

JPEG 容錯型影像驗證技術

柯炫安

玄奘大學資訊科學學系
spencerke@gmail.com

陳建彰

玄奘大學資訊科學學系
cchen34@hcu.edu.tw

摘要

浮水印驗證技術的主要目的是藉偵測出惡意的竄改而達到確定影像的完整性。在本篇論文中，我們提出一種能允許 JPEG 壓縮之影像驗證技術，此方法是在 DCT 頻率域下，用自訂之量化表將係數量化，再藉由量化後的係數進行互斥或運算得到影像的特徵值，此特徵值能在係數被其他量化值量化後重建，再將特徵值嵌入 DCT 的參數中。而嵌入過程則是利用量化值變化的特性來處理。本方法可以區分出 JPEG 壓縮和其它惡意的攻擊，在使用 JPEG 標準量化表為自訂量化表時，此方法可以允許 JPEG 壓縮至大於 Quality Factor 25。

關鍵詞：半易碎式浮水印、JPEG、DCT、量化、影像驗證。

Abstract

Image authentication verifies the originality of an image from malicious manipulations. Most methods for image authentication treat all types of manipulation equally. However, with the increasing demand of JPEG images, a need arise in image authentication which could distinguish some acceptable manipulations like JPEG compression from malicious ones. In this paper ,we propose a DCT-based image authentication method. It is tolerant to JPEG compression from quality factor 26 to quality factor 100 but is sensitive to other malicious attacks. The image feature codes are calculated and then embedded into DCT middle domain by our proposed quantization properties. The experimental results are provided to support the scheme.

Keywords: watermark, JPEG compression, quantization, image authentication.

1. 前言

隨著時代科技的進步，愈來愈多的資料可以很輕易的自網路上下載取得。但是由於這樣的便利，攻擊者也愈來愈容易針對數位內容做

攻擊。因此版權的保護變成一個很重要的議題，而數位浮水印技術與數位影像驗證技術可以有有效的解決此問題。

近年來主要被廣為討論的影像安全技術可分為以下二類：

數位浮水印技術：主要是針對版權的保護，其目的為數位影像在任何攻擊下仍可取出足夠資訊，以證明數位影像之版權擁有者。

數位影像驗證技術：主要是針對影像訊息的正確性進行保護，其目的是透過該方法可以驗證所收到的訊息是否正確。

對於數位影像認證技術可再細分為以下兩種：

易碎式影像驗證：此種技術對於任何的影像處理技術都非常敏感，因此任何的影像處理(包含失真性影像壓縮)在此種方法下，都被視為一種惡意的攻擊，並留下不可抹滅的痕跡。

半易碎式影像驗證：此種技術並不像易碎式那麼的敏感，若廣義的來說，此種技術可以在限定的影像處理方法下不會對所嵌入的驗證資訊造成傷害；反過來說，在限定外的處理都會傷害到驗證資訊，一般限定的處理是指失真性壓縮。

浮水印驗證技術的主要目的是為了確保影像之不遭受竄改，所以在影像中嵌入秘密資訊，當影像遭受竄改時我們所嵌入的資訊就會被更改，如此一來在抽取出已嵌入的浮水印資訊時，我們就能夠辨別此影像是否已遭竄改。而隨著 JPEG 壓縮影像的增加，浮水印技術開始將 JPEG 壓縮視為是允許的修改。在本篇論文中，我們提出一種半易碎型的浮水印架構，我們的目的是希望能有效的區分出 JPEG 壓縮的修改和惡意的修改，把壓縮對數位影像所產生的改變視為可接受，除了 JPEG 壓縮之外，均當成惡意的攻擊。

本文在第 2 章文獻探討略述前人所提及應用於影像驗證之方法。第 3 章描述本文所提出之影像驗證方法。第 4 章陳述本文所提方法之實驗結果，第 5 章為結論。

2. 相關研究

在 JPEG 壓縮的過程裡，會對影像 DCT 係數做「量化」的動作，此動作為一個失真性的行為，也就是在 JPEG 壓縮過程中，讓影像失真最嚴重的步驟。因此，為了能夠將 JPEG 壓縮修改與惡意竄改區分出來，我們需要找到某些數學特性，同時滿足下列兩種情況，1. 此特性在量化後仍存活著，2. 在量化行為以外的處理時，此特性會被破壞掉，如此即可將此特性拿來當成區分 JPEG 壓縮與竄改的一個準則。

Lin C.Y.及 Chang S.F. [3]他們於 1998 年提出了利用位於不同 DCT 區塊卻同樣位置的兩係數，他們之間的等價關係，並不會隨著量化處理而消失。再藉著利用不同的門檻值，記錄出兩係數的差值與門檻值間的關係，這樣的關係可在量化後仍然不變，然而在其他修改時，被破壞掉，而設定多個門檻值，所得到的多種關係，是為了增加影像的驗證性。在 2006 年 Lin C.Y.及 Chang S.F. [4]進一步提出了能夠更精確紀錄兩係數間差值的方法，再根據兩係數差值在量化後，所得到的差值呈現叢聚結果，並用量化值定義出其量化後差值跑動的範圍。只要差值的變化超過定義之範圍，即認為是惡意的竄改。但為了更準確的記錄兩係數的差值，因此得使用較多個位元來當特徵值，卻在驗證時，會有發生碰撞的機會。在影像驗證上，這兩篇已有相當不錯的成果，但缺點在於找出來的特徵值必須另外存在檔案庫裡，造成額外負擔。

Chen C. C.及 Lin C. S. [1]在 2007 年發表的方法解決了需要將特徵值另外存放在檔案庫的問題，其方法是利用兩個不同區塊相同位置的等價關係，得到特徵值，再利用量化後差值的變化，嵌入特徵值。其嵌入的方法，令兩係數介於一個固定差值，且在量化值小於或等於此固定差值的情況下，當兩係數的差為一倍固定差值時，與三倍固定差值時，兩係數經量化後，這兩種差值不會有所交集。當我們要判斷是否為 JPEG 壓縮處理或惡意竄改時，此方法可以根據 JPEG 壓縮的量化表與差值間的關係來決定驗證時的寬容度。

Ho C.K.及 Li C.T. [2]在 2004 提出了用一個自訂的量化表，先對係數做量化，往後只要量化值小於自訂的量化值，係數可以正確的被還原。其驗證碼的取得是由每個 DCT 區塊與其附近八個鄰居區塊，利用係數跟係數間正負號

的關係，與大小關係，把九個區塊產生關連。量化的處理可以經由還原而驗證成功，而其他惡意的竄改則是利用與八個鄰居關係的敏感性將其找出。卻會發生當只有一個區塊發生錯誤時，驗證出其鄰居區塊也錯誤的結果。

在[1]和[2]提出的方法中，他們都有一個共通的限制，就是量化值一定得滿足小於或等於初始的自訂值，也就是說如果我們想要拉高對 JPEG 壓縮的承受能力，我們就得放大初始的自訂值，相對的，這也影響了嵌完資訊後圖的品質。因此，我們提出了一個架構，試著放寬這樣的限制，並且在不需額外資訊的情況下，同樣具有影像驗證的能力。

3. JPEG 容錯型影像驗證方法

我們提出的方法包含了兩個部分，第一部分是特徵值的取出與嵌入，第二部分為驗證部分。而為了讓驗證可以區分出允許之量化處理與惡意攻擊，我們運用影像被量化後仍存在的兩個特性來做特徵值取出與嵌入。

3.1 兩個存在於量化後的特性

特性一：

假設 $P(v)$ 為一個 8×8 區塊裡的某一位置 DCT 係數， $Q(v)$ 為 JPEG 標準量化表之量化值， $T(v)$ 為使用者定義量化表， $v \in \{1, \dots, 64\}$ ， $Q(v) < 2 \cdot T(v)$ 且 $\lfloor \cdot \rfloor$ 為四捨五入取整數， $\lceil \cdot \rceil$ 為取下界整數。

$$\tilde{P}(v) \equiv \left\lfloor \frac{P(v)}{T(v)} \right\rfloor \cdot T(v) \quad (1)$$

$$\hat{P}(v) \equiv \left\lceil \frac{\tilde{P}(v)}{Q(v)} \right\rceil \cdot Q(v) \quad (2)$$

$$\left\lfloor \frac{P(v)}{T(v)} \right\rfloor - 1 < \left(\frac{\hat{P}(v)}{T(v)} \right) < \left\lceil \frac{P(v)}{T(v)} \right\rceil + 1 \quad (3)$$

從公式(3)我們可以得到，如果我們事先知道 $\left\lfloor \frac{P(v)}{T(v)} \right\rfloor$ 的值為奇數或偶數，我們就可以由

$\left\lceil \frac{\hat{P}(v)}{T(v)} \right\rceil$ 的值找回 $\left\lceil \frac{P(v)}{T(v)} \right\rceil$ 。換句話說，如果我

們先用一個自訂的量化值先將係數量化，並且紀錄其量化完結果之奇偶，只要往後在量化值小於兩倍的自訂量化值的情況下，我們都可以藉著再除一次自訂量化值和已知的奇偶，重新找回原倍數。

假設 $P(v)=100$ ， $T(v)=15$ ， $Q(v)=25$

$$\left\lceil \frac{P(v)}{T(v)} \right\rceil = 7$$

由 公式(1)

$$\tilde{P}(v) \equiv \left\lceil \frac{P(v)}{T(v)} \right\rceil \cdot T(v) = 105$$

由 公式(2)

$$\hat{P}(v) \equiv \left\lceil \frac{\tilde{P}(v)}{Q(v)} \right\rceil \cdot Q(v) = 100$$

$$\frac{\hat{P}(v)}{T(v)} = 6.667, \left\lceil \frac{\hat{P}(v)}{T(v)} \right\rceil = 7$$

由 公式(3)

$$\left\lceil \frac{P(v)}{T(v)} \right\rceil - 1 < 6.667 < \left\lceil \frac{P(v)}{T(v)} \right\rceil + 1$$

$$\therefore \left\lceil \frac{P(v)}{T(v)} \right\rceil = 7 \text{ 為奇數，而 } \left\lceil \frac{\hat{P}(v)}{T(v)} \right\rceil = 6 \text{ 為偶數，}$$

$$\therefore \text{我們可以由 } \left\lceil \frac{\hat{P}(v)}{T(v)} \right\rceil + 1 = 6 + 1 = 7 \text{ 就可將原}$$

倍數找回。

因為我們無法確定欲保護係數的量化後的結果為奇數或偶數，所以我們使用一張二元圖來當作一組對應的 key，當量化後係數對應到二元圖裡的 1 時，則將其調整成奇數，若已為奇數，則保留。若量化後係數對應到二元圖裡的 0 時，則將其調整成偶數，若已為偶數，則保留。嵌入流程中的調整係數就是在做這樣的對應。我們運用此特性之目的在於當係數經過量化後，我們可以完整的將其重建，以確保係

數互斥或運算所得的特徵值保持不變。

特性二：

Chen C. C 及 Lin C. S. 在[1]所提出的「進一步量化特性」定理，此特性滿足於量化值小於或等於其所自訂的差值情況下。本文所提出的特性二，則是由「進一步量化特性」所延伸出來，放寬其對量化值的範圍限制至小於兩倍的自訂差值。

假設 p 、 q 為兩個不同區塊中同位置的 DCT 係數， D 為兩個係數的差值， T 為用來量化 p 、 q 的量化值且 $T < 2 \cdot D$ ， $s = \left\lfloor \frac{D}{T} \right\rfloor$ ，則

我們可以得到

1. If $p - q = D$ then

$$s \cdot T \leq \left\lfloor \frac{p}{T} \right\rfloor \cdot T - \left\lfloor \frac{q}{T} \right\rfloor \cdot T \leq (s+1) \cdot T \quad (4)$$

2. If $p - q = 4 \cdot D$ then (5)

$$s \cdot T \leq \left\lfloor \frac{q+D}{T} \right\rfloor \cdot T - \left\lfloor \frac{q}{T} \right\rfloor \cdot T \leq (s+1) \cdot T \leq \left\lfloor \frac{p}{T} \right\rfloor \cdot T - \left\lfloor \frac{q}{T} \right\rfloor \cdot T$$

從式子(4)跟式子(5)中，我們可以得到，如果兩個係數的差值為 D 和 $4 \cdot D$ 時，在量化後它們可以被區分出來。因此，當我們要嵌入 1 時，則讓兩係數的差值在一個 D 值，若要嵌 0，則讓它們的差值為 $4 \cdot D$ 。

3.2 嵌入的步驟如下：

- 一、將影像轉成 DCT 的頻域係數，每兩個區塊為一組。
- 二、從每一組區塊中，選出欲保護的係數，並將其用自訂的量化表做量化。
- 三、產生一組二元 key，每對根據二元 key 的值來調整量化完後係數的奇偶。若係數對應到的 key 值為 1，則將係數調整為奇數，若已為奇數則不調整，若對應到的 key 值為 0，則係數調整成偶數，若已為偶數則不動。
- 四、每組將調整完的係數進行互斥或(XOR)，轉成二進位，每組各得到一串特徵值。
- 五、運用特性二，每組將特徵值依序嵌入自己的中頻係數。
- 六、將處理完結果做 IDCT，得到已嵌入資訊之圖。

3.3 驗證的步驟如下：

- 一、將影像轉成 DCT 的頻域係數，找回原來的分組。
- 二、以組為單位，找到欲保護的係數，並將其用自訂的量化表做量化。
- 三、根據每組二元 key，還原與 key 相同奇偶的量化後係數。
- 四、每組將還原後的係數做進行互斥或 (XOR)，使各組得到一組特徵值。
- 五、根據特性二，從中頻區取出原本嵌入的特徵值。
- 六、將第四步驟與第五步驟所得的特徵值做比較。完全相同則表示驗證成功，反之則表示驗證失敗。

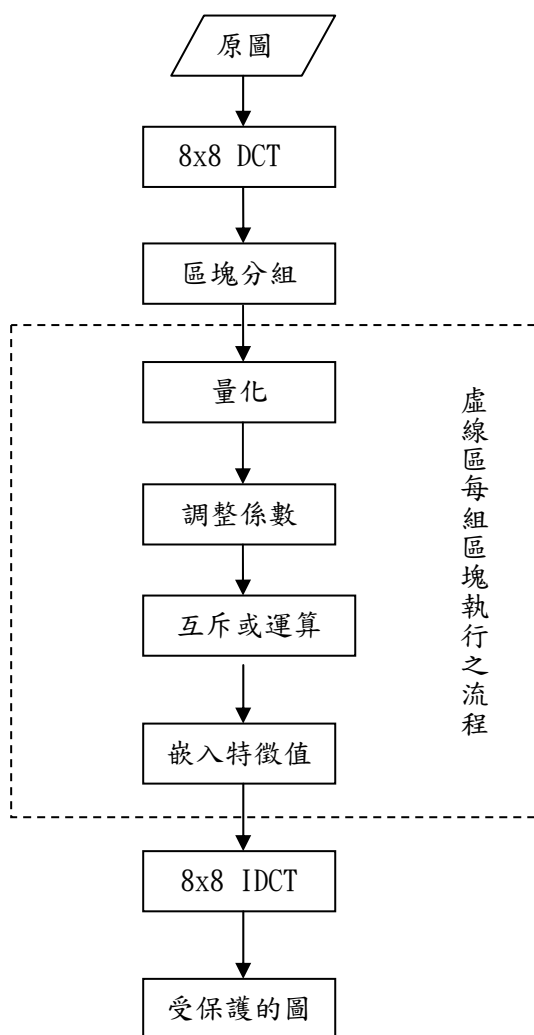


圖 1. 浮水印嵌入之處理流程

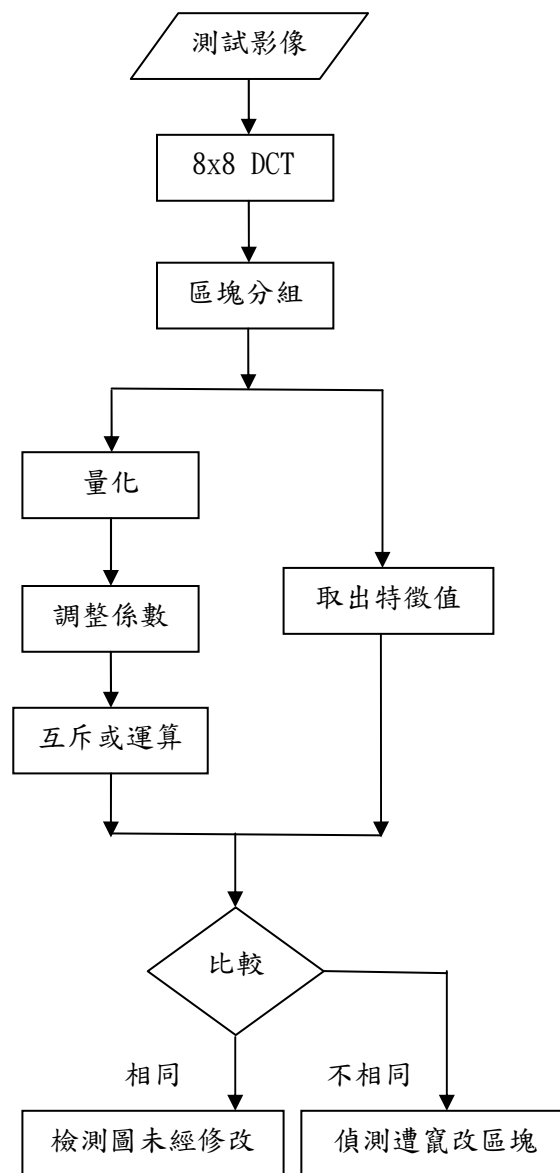


圖 2. 影像驗證之處理流程

下圖為我們拿來當 key 的二元圖，每個欲保護係數對應到二元圖中的不同位置的像素值，再根據對應的值把量化後之係數調整成不同的奇偶數。



3.4 例子：

假設我們將調整完係數作互斥或後所得到的結果為 1010。則我們利用特性二，嵌 1 的時候，利用式子(4)，將兩係數差值改成 Q ，因此 $p = (p + q) / 2$ ，而 $q = (p + q) / 2 + Q$ 。嵌 0 的時候，利用式子(5)，將兩係數的差值調成 $4 \cdot Q$ ，因此 $p = (p + q) / 2 + 2 \cdot Q$ 而 $q = (p + q) / 2 - 2 \cdot Q$ 。而 Q 值的決定，我們使用 JPEG 的標準量化表 quality factor 50，每個係數以其位置的量化值來做為 Q 值的選取，因此 p 、 q 對應到的 Q 值為相同的值。

			0				
		0					
	0						
6							

(a)原 DCT 區塊 p

			6				
		0					
	0						
0							

(b)原 DCT 區塊 q

			3				
		28					
	0						
31							

(c)嵌完後的 DCT 區塊 p

			19				
		-28					
	13						
-25							

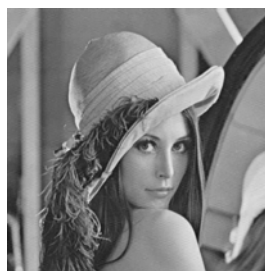
(d)嵌完後的 DCT 區塊

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	59
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

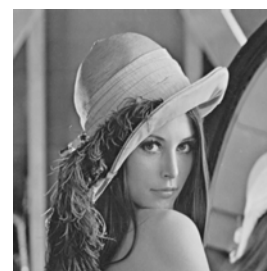
(e)JPEG 標準量化表

4. 實驗結果

我們實驗的方式是以一張 512x512 大小的 Lena 圖做測試。圖 3(a)為原圖，圖 3(b)為嵌完浮水印後的圖，其 PSNR 值為：36.0582。



(a)



(b)

圖 3、(a)原圖

(b)浮水印圖

4.1 JPEG 壓縮的驗證

我們的方法在 JPEG 量化值小於兩倍的自訂量化值的情況下，所嵌入的值均能存活，因此可以依據實際的需要來決定自訂量化值的大小。在實作中，我們使用的自訂量化表為 JPEG 的標準量化表，故理論上可以承受 JPEG 壓縮至 QF26。



圖 4、(a) JPEG 壓縮(QF70) (b) (a)之驗證結果
(c) JPEG 壓縮(QF50), (d) (c)之驗證結果
(e) JPEG 壓縮(QF30), (f) (e)之驗證結果
(g) JPEG 壓縮(QF10), (h)(g)之驗證結果

從圖 4 證明了我們的方法的確可以把 JPEG 壓縮視為可接受的修改，理論上應可將允許的 JPEG Factor Quality 範圍放寬為 QF100 至 QF26，實驗的結果符合理論上的期望。而當 QF 值降至 25 以後，則會有驗證錯誤的情況發生，如圖四中的(h)。驗證的錯誤率會隨著 QF 值的降低而增加。QF 跟錯誤率的關係，我們列於表 1。

4.2 剪貼的修改



圖 5、(a)被修改後的圖 (b) (a)之驗證結果

在圖 5 的實驗中，我們在 Lena 的帽子上加了一朵花，經我們驗證系統偵測後，正確的標示出遭竄改的區塊。

4.3 Quality Factor 和錯誤率的比較

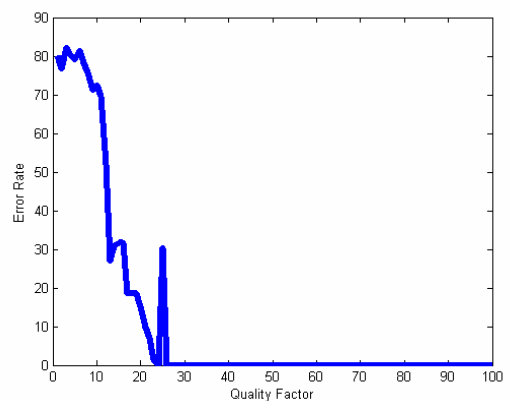


表 1 Quality Factor 與 Error Rate 的關係

從表 1，我們可以看出在 Quality Factor 26 之前，我們提的方法對 JPEG 壓縮驗證的錯誤率為零。在 Quality Factor 小於 25 以後，錯誤率會隨著 Quality Factor 的值愈小而升高。而在 Quality Factor 等於 25 時錯誤率突然拉大的原因，可由我們提出的特性一推得。因 Quality Factor 25 所算出的 $Q(v)$ 剛好等於 2 倍 $T(v)$ ，

$$\text{套到特性一，} \left[\frac{P(v)}{T(v)} \right] = 2 \cdot \frac{\tilde{P}(v)}{T(v)}, \text{ 只要 } \left[\frac{P(v)}{T(v)} \right]$$

$$\text{為奇數時，} \left[\frac{1}{2} \cdot \left[\frac{P(v)}{T(v)} \right] \right] \text{ 會剛好進位，使得}$$

$\hat{P}(v)$ 會變的太大，使得公式(3)一定不成立。故錯誤率明顯拉高。

5. 結論

在本篇論文中，我們提出了一個允許 JPEG 壓縮處理的影像認證技術，其架構運用了兩個可以存活於 JPEG 壓縮的特性，在第一個特性中，若我們預先用已知量化值，將係數量化且記錄其奇偶數，只要在 JPEG 的量化值小於兩倍的已知量化值的情況下，我們可以完整的重建原來的係數。我們運用特性一來確保我們從係數中取出的特徵值可以在量化後保持不變；第二個特性指出在兩個不同區塊裡且相同位置的係數，它們的差值在量化後會在一個限定的區間裡改變，因此我們可以根據欲嵌入特徵值的不同，在兩係數間給予不同的差值，讓不同的差值在量化後能限制在不同的區間裡而不相互影響，使得我們在量化後仍然可以完整的取回特徵值。由實驗的結果顯示，我們提出的方法確實能有效的區分出 JPEG 壓縮和惡意的攻擊，把 JPEG 壓縮對數位影像所產生的改變視為可接受，其餘均當成惡意的攻擊。

在我們提出的方法中，我們對原圖係數值做了較大的更動來達到我們的目標。未來，我們嘗試著在功能不變的情況下，降低影像嵌入量來提升影像品質。

參考文獻

- [1]Chen C. C. and Lin C. S., "Toward a Robust Image Authentication Method Surviving JPEG Lossy Compression", *Journal of Information Science and Engineering*, 23(2) March, 2007.
- [2]Ho C.K. and Li C.T. "Semi-Fragile Watermarking Scheme for Authentication of JPEG Images" *Proceedings of the International Conference on Information Technology: Coding and Computing* (ITCC'04)0-7695-2108-8/04
- [3]Lin C.Y. and Chang S.F., "A Robust Image Authentication Method Surviving JPEG Lossy Compression", *Proc. SPIE*, vol.3312, 1998, pp.296-307.
- [4]Maeno K., Sun Q.B., Chang S.F, Suto M. "New Semi-Fragile Image Authentication Watermarking Techniques Using Random Bias and Nonuniform Quantization." *IEEE Transactions on Multimedia*, 8(1):32-45, February 2006