運用群聚交集特性為基礎之影像驗證技術

吳汶涓 [1*]、許懷方 [2]
[1,2] 真理大學 資訊工程學系
[1] au4387@au.edu.tw、[2]fm030110@au.edu.tw

摘要

雲端檔案服務改變數位資料儲存的方式，使得擁有者只要將檔案資料上傳至雲端，即能同步到所有電腦，讓管理更加方便且更有效率，但其資料傳送及儲存之安全性備受關注。本篇論文針對影像資料提出一種數位影像驗證技術，主要用以偵測數位影像是否曾於傳送或儲存階段遭受惡意或不法之竄改，並進而針對這些疑似竄改區域加以復原，儘量恢復原本資料的樣貌。本篇論文將利用向量量化編碼技術來取得影像資料重要的驗證資訊，並進一步地運用區塊群聚交集特性來改善竄改誤判的情況與提升復原後的影像品質。從實驗結果顯示出本篇方法在相同竄改量之下，相較於其他先前方法有較精準的錯誤偵測能力以及較高品質的影像復原能力。

關鍵詞：影像驗證、竄改偵測、資料回復、向量量化編碼、交集運算

An Improved Image Authentication Scheme using Grouped Intersection Property

Wen-Chuan Wu[1*], Huai-Fan Hsu[2]
[1,2]Dept. of Computer Science and Information Engineering, Aletheia University
[1]au4387@au.edu.tw, [2]fm030110@au.edu.tw

Abstract

Cloud service changes the way of digital data storage. As long as the data owner uploads digital file to the cloud, these data will be synchronized between all computer devices. It makes management easier and more efficient. However, data security during transmission and storage is one of the biggest concerns for the data owner. This paper proposes an image authentication scheme to detect whether an image has been illegally tampered with or not and to recover these suspected tampered regions into their original states. This paper utilizes the property of grouped block intersection to avoid possibly detected misjudgments and enhance the restored image quality. According to experimental results, the proposed scheme is indeed superior to other earlier works in terms of accurate detection and high-quality data recovery.

* 通訊作者 (Corresponding author.)

Keywords: Image authentication, tamper detection, data recovery, vector quantization, intersection set

壹、前言

隨著現代科技快速的發展、3C 產品的普及，人們普遍使用網路來傳輸數位影像至雲端檔案服務或是將其分享給他人，而在現今軟體技術越來越便利以及越來越簡單使用的同時，就算不是專業人士也能輕易地利用影像相關軟體將數位影像做編修，再將修圖後的影像傳輸給他人或是作為自己的圖像公開分享於網路上；但當有心人士擷取到他人分享在網路上的數位影像，並利用這些軟體來進行竄改進而盜用，這樣的行為將會造成影像擁有者的權益受損，同時增加影像在傳輸及儲存的不安全性。若接收者沒有對影像做驗證動作，可能無法得知影像的完整度以及可信度。而影像驗證的技術便是用於防止數位影像於傳輸時遭受到他人的惡意竄改，並進而保護影像內容的完整性[4]，當該數位影像遭受到惡意攻擊時，此項技術能夠將被竄改的位置標示出來，此稱為竄改偵測能力(Tamper Detection)，隨著這項技術的發展以及改良，有些方法甚至能更進一步的將竄改區域的內容還原回未遭受到竄改時的狀態，此稱為資料還原能力(Data Recovery)[10]。

影像驗證技術大致可分為主動防偽驗證與被動防偽驗證兩大分支[3]。主動防偽驗證[10]的做法是資料擁有者在影像未被竄改之前先對影像進行的防範措施，當影像被竄改後使用的驗證碼將會不同，便可用此來判定疑似被竄改的位置;而被動的防偽驗證[2]則是不需要借助事前進行特殊的處理，反倒是透過檢查數位影像生成時的故有特性或是影像內容來判定是否遭受變更。而主動驗證技術又可依執行的方法再細分為數位簽章技術(Digital Signature)[1][7]及數位浮水印技術(Digital Watermark)[4][6]，前者是使用密碼學之公開金鑰加密系統對影像的特徵資訊作數位簽章處理，並將該簽章視為訊息認證碼(Message Authentication Code, MAC)額外儲存起來，以作為之後驗證比對的依據，雖然會浪費額外的硬體空間來儲放認證碼，但其優點是不需要更動原始影像的內容;後者則是將浮水印圖樣鑲嵌至影像之中，偵測時再提取出浮水印並判斷其完整性即可，此種技術又稱之為脆弱型浮水印(Fragile Watermarking)，其優點在於毋須額外儲存資訊，但由於需要將浮水印鑲嵌至影像中，故會破壞原始影像的影像品質。

於 1995 年，Walton 提出最早的影像竄改偵測技術，即為 LSB Flipping Method[8]，它主要利用總和檢查法(Checksum)計算出每個像素前七個位元的認證資料，並將其藏匿於影像像素的最低位元(LSB)之中。Walton 的方法非常容易驗證，只需檢查 Checksum 值與剛嵌入的資訊是否相同即可，但它並沒有提供任何安全機制，竄改者可以在不改變 LSB 的情況下，巧妙地竄改這張影像讓 Checksum 值保持不變。Wong 等學者[9]提出一種植基於區塊式之易脆型浮水印驗證技術，它利用密碼學的 MD5 雜湊函數解決上述 Walton 方法之缺點，提供了更安全的影像保護機制。於 2010 年後，陸續有學者皆採用

向量量化編碼法(Vector Quantization)來執行竄改偵測，向量量化編碼法是一種有失真的壓縮方法[5]，以編碼簿(Codebook)的索引值來取代原本區塊內的像素值，以達到壓縮的效果。Yang 和 Shen[12]不僅將每個影像區塊的 VQ 索引值視為該影像的重要還原資訊，藏匿於像素的 LSB 位元，還利用浮水印資訊作為影像的認證資料；Chuang 等學者[4]亦運用影像區塊的 VQ 資訊來作為認證資料，但在方法中他們將區塊索引值做多份藏匿，主要用意是減少區塊誤判的可能性並且提高還原後的影像品質;Wu 等學者[11]則利用每個區塊最像與最不相像 VQ 索引值的差值作為認證碼，而且為了還原目的，其最像的 VQ 索引值則被視為還原資訊。

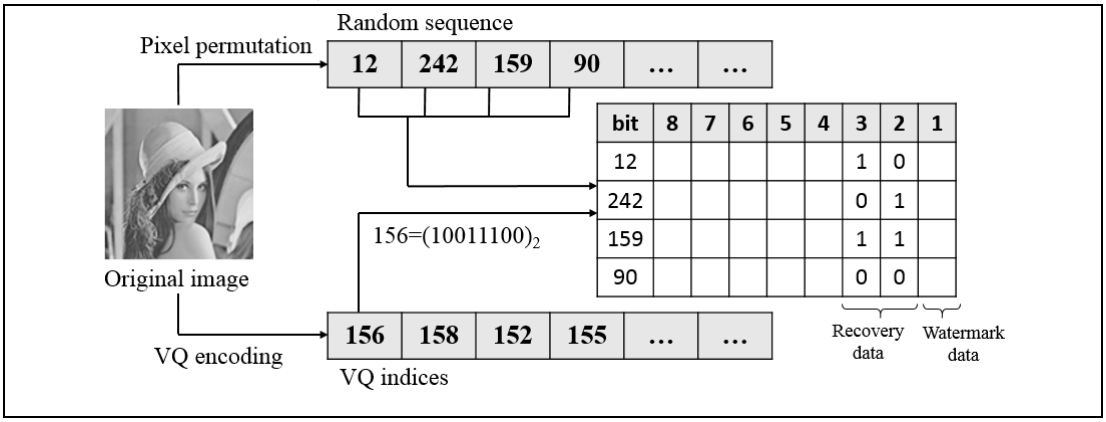
在這篇論文中，我們亦提出一個植基於 VQ 編碼技術的數位影像主動驗證方法，其主要採用區塊群聚交集(Intersection Sets)的方式來擷取驗證碼，用以改善 Wu 等學者方法[11]之竄改誤判情況以及 Yang 和 Shen 方法[12]之影像品質低落狀況。首先，原始影像每個像素的最後一個位元清空，再利用 VQ 壓縮產生體積較小的索引表，此 VQ 索引表進行區域群聚處理得到一個八位元的區域認證碼，並將該認證碼藏匿於影像像素的最後位元中，當在竄改偵測時，可利用這些區域的交集運算得知到底是哪一個索引值出錯，以提升竄改偵測的準確度。第二節將會詳細介紹兩篇使用 VQ 編碼技術的影像驗證方法之做法，接下來，在第三節則會解釋我們提出的驗證方法，裡面包含認證資料的產生與嵌入程序、竄改偵測與資料復原之程序，而第四節的實驗結果將會展現我們所提方法與其他方法相比的優勢，最後第五節則為此篇論文的結論。

貳、文獻探討

2.1 Yang 和 Shen 方法

於 2010 年，Yang 和 Shen 提出一篇植基於向量量化編碼法的影像認證技術[12]，這項技術使用向量量化編碼方法的壓縮結果作為影像重要的還原資訊，並將此還原資訊和認證用的浮水印藏匿於該影像之中。首先，將一張灰階影像的每個像素值最不重要的後三個位元清空，接著，將影像切成大小為 $w \times h$ 不重疊的區塊，針對這些影像區塊分別進行向量量化編碼處理，每個區塊會得到一個 VQ 索引值，此索引值是在 VQ 編碼簿中與該區塊內容極為相似的編碼字編號，因此有能力作為該區塊未來的還原資訊。為了驗證與還原資料的安全性，Yang 和 Shen 使用亂數序列來打亂資訊藏匿的順序，將各區塊的索引值藏匿於其他像素值的位元內。以圖一為例，假設第一個區塊索引值為 156，其值的二進位表示為$(10011100)_2$，這八個位元將依序藏匿於打亂後的像素值 12, 242, 159 和 90 中，每個像素值能夠背負兩個索引位元並藏匿於最不重要的第二個和第三個位元，其餘索引值也是如此操作。這裡，Yang 和 Shen 方法有足夠空間能夠藏匿 t 份的索引值拷貝，t 為 $2\times w\times h / \log_2|N|$，其中 N 為 VQ 編碼簿內編碼字的數量。最後，再使用 Wong

等學者[9]所提出的浮水印方法來將認證浮水印藏匿於像素值最不重要的第一個位元中，即可產生一個認證影像。



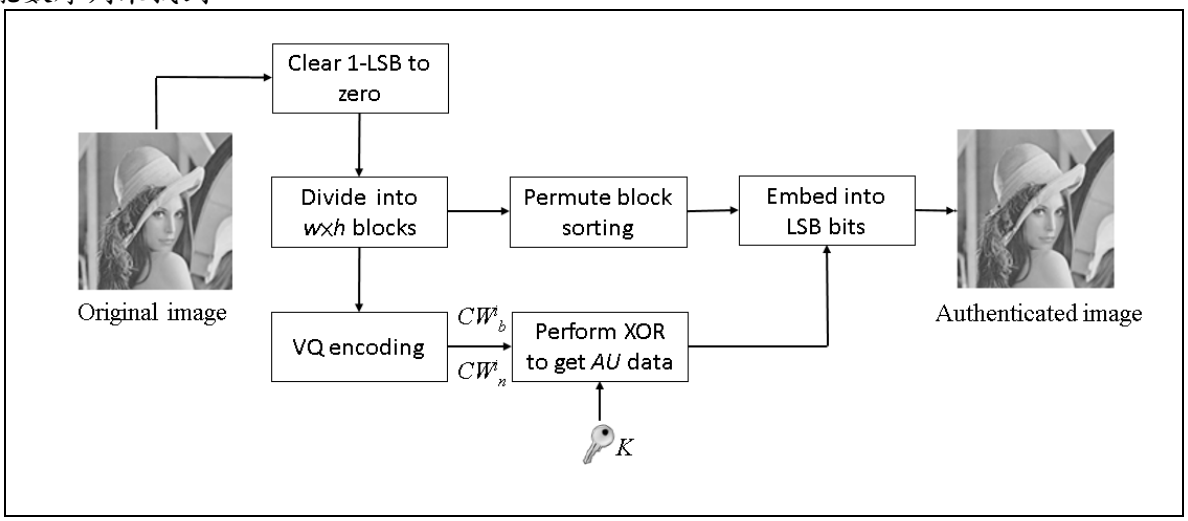
圖一：Yang 和 Shen 方法的認證嵌入流程圖

當進行影像竄改偵測及還原程序時，首先使用相同的亂數金鑰來打亂影像像素值，接著分別擷取出像素值最不重要的第一個位元和第二、第三個位元，同時間對未打亂前的影像執行每個像素最不重要的後三個位元清空，再針對清空後的結果作 Wong 方法的浮水印擷取動作，最後比對擷取出的浮水印與原始浮水印資訊是否一致，若是相同，則代表該影像區塊未曾被修改；否則，代表該影像區塊恐曾遭到不法竄改，需再從第二、第三位元蒐集的資訊中取出該區塊事先藏匿的索引值，接著利用此索引值與 VQ 編碼簿還原該區塊的內容，由於 VQ 編碼操作是屬失真壓縮，故還原後的影像區塊僅極相似於先前的區塊內容，無法還原一模一樣的像素資訊。藏匿的索引值位元仍可能因惡意竄改而導致遺失或錯誤，因此作者打算透過 t 份索引值拷貝的藏匿來提高影像還原的效果，不過，此方法仍有其他缺失，也就是需要原始浮水印才能偵測影像的完整性，進而執行影像復原的處理；而且，三個像素位元的藏匿量使得認證影像的品質受到極度的影響與破壞。

2.2 Wu 等學者的方法

於 2015 年，Wu 等學者亦提出一個植基於向量量化編碼法的影像認證技術[11]，其方法雷同 Yang 和 Shen 的驗證作法，主要利用向量量化後的壓縮碼作為影像驗證及還原的資訊，並將這些重要的資料藏匿於影像本身像素之中。圖二為 Wu 等學者所提之影像認證方法的流程圖，一開始，該認證方法輸入一張大小為 $W \times H$ 像素的原始灰階影像，然後執行公式(1)將該影像中每個像素最不重要的第一個位元清空，在公式(1)中的 X_{ij} 為影像座標(i, j)位置的像素值，X'_{ij} 則為影像座標(i, j)位置的新像素值；接著，將清空後的結果切割成許多不重疊且大小為 $w \times h$ 的小區塊，為了取得第 i 個區塊的認證資料，作者將區塊進行 VQ 編碼處理，得到該區塊最相似編碼字以及最不相似編碼，其索引值分別為 CW^i_b 與 CW^i_n，利用上述的兩個索引值和機密金鑰 K 將可獲得區塊認證資料 AU^i，其

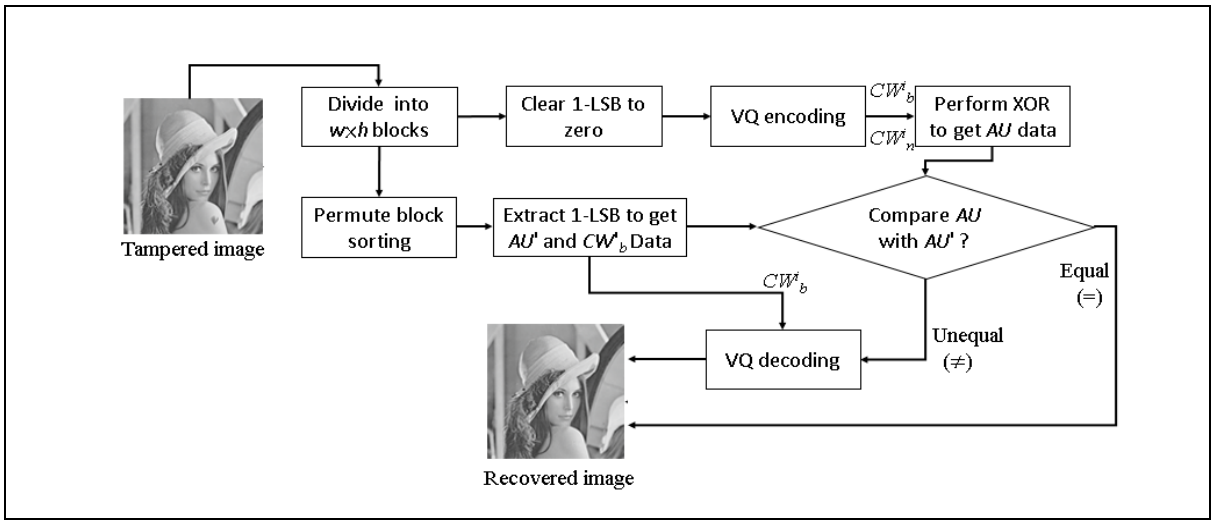
計算公式如公式(2)所示，其中 i 代表影像的區塊編號，其數值界在[0, $W\times H/w\times h$]之間。最後，將每個區塊的最相似編碼字 CW^i_b 以及認證資料 AU^i 分別藏匿於其他區塊像素的最不重要位元上，便可得到一張認證後的灰階影像，其中相對應的藏匿區塊主要是透過亂數序列來找到。



圖二：Wu 等學者的認證嵌入流程圖

$$X'_{ij}=X_{ij}-(X_{ij} \bmod 2), \text{ where } 0\leqq i<W \text{ and } 0\leqq j<H \quad (1)$$

$$AU^i=|CW^i_b-CW^i_n|\oplus K, \text{ where } 0\leqq i<(W\times H/w\times h) \quad (2)$$



圖三：Wu 等學者的竄改偵測及影像還原流程圖

圖三為 Wu 等學者所提出之影像竄改偵測及還原的流程圖，當需要偵測一張灰階影像是否曾遭受到惡意竄改時，首先先將該影像切割成大小為 $w\times h$ 且不重疊的數個區塊，並且將之前藏匿於相對應區塊內最不重要的像素位元取出，組合成認證資料 AU 和還原資料 R，接著，同樣地使用公式(1)將區塊內像素的最不重要位元清除，再利用 VQ 編碼技術取得該區塊最相似及最不相似的編碼字之索引值 $CW^i{}_b$ 與 $CW^i{}_n$，最後將這兩個索引

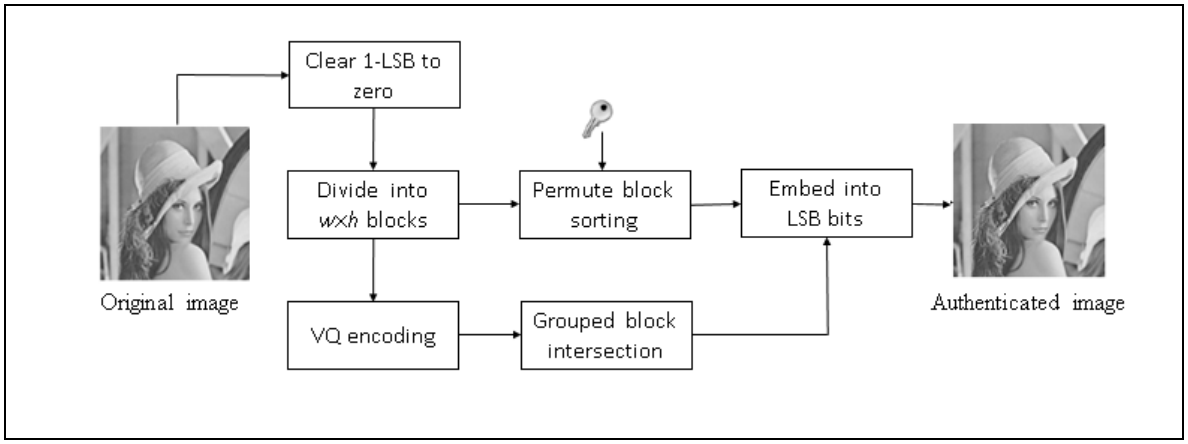
值和機密金鑰套入公式(2)即可計算出該影像區塊的認證碼 AU^{i}。只要利用 AU^{i} 和 AU^{i} 進行比對動作，就可知曉影像第 i 個區塊錯誤的情況，若比對的數值皆相同，則代表該區塊被判定未曾被修改過；相反地，比對結果數值不同，則表示區塊曾遭受到惡意竄改，因此，可透過先前藏匿的還原資料 R 至 VQ 編碼簿中找到該索引值所表示的編碼字，用以還原此影像區塊。此方法不僅將 VQ 編碼的索引值視為認證碼，同時也作為區塊還原資訊，因此，減少藏匿的資料量，進而改善 Yang 和 Shen 方法的驗證影像之品質；不過，藏匿的區塊認證碼恐會因為另一區塊內容的竄改而導致錯誤或遺失，進而造成竄改偵測的誤判情況發生，也就是第 i 個區塊內容被竄改，可能使得藏匿其中的第 j 個區塊認證碼或還原資訊改變，造成第 j 個區塊被判定為竄改區塊，如此一來，最後還原的影像品質將會因此而降低。

參、方法

第二節所提到的 Yang 和 Shen 方法因在藏匿認證及還原資料時更動到三個最不重要的像素位元，使得認證後影像品質略差，而 Wu 等學者的方法在偵測竄改時會產生較多的誤判，於是本章節將介紹我們所提出的影像驗證方法來改善上述的缺失，這裡將分為兩個小節來說明：3.1 小節為影像認證資料的產生與鑲嵌程序、3.2 小節則為竄改偵測與影像資料復原之程序。

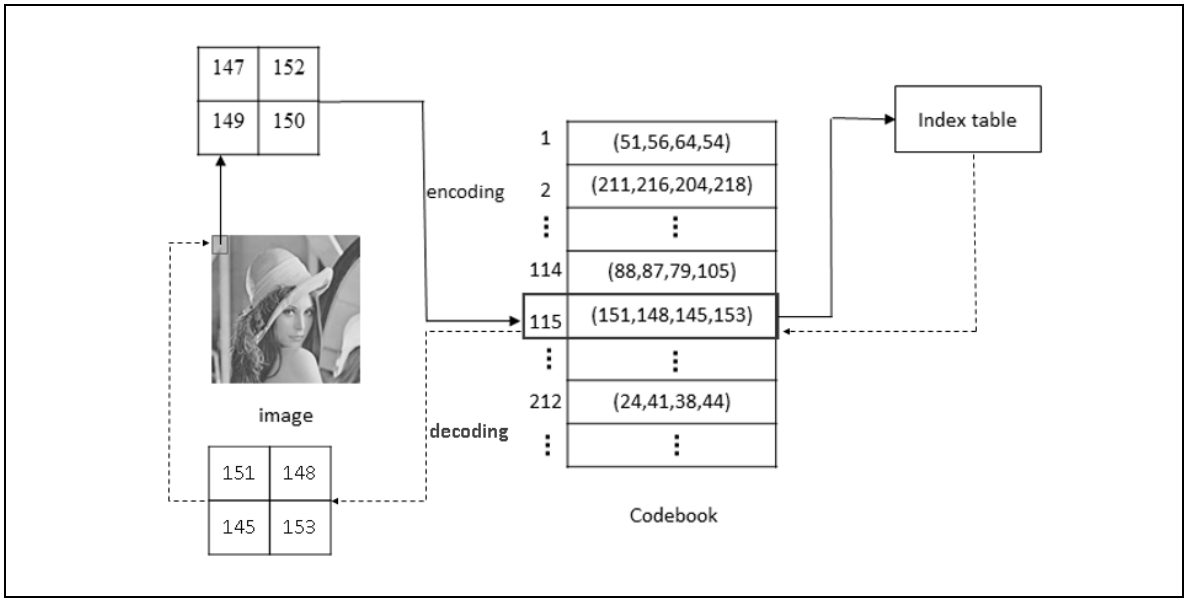
3.1 認證資料的產生與嵌入程序

認證資料的產生與嵌入程序主要是從一張影像中取得其認證用資料，並將它鑲嵌入該影像像素內，這些嵌入的資訊將於未來在竄改偵測階段作為是否被修改之評斷依據。圖四是我們所提方法之認證資料產生與嵌入之流程圖，首先，將一張 $W \times H$ 大小的灰階影像每個像素的最後一個位元清空，再切割成大小為 $w \times h$ 的不重疊區塊，每個區塊進行 VQ 編碼處理，取得其對應的索引編號，然後套用區塊集合交集的概念計算出每個區塊的驗證碼，這些區塊驗證碼將透過私密金鑰方式鑲嵌入其他區塊的最後一個位元像素中，最後則會得到一張認證後的數位影像。圖五為 VQ 編碼與解碼技術的說明示意圖，圖中實線箭頭流向代表編碼的流程，反之，虛線箭頭流向則代表解碼的流程，每個影像區塊會從 VQ 編碼簿中找到一個最為相似且距離最小的編碼字，利用該編碼字的編號來代替該區塊內容，以達到壓縮之目的。當進行解碼程序時，找尋編碼簿中該編號對應的編碼字，即可利用編碼字來還原其區塊內容，還原後的影像略為失真，但是視覺上幾乎看不出任何差異。



圖四：我們所提方法之認證資料產生與嵌入的流程圖

在所提方法中，我們套用區塊集合交集的概念到該 VQ 索引表內，也就是將索引表每 n 個索引值視為一個小集合並做互斥運算得到一個八位元的區塊認證碼，此認證碼將藏匿於影像區塊的位元中，當在竄改偵測時，可利用這些集合的交集運算得知出到底是哪一個索引值出錯。以圖六的索引表(VQ index table)為範例，當 n=3 時，第一個區塊的認證碼可由第一個、第二個以及第三個索引值代入互斥或(XOR)運算，得到一個八位元的數值，此例子為$(125)_{10}$ =$(0111\ 1101)_2$，而第二個區塊的認證碼則可由第二個、第三個以及第四個索引值計算出結果為$(117)_{10}$ =$(0111\ 0101)_2$，其他區塊也依序如此的運算計算本身區塊的認證碼；接著，每個區塊認證碼共有八個位元，將它鑲嵌於其他區塊前八個像素的最後一個位元中，以範例來說，第一區塊的認證碼 125 則會被藏匿於第二十七個區塊內。



圖五：VQ 編碼與解碼技術之示意圖

最後，每個區塊後八個像素的最後一個位元則用來藏匿其他區塊的 VQ 索引編號，其目的是用來還原那些疑似被竄改的區塊內容。以下為我們所提方法詳細的執行步驟：

驗證碼嵌入演算法

Step 1: 讀入灰階影像並將每個像素最後一個 LSB 的位元清除為 0；

Step 2: 將結果影像切割成許多相同 $w \times h$ 大小且不重複的區塊 B_m；

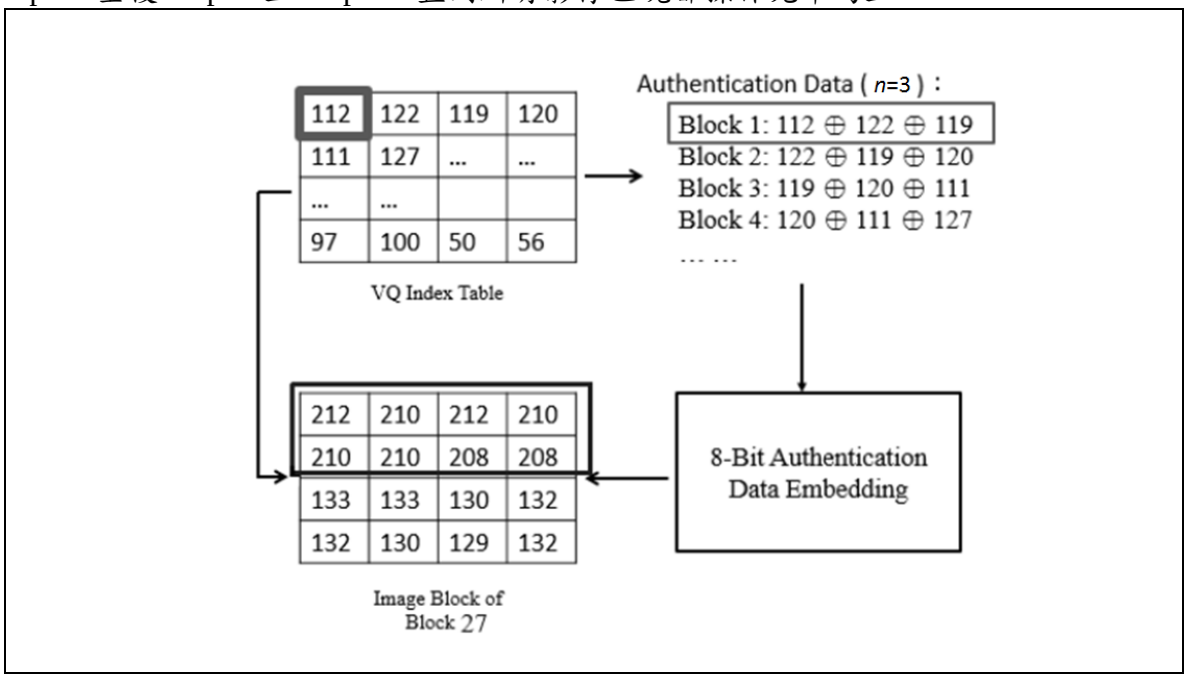
Step 3: 利用 VQ 的編碼簿 CB 找出每個影像區塊 B_m 最像的編碼字 a_m；

Step 4: 針對每個區塊 B_m，計算公式(7)的集合互斥或運算，得到該區塊的認證碼 F_m，其中 n 為區塊集合長度，N 為影像區塊的總數量；

$$F_m = a_m \oplus a_{m+1} \oplus \ldots \oplus a_{(m+n-1)\%N} \quad (3)$$

Step 5: 嵌入認證碼 F_m 於區塊 B_k 內前八個像素的最後一個 LSB 位元，另後八個像素的 LSB 則藏匿其他區塊的還原資訊 a，最後產生認證後的影像區塊 B'_m，其中 k 的選擇是隨機產生且非為 m 的亂數，用來增加認證碼的安全性；

Step 6: 重複 Step 4 至 Step 5，直到所有影像區塊都操作完畢為止。



圖六：VQ 索引集合交集運算之示意圖

3.2 竄改偵測與資料復原之程序

竄改偵測程序是當接收到他人傳送的影像時，我們可以檢驗其認證資訊來判定該張影像是否在傳輸過程遭受到有心人士的惡意竄改。在我們所提的方法中，我們一樣先將影像切割成大小為 $w \times h$ 的不重疊區塊，接著，把藏匿於區塊前八個像素的最後一個位元取出，得到原先區塊的認證碼，而區塊後八個像素的最後一個位元亦取出並於還原階段備用。下一步將每個區塊像素的最後一個位元清空，每個區塊進行 VQ 編碼處理，取得其對應的索引編號，然後套用區塊集合交集的概念計算出每個區塊的驗證碼，只要透過兩個驗證碼的比對，即可知道哪些區塊內容可能疑似被修改過，當兩個驗證碼相同，則

代表該區塊可能沒有被破壞；反之，當兩個驗證碼不同，則代表該區塊有可能被竄改過。不過，由於我們所提方法使用索引編號交集的方式，該區塊的驗證碼可能因為其他區塊的改變而變得不相同，以圖六為範例，當第三個區塊實際被修改時，它也會造成第一個區塊計算出的驗證碼與原先不一樣，使第一個區塊被判定為竄改區域；再者，它也可能因為第二十七個區塊內容的改變而導致錯誤或遺失，進而產生誤判情況，所以我們需再進行第二階段還原處理，檢查每個疑似竄改區塊的其他 n 個鄰居是否皆為疑似竄改，若不是，則代表該區塊被誤判，不需做還原處理；反之，該區塊則很有可能是被竄改過。而於區塊資料還原階段，我們則是利用先前取出備用的後八個像素位元來對那些判定被竄改的區塊來進行還原，只要操作 VQ 的解碼流程，即可還原出相似於原先區塊的內容。以下為我們所提方法詳細的執行步驟：

竄改偵測與還原演算法：

第一階段竄改偵測

Step 1: 讀入影像並將它切割成許多相同 w×h 大小且不重複的區塊 B^*_m；

Step 2: 擷取每個區塊內前八個像素的最後一個 LSB 位元並組成一認證碼 F_m，收集所有區塊驗證碼得到一集合 $F=\{F_1, F_2, \ldots, F_N|\}$；另擷取區塊後八個像素的 LSB 位元，視為一索引值 a_m，最後得到一索引表 IDX=$\{a_1, a_2, \ldots, a_N\}$；

Step 3: 利用 VQ 編碼簿 CB 找出每個擷取後區塊最像的編碼字 a^*_m；

Step 4: 針對每個區塊 B^*_m，計算公式(3)的群組互斥或運算，得到該區塊的認證碼 F^*_m；

Step 5: 比較 F 集合中 F^*_m 和 F_k 的驗證值是否相同，若相同則代表該區塊 B^*_m 未遭破壞，若不同則代表該區塊遭到竄改，需進一步執行第二階段的還原處理；其中，k 值是隨機產生的，如同上述的嵌入演算法。

Step 6: 重複 Step 4 至 Step 5，直到所有影像區塊都操作完畢為止。

第二階段還原處理

Step 1. 針對每個疑似竄改區塊 B^*_m，檢查區塊 $B^*_m, B^*_{m-1}, \ldots, B^*_{(m-n+1)\%N}$ 是否皆為疑似竄改，若不是，則代表區塊 B^*_m 被誤判，不需做還原處理；否則，執行公式(4)交集運算得到交集結果，其交集結果 INS 代表實際真正竄改的區域，需執行後續的 Step 2，其他區域則亦是誤判地方，不需做還原處理；

$$INS = F_m \cap F_{m-1} \cap \ldots \cap F_{((m-n+1)\%N} \quad (4)$$

Step 2. 找出區塊 B^*_m 的映射區塊 k，若第 k 區塊為正常區塊，則取出索引表 IDX 中的索引值 a_k，並用此值來還原該影像區塊，假若第 k 區塊亦為疑似區塊，則執行邊緣吻合預測法來還原區塊內容。

肆、實驗結果

在實驗的過程中，我們使用 Intel Core i5、CPU 3.2GHz 和 4Gbytes RAM 的電腦硬體規格和 Dev C++的軟體環境來執行 Yang 和 Shen 方法[12]、Wu 等學者之方法[11]與我們所提出的方法，其中使用五張大小為 256×256 的灰階影像作為實驗測試影像，分別是 Baboon、Lena、Pepper、Sailboat 與 Toys；另外，為了評估各方法的優劣，我們使用 PSNR 來作為影像品質的檢驗標準。一開始的實驗，我們先觀察所提方法在多少群組大小下能得出較好的認證影像及修復影像，在表一我們測試三種群組大小，分別為 n=3、n=4 及 n=5，從表一的結果可看出當設定群組大小 n 為 4 時，其認證後影像與修復影像的品質皆略高於其他兩個群組大小，故接下來的實驗我們則是採用群組大小 n 為 4 的設定來和其他兩個先前方法做比較。

表一: 我們所提方法在不同大小群組下之藏匿和修復 PSNR

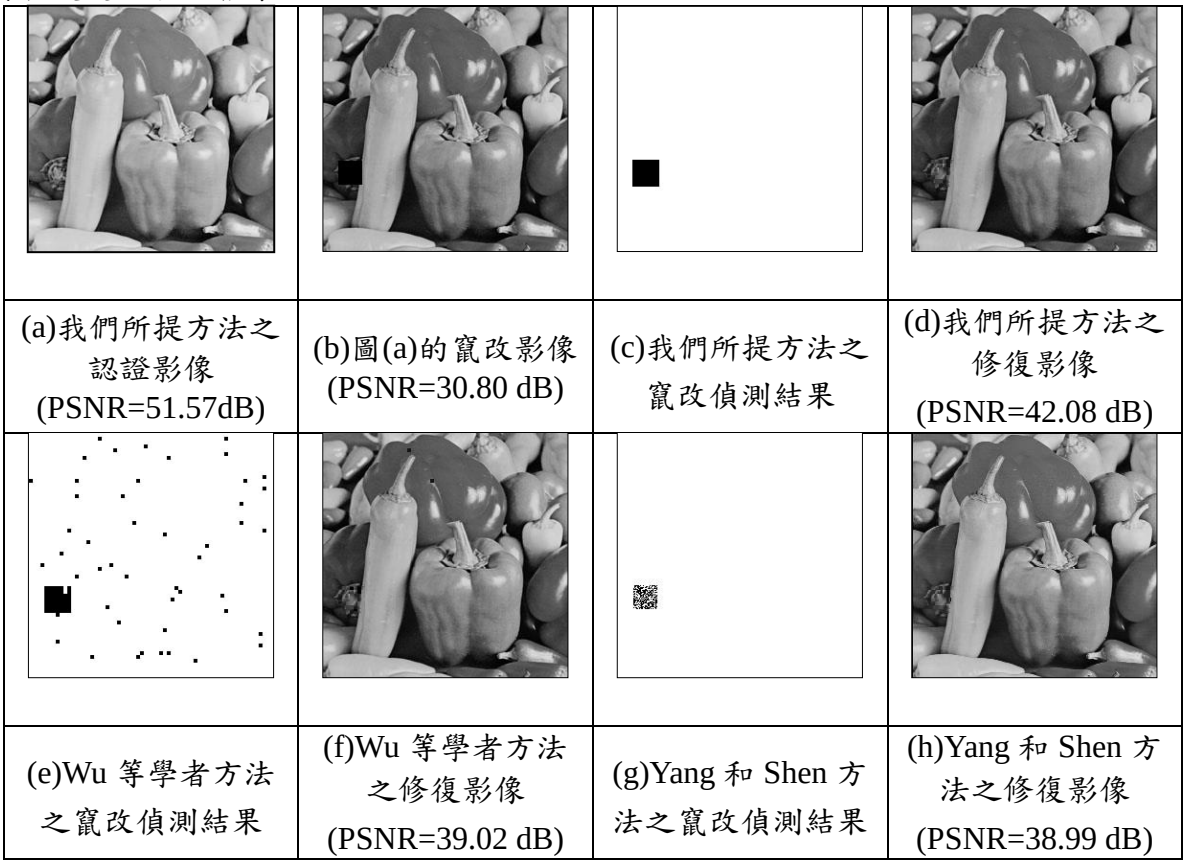
Images	n=3		n=4		n=5	
	認證影像	修復影像	認證影像	修復影像	認證影像	修復影像
Baboon	51.10	40.15	51.36	40.04	51.10	39.60
Lena	51.17	44.14	51.42	44.13	51.14	44.13
Pepper	51.24	42.08	51.57	42.08	51.22	42.08
Sailboat	50.89	37.56	51.32	43.15	50.91	37.56
Toys	52.06	40.39	52.80	40.39	52.07	40.39
Average	51.29	40.86	51.69	41.96	51.29	40.75

表二: 各方法認證後影像的 PSNR (dB)

Images	Yang 和 Shen 方法[12]	Wu 等學者的方法[11]	我們提出的方法(n=4)
Baboon	43.36	51.22	51.36
Lena	43.23	51.25	51.42
Pepper	43.17	51.29	51.57
Sailboat	44.21	51.03	51.32
Toys	44.67	51.69	52.80
Average	43.73	51.30	51.69

表二呈現使用三種不同方法的認證影像結果，從數據中可看出平均而言我們所提的方法比其他兩個方法有較高的認證影像品質，平均將近 51.70dB，其中數值遠高於 Yang 和 Shen 方法，其主要原因是因為 Yang 和 Shen 方法在藏匿資料時更動三個最不重要的像素位元，修改影像內容的幅度較大，而 Wu 等學者的方法和我們所提的方法則在藏匿認證資料時都只更動到一個最不重要的像素位元，因此 Yang 和 Shen 方法所產生的認證影像品質當然是三種方法中最差的。除了客觀的數據衡量外，圖七亦呈現出三種方法在主觀上的影像視覺效果，其中三種方法的認證影像皆遭受 25×25 相同大小的竄改攻擊，

如圖七(b)左下角的黑色方塊剪裁攻擊，從視覺上可明顯地看出來我們所提方法能較準確的標示疑似被竄改的區域位置，如圖七(c)所示，而另外兩個方法分別在圖七(e)和圖七(g)則顯示出該偵測結果有些許被誤判的情況，其中 Yang 和 Shen 方法因藏匿較多份的認證資料拷貝，故比圖七(e)的結果還減緩了誤判的狀況。當誤判的情況越多，則會導致需要越多的時間來處理疑似竄改區域的 VQ 解碼動作，當然也更讓修復的影像品質更加低落。從圖七的主觀結果可觀察出我們所提方法較其他兩個方法有較準確的偵測結果以及有較優越的修復影像。



(a)我們所提方法之認證影像 (PSNR=51.57dB)	(b)圖(a)的竄改影像 (PSNR=30.80 dB)	(c)我們所提方法之竄改偵測結果	(d)我們所提方法之修復影像 (PSNR=42.08 dB)
(e)Wu 等學者方法之竄改偵測結果	(f)Wu 等學者方法之修復影像 (PSNR=39.02 dB)	(g)Yang 和 Shen 方法之竄改偵測結果	(h)Yang 和 Shen 方法之修復影像 (PSNR=38.99 dB)

圖七：三種不同方法所產生的竄改偵測結果與修復影像

伍、結論

在先前的方法中，向量量化編碼法被運用來發展主動式影像驗證技術，將體積較小的 VQ 壓縮索引表視為影像重要的認證資料及還原資訊，不僅達到驗證之目的，還能將疑似被竄改的區域還原部分內容。在本篇論文中，我們亦提出一個準確標示並還原影像內容的數位驗證方法，同樣的採用 VQ 編碼技術來產生認證資訊，但為了減少影像品質的低落以及避免被誤判的情況發生，我們特別進行 VQ 區塊索引值的交集運算並將結果藏匿於像素的最後一個位元中。從實驗結果可發現我們所提出的方法有較高的認證影像

品質，其 PSNR 皆高於 51dB 以上，而且和其他兩個先前方法相比，我們的方法能夠更準確地標示出疑似被竄改的位置，減緩竄改誤判的可能，並還原出較佳的數位修復影像。

參考文獻

[1] F. Ahmed, M. Y. Siyal and V. U. Abbas, "A secure and robust hash-based scheme for image authentication," *Signal Processing*, vol. 90, pp. 1456-1470, 2010.

[2] S. Amtullah and A. Koul, "Passive image forensic method to detect copy move forgery in digital images," *Journal of Computer Engineering*, vol. 16, no. 2, pp. 96-104, 2014.

[3] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: a survey," *Digital Investigation*, vol. 10, no. 3, pp. 226-245, 2013.

[4] J. C. Chuang, Y. C. Hu, C. C. Lo and W. L. Chen, "Grayscale image tamper detection and recovery based on vector quantization," *International Journal of Security and Its Applications*, vol. 7, pp. 209-228, 2013.

[5] Y. Linde, A. Buzo and R. M. Gray, "An algorithm for vector quantizer design," *IEEE Transactions on Communications*, vol. 28, no. 1, pp. 84-95, 1980.

[6] Y. Park, H. Kang, K. Yamaguchi and K. Kobayashi, "Watermarking for tamper detection and recovery," *IEICE Electronics Express*, vol. 5, no. 17, pp. 689-696, 2008.

[7] P. Tsai, Y. C. Hu and C. C. Chang, "Using set partitioning in hierarchical trees to authenticate digital images," *Signal Processing: Image Communication*, vol. 18, pp. 813-822, 2003.

[8] S. Walton, "Information authentication for a slippery new age," *Dr. Dobbs Journal*, vol. 20, no. 4, pp. 18-26, 1995.

[9] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1593-1601, 2001.

[10] W. C. Wu, "Subsampling-based image tamper detection and recovery using quick response code," *International Journal of Security and Its Applications*, vol. 9, pp. 201-216, 2015.

[11] W. C. Wu, H. F. Hsu and P. Y. Lin, "Active tamper detection of digital images using VQ compression," *Proceedings of IEEE International Conference on Consumer Electronics-Taiwan*, Taipei Taiwan, pp. 508-509, 2015.

[12] C. W. Yang and J. J. Shen, "Recover the tampered image based on VQ indexing," *Signal Processing*, vol. 90, no. 1, pp. 331-343, 2010.