碼以取得該影像之量化表與各量化 DCT 係數；若影像為其他檔案格式，則需先將其轉換成 JPEG 影像之中間格式，以得到量化表及各量化 DCT 係數。首先對影像進行色相轉換，由 RGB 色彩模式轉換成 YCbCr 模式。接著將影像切割成不重疊之 8×8 區塊，分別對每個區塊做離散餘弦轉換(Forward Discrete Cosine Transform; FDCT)。每個區塊各可得到 64 個 DCT 係數值。將這些係數值分別除以自訂之量化表或標準量化表中之相對應量化值後，再將所得商值四捨五入就得到所需之量化 DCT 係數。確定量化表及各量化 DCT 係數後，將每個區塊內之量化 DCT 係數值再分別乘以量化表中相對應之量化值，便得到量化還原 DCT 係數值。

以人臉偵測技術找尋臉部位置，將臉部所在之所有 8×8 區塊標出，令人臉區塊為 F_i，i=1, 2, …, m，m 為人臉區塊總數。本方法並找出能包含這些區塊之最小長方形區域，視為人臉區域。記錄此區域之左上角與右下角座標。人臉區域以外之非人臉區塊將用來嵌入資訊。令非人臉區塊為 D_i，i=1, 2, …, n，n 為非人臉區塊總數。令某非人臉區塊 D_d 之 64 個量化還原 DCT 係數，依 zigzag 順序分別為 $z_d(i)$，i=0, 1, …, 63。令 $z_d(\beta_d)$ 為 D_d 依 zigzag 順序之最後一個非零係數，換言之 $z_d(\beta_d+1)$, $z_d(\beta_d+2)$, ..., $z_d(63)$ 之係數值均為 0。本方法在 $z_d(\beta_d)$ 之前的 AC 係數中嵌入資訊，每個係數將嵌入 2 個位元資料於其最低之兩個位元中。本方法先依據欲嵌入資訊總位元數與 β_i，i=1, 2, …, n，計算出一合適之 α 值，以便足夠嵌入所欲嵌入之全部資料(於後段詳述)。以 D_d 為例，若 $\alpha < \beta_d$，則資料將可嵌在 $z_d(\alpha)$ 至 $z_d(\beta_d-1)$ 間之係數值；若 $\alpha \geq \beta_d$，則 D_d 中將不會嵌入任何資訊。

令量化表中之量化值依 zigzag 順序分別為 $q(i)$，i=0, 1, …, 63。將 $q(\alpha)$ 到 $q(63)$ 均設為 1，若 $q(\alpha-1)$ 為 1，也將 $q(\alpha-1)$ 改設為 2。再將影像中所有區塊之各 DCT 係數分別除以此新量化表中相對應之量化值，各得到新的量化 DCT 係數。

將檔頭識別訊號及人臉區之座標值位元資訊，先嵌入於影像區塊中，此嵌入步驟使用區塊是依掃描順序由左而右、由上而下，不論區塊是屬於人臉區域或非人臉區域，直到嵌入完畢為止。嵌入方法類似先前所述嵌入資訊之方式：以區塊 b 為例，$z_b(\beta_b)$ 為依 zigzag 順序，最後一個非零係數。若 $\alpha < \beta_b$，則在 $z_b(\alpha)$ 至 $z_b(\beta_b-1)$ 間所有係數以置換方式各嵌入 2 個位元資訊於係數值中；若 $\alpha \geq \beta_b$，則不嵌入任何資訊。

透過雜湊函數(hash function) h_1 以每個非人臉區塊 D_i (i=1, 2, …, n，n 為非人臉區塊總數)之量化 DCT 係數計算出 k 位元的雜湊值做為 D_i 之驗證訊號，共可得到總長度為 $n \cdot k$ 位元之二元驗證串列 P。由於非人臉區塊之量化 DCT 係數稍後會嵌入資訊於其最低 2 個位元中，所以計算雜湊值時要將各量化 DCT 係數值之最低 2 個位元忽略不計。至於人臉區域，本方法透過雜湊函數 h_2 以每個人臉區塊之量化 DCT 係數計算出 l 個位元的雜湊值做為驗證訊號，共可得到總長度為 $m \cdot l$ 的二元驗證串

列 Q。將交易相關資訊透過雜湊函數 h_3 計算交易資訊的雜湊值，得到長度為 r 的二元驗證串列 R。所以除了先前已嵌入之檔頭識別訊號及人臉區域的座標值位元資訊，尚需在非人臉區域嵌入之資訊為交易資訊、時戳與 P、Q、R 三種驗證串列。

依掃描順序對各非人臉區塊(需扣除先前已於嵌入檔頭識別等訊號之區塊)依先前所述之方法逐一嵌入所有資訊，直到完全嵌入完畢為止。最後透過熵編碼，以各量化 DCT 係數及量化表編碼成 JPEG 影像檔案，傳送到伺服器端。

肆、以資訊隱藏技術傳送雜訊影像之安全保護技術

本方法將所攝取之買家影像製作成如加密般的雜訊影像，再傳送至伺服器以供查驗。本方法對 DCT 係數值進行無失真壓縮，並利用壓縮後所剩餘的空間嵌入欲隱藏資訊，可達到無失真還原回原始臉部影像的需求。

本嵌入技術直接在 JPEG 影像之量化 DCT 係數運作。若攝取之影像格式為 JPEG 檔，則對 JPEG 影像檔做熵解碼以取得該影像之量化表與各量化 DCT 係數；若為其他影像檔案格式，則需先將其轉換成 JPEG 影像之中間格式，方法與前節相同，再此不再贅述。每個區塊各可得到 64 個 DCT 係數值，將這些係數值分別除以自訂之量化表或標準量化表中之相對應量化值，將所得之商四捨五入就得到所需之量化 DCT 係數。量化表之量化值為正整數，最小值為 1。JPEG 壓縮方法使用之量化 DCT 係數之編碼表的可編碼範圍在 $-1023 \sim 1023$ 之間，也就是各量化 DCT 係數在此範圍內均屬合理。但在量化步驟時，若 DCT 係數要除以之量化表之相對應量化值大於 1，得到的 DCT 量化係數值之合理範圍也會相對變小。而 DCT 係數值分佈有集中於零軸的特性[19]，若對其進行無失真壓縮，再將壓縮後之值放回原存放係數之位元空間，所剩餘之空間即可供本方法隱藏資訊之用。

影像各 8×8 區塊之相同位置的 DCT 係數會以相同量化值進行量化，所以相同位置的量化係數值合理範圍會一致。令 $-r\sim r$ 為某位置之量化係數值合理範圍，本方法為該位置之量化係數找尋滿足 $2^{b-1} \le r$ 條件之最大整數 b。則可以用 b 個位元之任意整數來做為該位置量化係數之新值。因為 b 個位元的整數可表示範圍為 $-2^{b-1} \sim 2^{b-1}-1$，仍不會超出其合理範圍 $-r\sim r$ 區間。換言之，該位置 DCT 量化係數可嵌入之位元數為 b。令影像區塊之 DCT 量化係數之位置，依 zigzag 順序分別為 $z(j)$，j=0, 1, …, 63，則任一區塊在位置 $z(j)$ 之可嵌入位元數為 $b(j)$，$b(j)=\left\lfloor \log_2 round\left(\frac{1023}{q(j)}\right)+1 \right\rfloor$，其中 $q(j)$ 為量化表中相對位置之量化值。

本方法使用無失真壓縮技術將整張影像之量化 DCT 係數值壓縮，形成位元串列 T。將交易資訊透過雜湊函數 h_1 計算出長度為 p 的二元驗證串列 P。全部欲嵌入資訊 S 包括檔案識別訊號、交易資訊、時戳、T、P 等一般性資訊以及最後會為每個區塊所嵌入一般性資訊而分別產生之驗證訊號。令 S 之總位元長度為 s。本方法先根據 s 及各位置量化係數之可嵌入位元數，找出滿足 $s \le \sum_{i=1}^{n}\sum_{j=0}^{r} b_i(j)$ 條件之最小整數值 r，以便足夠將所有資料全部嵌入影像各區塊之 $z(0)$ 至 $z(r)$ 係數間，其中 n 為區塊總數，$b_i(j)$ 為區塊 b_i 之 $z(i)$ 係數。整張影像可供嵌入位元總數為 $\sum_{i=1}^{n}\sum_{j=0}^{r} b_i(j)$，本方法以亂數產生器產生位元長度為 $(\sum_{i=1}^{n}\sum_{j=0}^{r} b_i(j))-s$ 之二元串列串接在 S 之後成為 S'，S' 位元長度即為 $\sum_{i=1}^{n}\sum_{j=0}^{r} b_i(j)$。這樣每個區塊均可嵌入 S' 中之 $\sum_{j=0}^{r} b(j)$ 個位元資訊，其中包括 $(\sum_{j=0}^{r} b(j))-k$ 位元的一般性資訊 X 與以雜湊函數 h_2 所產生之長度為 k 之 X 的驗證資訊。再根據已計算出之各量化係數位置之可嵌入位元數，將資料

嵌入各區塊之 $z(0)$ 至 $z(r)$ 係數內。最後透過熵編碼，將各量化 DCT 係數編碼成加密般的 JPEG 雜訊影像，傳送到伺服器端。

伍、傳送影像特徵值之安全保護技術

本方法對所攝取的買家影像進行臉部特徵抽取，將所抽取出的臉部特徵值傳送至伺服器以供查驗。由於臉部特徵值所佔的記憶體空間遠小於所攝取臉部影像所需之記憶體空間。所以可以降低傳輸之資料量，也分擔了伺服器在確認買家身份時抽取臉部特徵之工作負擔，加快反應時間。

對買家影像進行臉部特徵抽取，取得臉部特徵值 f_i ，i=1, 2, …, n，其中 n 為特徵值個數，將特徵值、交易資訊及時戳透過雜湊函數 h 計算其摘要。利用伺服器之公鑰分別對臉部特徵值、交易資訊、時戳及摘要以 RSA 非對稱式加密演算法加密[19]。最後將加密過後的資料傳送至伺服器端。

陸、實驗結果與討論

本節將介紹本論文所提出之以資訊隱藏技術傳送臉部影像、以資訊隱藏技術傳送雜訊影像及傳送影像特徵值之三種安全保護技術之實驗結果與討論。

6.1 以資訊隱藏技術傳送臉部影像

圖 2 為實驗所使用之 320×240 之 JPEG 影像，其使用之量化表為標準量化表。嵌入之總資訊量為 7030bits，圖 3 為嵌入資訊後之結果影像，PSNR 為 54.91dB，影像品質相當好。圖 4 為將圖 3 眼睛周圍竄改之影像，本方法可驗證出影像是否遭受到竄改並標示出遭受到竄改的部份(圖 5)，黑色區塊為遭受到竄改的區域。

6.2 以資訊隱藏技術傳送雜訊影像

圖 6 為圖 2 以本方法嵌入資訊所產生如同加密般之雜訊影像。倘若駭客攔截並竄改影像(圖 7)，本方法亦可偵測並以黑色標示出遭受到竄改的區塊(圖 8)。

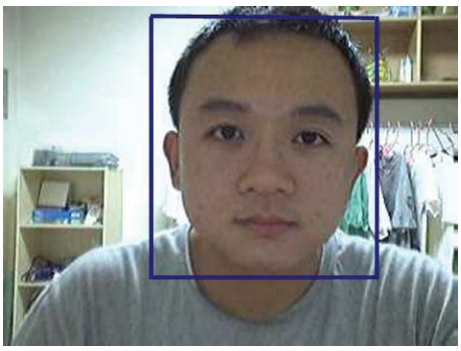

圖 2：原始臉部影像及所偵測出之臉部區域。

圖 3：使用方法一嵌入資訊於圖 2 之結果影像。

圖 4：圖 3 經竄改後之影像。

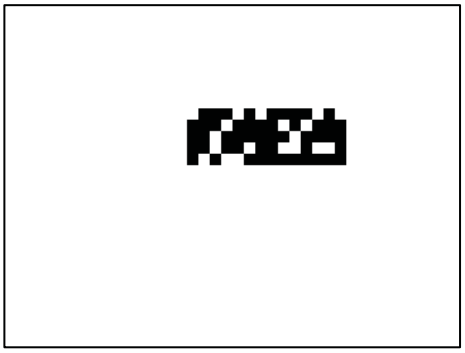

圖 5:圖 4 之竄改偵測結果。

6.3 傳送影像特徵值

本方法直接抽取圖 2 之人臉特徵，將特徵資訊量為 526 位元之人臉特徵、交易資訊及時戳經由雜湊函數進行運算，得到一個長度為 160 位元的雜湊值。再將特徵值、交易資訊、時戳及雜湊值結合，利用伺服器之公鑰透過非對稱式加密演算法對資料加密，將加密過後的資料傳送至伺服器端。倘若駭客攔截此資料並試圖解密，由於駭客並沒有伺服器之私鑰所以無法順利解開資料。若駭客竄改資料，伺服器可利用解密後的資料再透過雜湊函數計算出雜湊值，與解密後的雜湊值相互比對，即可判定資料是否有遭受到竄改。

6.4 討論

本論文所提出的三種臉部影像在網路上傳輸之安全保護技術，能正確判斷影像或資料是否遭受竄改及那些區域遭受竄改。但是若影像遭受到非惡意性修改，如失真性壓縮、影像縮放等，所嵌入之交易資訊也很容易被破壞。因此如何在人臉影像中同時加入易碎浮水印(fragile watermarks)與半易碎浮水印(semi-fragile watermarks)又同時保持影像之品質，為未來之研究目標之一。

致謝

本研究之部分經費由國科會資助，計畫代號為 NSC95-2745-P-327-00。

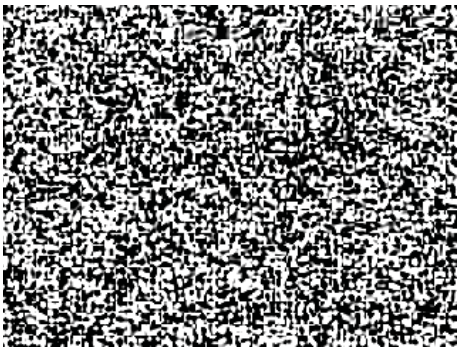

圖 6：圖 2 使用方法二嵌入資訊產生之雜訊影像。

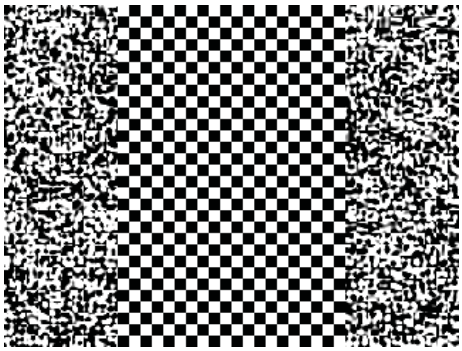

圖 7：圖 6 經竄改後之影像。

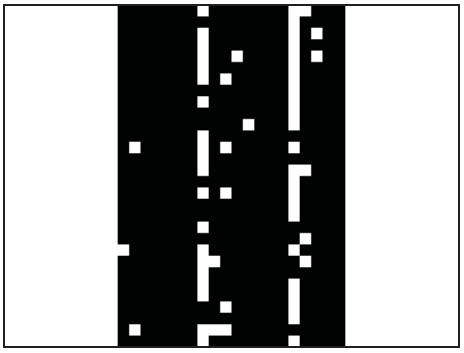

圖 8：圖 6 之竄改偵測結果。

參考文獻

[1] R.C. Marchany, J. G. Tront, “E-commerce security issues,” *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, pp. 2500-2508, Jan 2002.

[2] Kroeker, K.L., “Graphics and Security: Exploring Visual Biometrics,” *IEEE Computer Graphics and Applications*, vol. 22, pp. 16-21, July-Aug. 2002.

[3] Pentland and T. Choudhury, “Face Recognition for Smart Environments,” *IEEE Computer*, pp. 50-55, 2000.

[4] A.V. Nefian and M. H. H III, “Face Detection and Recognition Using Hidden Markov Models,” *Proc. IEEE Int’l Conf. Image Processing*, vol. 1, pp. 141-145, 1998.

[5] S.-H. Lin, S.-Y. Kung, and L.-J. Lin, “Face Recognition/Detection by Probabilistic Decision-Based Neural Network,” *IEEE Trans.*

Neural Networks, vol. 8, no. 1, pp. 114-132, 1997.

[6] K.W. Bowyer, K. Chang, and P. Flynn, "A Survey of Approaches to Three-Dimensional Face Recognition," *Proc. 17th Int'l Conf. Pattern Recognition*, pp. 358-361, 2004.

[7] A. Westfeld, F5 - A Steganographic Algorithm High Capacity Despite Better Steganalysis, *Proc. 4th International Workshop on Information Hiding*, Pittsburgh, PA, USA, pp. 289-302, 2001.

[8] Chang, C. C., Chen, T. S., and Chung, L. Z. (2002), "A Steganographic Method Based upon JPEG and Quantization Table Modification," *Information Sciences*, pp. 123-138.

[9] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography," *IEEE Trans. Security & Privacy Magazine*, vol. 1, no. 3, pp. 32-44, 2003.

[10] C. H. Tzeng and W. H. Tsai, "Hiding binary images behind noise with authentication capability: a new approach to covert communication," *2003 International Carnahan Conference on Security Techonology*, Taipei, Taiwan, R. O. C., 2003.

[11] C. T. Hsu and J. L. Wu, "DCT-Based watermarking for video," *IEEE Transactions on Image Processing*, vol. 8, pp. 58-68, 1999.

[12] I. J. Cox, J. Kilian, T. Leighton, and T. Shammoon, "**S**ecure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-87, 1997.

[13] G. K. Wallace, "The JPEG Still Picture Compression Standard," *IEEE Transactions on Consumer Electronics*, vol. 38, no. 1, February 1992.

[14] Saraju P. Mohanty, "Digital Watermarking: A Tutorial Review," http://citeseer.ist.psu.edu/mohanty99digital.htm .

[15] D. C. Wu and W. H. Tsai, "Spatial-domain Image Hiding Using Image Differencing," *IEE Proceedings-Vision, Image and Signal Processing*, vol. 147, no. 1, pp. 29-37, 2000.

[16] J.L. Dugelay and S. Roche, *Information hiding techniques for steganography and digital watermarking*, Artech House, Norwood, 2000.

[17] Derek Upham, 1999, "Jsteg Steganographic Algorithm", Available: ftp://ftp.funet.fi/pub/crypt/steganography.

[18] Y. Q. Shi, Z. Ni, D. Zou, C. Liang and G. Xuan, "Lossless data hiding: Fundamentals, algorithms and applications," *Proceedings of IEEE International Symposium on Circuits and Systems* (ISCAS04), vol. II, pp. 33-36, Vancouver, Canada, May 2004.

[19] Edmud Y. Lam, Joseph W. Goodman, "A Mathematical Analysis of the DCT Coefficient Distributions for Imges," *IEEE Transactions on Image Processing*, vol. 9, Issue 10, pp. 1661-1666, Oct. 2000.