國立中興大學資訊工程學系

資訊專題競賽報告

基於 APPM 的近似灰階不變性彩色影像驗證

專題題目說明、價值與貢獻自評（限100字內）:

本專題設計具近似灰階不變性的彩色影像驗證系統，結合 APPM 嵌入技術與參考表法，有效提升嵌入品質與篡改偵測力，實驗證明 PSNR 均值達 37 dB，具實用價值。

專題隊員：

姓名	E-mail	負責項目說明	專題內貢獻度(%)
邱睿棋	rich92122@gmail.com	實驗、報告	50
王睿毅	scotts50110@gmail.com	實驗、報告	50

【說明】上述表格之專題內貢獻度累計需等於100%。

指導教授簡述及簡評：

指導教授簽名：_____

中 華 民 國　　1 1 4 年　　5 月　　1 4 日

基於 APPM 的近似灰階不變性彩色影像驗證

一、摘要 (含關鍵詞)：

本專題旨在實作一套具近似灰階不變性的彩色影像驗證，目的是在不明顯改變原圖片灰階值的前提下，於影像中嵌入驗證碼以達成影像完整性驗證的目標。該研究受到近年文獻影響，特別是 Hong 等人於 2020 年[1]提出的「Color Image Authentication Scheme with Grayscale Invariance」，該方法首度針對灰階不變性進行深入探討並提出調整色彩通道的方式以維持視覺一致性。本研究於其基礎上進行改良與實作，並透過建立參考表與調整綠色通道實現驗證碼嵌入與灰階保持之雙重目標。實驗顯示，系統可有效偵測影像篡改，且平均 Peak Signal-to-Noise Ratio (PSNR，峰值信噪比是一種計算影像的失真的指標，當兩張圖片比較後所得的 PSNR 高於 30dB，則人眼難以分辨) 值介於 36~37 dB 之間，證明具備良好視覺品質與偵測能力。

關鍵詞：彩色影像驗證、灰階不變性、影像完整性。

二、專題研究動機與目的：

影像驗證技術能協助辨識數位圖片是否遭篡改，例如: 把名人頭像放到另一個人身體上，製造假新聞。傳統方法雖具高偵測能力，但常導致視覺品質劣化或灰階變異。灰階不變性在許多影像應用中至關重要，例如邊緣偵測、影像濾鏡與電子墨水顯示等，皆仰賴穩定灰階值進行後續處理。為此，本專題希望在嵌入驗證碼的同時，維持原之灰階值，提升驗證應用的實用性與穩定性。

三、專題重要貢獻：

1. 實作並改良具灰階不變性的彩色影像驗證技術。
2. 引入參考表映射機制以降低紅藍通道修改幅度。
3. 可實現像素層級的影像篡改偵測與定位。
4. 提供高影像品質的嵌入結果，平均 PSNR 值達 37。

四、 團隊合作方式:

本專題由兩位成員協作完成，各自分工如下：

- 文獻研究與概念發展：分析灰階不變性重要性與既有方法。
- 演算法設計與改良：擬定驗證碼生成與灰階平衡策略。
- 程式撰寫與處理：實作嵌入與提取演算法。
- 系統評估與測試：進行實驗分析與結果呈現。
- 報告撰寫與排版：撰寫本報告與製作發表資料。

五、 設計原理、研究方法與步驟:

5.1 設計原理概述 :

本研究基於 Hong 等人於 2020 年[1]所提出的彩色影像驗證方法，該方法首度考量灰階值不變性問題。其核心概念在於：

1. **驗證碼嵌入：**將驗證碼分別嵌入紅與藍通道。
2. **綠色通道調整：**根據灰階變化反向調整綠色通道，以抵銷前述嵌入導致的灰階偏差。
3. **類型分流嵌入：**根據嵌入是否可行分為兩類（Type I 與 Type II）處理方式，前者使用公式精確調整 (保持灰階不變)，後者使用摺疊以求穩定灰階值，也就是盡可能降低灰階值的變化。

5.2 Related Work :

- **A Color Image Authentication Scheme With Grayscale Invariance**
  1. **簡介 :**

     Hong 等人[1]首次提出具「灰階不變性」的彩色影像驗證框架。該方法著重於嵌入驗證碼後仍能保持原圖與嵌入圖之灰階值一致，確保後續處理（如邊緣偵測、灰階濾鏡等）結果一致。其方法以紅、藍通道為嵌入目標，綠色通道則負責調整以維持灰階計算值不變。當綠色通道無法補償誤差時，則以退而求其次的方式僅於藍通道嵌入少量資訊，並透過鄰近像素擾動法找到最合適嵌入組合，從而兼顧灰階穩定與驗證能力。實驗顯示該方法在影像品質與偵測能力間取得良好平衡，是本研究延伸與改良的基礎依據。

2. 灰階不變性演算法說明 ：

灰階值的計算採用下列權重轉換公式：

$$gv = round(0.299r + 0.587g + 0.114b) \quad (1)$$

當驗證碼嵌入紅與藍通道後，會導致原灰階值偏移，因此需動態調整綠色通道值 g'：

$$g' = round(\frac{gv - 0.299r' - 0.114b'}{0.587}) \quad (2)$$

其中 r', b' 為嵌入後的新通道值。若 g' 合法（即介於 0~255），則稱此像素為「可調整像素」，也就是 Type I，若不合法，則需使用 Type II ，也就是將嵌入量降為 2 bits，並嵌入藍色通道，因為藍色通道的係數最小，也就是人眼對藍色通道最不敏感。

- **An unsolvable pixel reduced authentication method for color images with grayscale invariance**

1. 簡介 ：

Hong 等人於 2023 年[2]提出了一種針對彩色圖像的進階灰度不變性認證方法。先前的研究直接使用紅色和藍色通道的最高有效位 (MSB) 來產生認證碼，並將這些代碼嵌入到最低有效位 (LSB) 中。同時，調整綠色通道以維持一致的灰度值。然而，這種直接使用 MSB 的方式通常會導致圖像品質(PSNR)下降，並產生大量無法解決的像素(Type II)。

2. 方法 ：

為了應對這些挑戰，Hong 等人於 2023 年的論文提出了一種新的方法，專門設計用於改善圖像品質的劣化和無法解決像素的普遍性。此方法提出了最高有效位元變更 (MSBA) 技術，該技術修改紅色和藍色通道的 MSB，以產生具有最小失真的認證碼。此技術有效地減少了圖像失真和無法解決的像素數量。此外，論文還介紹了像素替換策略 (PSS) 和約束降低策略 (CRS)，以提高嵌入效率。

a. MSBA :

先從紅色通道提取長度為 8 - l_r 的 MSB，從藍色通道提取長度為 8 - l_b 的 MSB，l_r 和 l_b 為紅色和藍色通道嵌入的驗證碼長度，並將他們轉成 10 進位後加減 1，或是不作任何更動，分別放入 hash function，以及透過維持灰階不

變性，接著透過歐幾里得距離計算嵌入驗證碼後的像素和原像素的差異，公式如下，選擇差異最小的組合當作最終的嵌入結果，這樣就有 9 種可能性，可以有效降
低像素的變異，提升影像品質，每次嵌入都會計算該像素的灰階值和它的索引記錄在表格中。

$$(r_i' - r_i)^2 + (g_i' - g_i)^2 + (b_i' - b_i)^2 \quad (3)$$

b. PSS :
使用 MSBA 之後，可能會有一些像素是無法維持灰階不變的，這時候就從表格中取出與當前像素灰階值相同的所有像素，依照他們與當前像素的歐幾里得距離排序，從距離最近的開始逐一使用 MSBA 技術，找出可行的方案並以此替代當前像素。

c. CRS :
為前兩種方案皆失敗後採用的折衷方案，最多只能嵌入 2 bits。

5.3 先備知識 :

- **Adaptive Pixel Pair Matching (APPM) 嵌入技術**

Hong 與 Chen 在 2012 年提出了一種具代表性的資訊隱藏技術——Adaptive Pixel Pair Matching (APPM) 嵌入法。此方法是針對灰階圖片透過像素對匹配與參考表（Reference Table, RT）結合，在兩個像素中嵌入一個 B 進制的數字，兼具資料載量與影像品質的平衡。

APPM 的核心在於以像素對 (r, c) 作為座標中心，在其鄰域 Φ(r, c) 內尋找一個目標像素對 (r′, c′)，使其對應的參考表值符合欲嵌入的數字 s。嵌入時會將原像素值 (r, c) 改為 (r′, c′)，而擷取時則透過該像素對在參考表中的值，回推原嵌入的數字。參考表的值是經由函數：

$$f(r, c) = (r \times c_B + c)\%B \quad (4)$$

所產生，其中 r 為參考表的列索引值座標，c 為行索引值座標， c_B 為一個常數，出自 figure 1

C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}	C_{16}	C_{17}	C_{18}
1	1	2	2	2	3	3	3	3	4	4	4	5	4	6	4	4
C_{19}	C_{20}	C_{21}	C_{22}	C_{23}	C_{24}	C_{25}	C_{26}	C_{27}	C_{28}	C_{29}	C_{30}	C_{31}	C_{32}	C_{33}	C_{34}	C_{35}
4	8	4	5	5	5	10	5	4	5	12	5	6	6	6	6	10
C_{36}	C_{37}	C_{38}	C_{39}	C_{40}	C_{41}	C_{42}	C_{43}	C_{44}	C_{45}	C_{46}	C_{47}	C_{48}	C_{49}	C_{50}	C_{51}	C_{52}
15	6	6	7	7	6	12	8	7	7	7	7	14	14	9	9	22
C_{53}	C_{54}	C_{55}	C_{56}	C_{57}	C_{58}	C_{59}	C_{60}	C_{61}	C_{62}	C_{63}	C_{64}	C_{128}	C_{256}	C_{512}	C_{1024}	
8	12	21	16	24	22	9	8	8	8	14	14	12	60	200	271	

figure 1： 不同數字範圍的 c_B 值

範例說明：

參考下圖，假設像素為 (x, y)，左上角為(0, 0)，橫軸為 x 軸，縱軸為 y 軸，橫軸越往右 x 值越大，縱軸越往下 y 值越大，以 B = 256 為例，假設原始像素對為 (5, 10)，欲嵌入的數字為 14。根據參考表，(5, 10) 對應的值為 54，需尋找與 54 最接近且值為 14 的像素對，例如 (0, 14) 的值為 14，且其與 (5, 10) 的歐幾里得距離最小。因此嵌入後的像素值變為 (0, 14)，在解碼階段則可從 (3, 11) 回推得知原嵌入的數字為 13。透過此嵌入技術可有效減少藍色和紅色通道的變化量。舉個更極端的例子，如果透過 LSB 嵌入 128 的話，那變化量就會很可觀，但如果用 APPM 嵌入法就能有效降低像素的變化量。

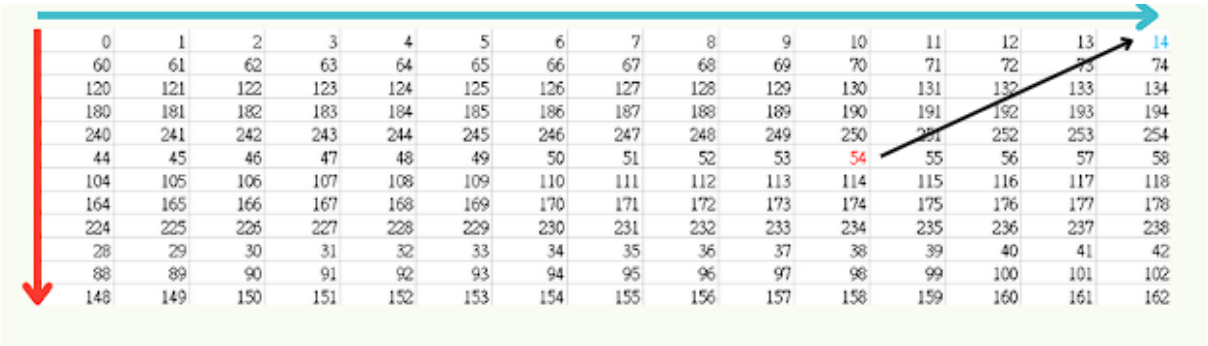


figure 2: APPM 嵌入示意圖

5.4 方法與步驟 ：

以下步驟分為傳送方和接收方，傳送方負責嵌入驗證碼，接收方負責驗證圖片是否遭篡改:

- **以下為傳送方的介紹 ：**

1. 生成參考表和 extra_table :

我們透過 APPM 技術嵌入驗證碼，因此需要建立參考表，因為嵌入量為 8 位元(範圍由 0 至 255)，因此可以視為嵌入 B=256 進制的數字，透過 figure 1 可以得知 c_B 值為 60 ，參考表的大小是 256 × 256，接著透過式(4)即可生成參考表，以下為部分截圖，可以看出參考表在同一列的數字是由左至右循環遞增，值為 0 到 255，且每一列的初始值皆由公式決定，這樣就能在有限距離內找到範圍內的任意數字。

60	61	62	63	64	65	66	67	68
120	121	122	123	124	125	126	127	128
180	181	182	183	184	185	186	187	188
240	241	242	243	244	245	246	247	248
44	45	46	47	48	49	50	51	52

figure 3: 參考表部分截圖

- 參考表的目的在於盡可能將各個數字彼此緊密靠近，讓我們之後在查表時能減少尋找距離。
- 因為距離正比於變化量，因此可以提升圖片品質。

extra_table 是 512(圖片的列大小) × 512(圖片的行大小)的布林陣列，用途在第 2 點進行介紹。

2. 生成並嵌入驗證碼 ：

迭代每個像素，假設目前像素值為 (r, g, b) ，透過式(1)計算灰階值 gv，接著透過 hash function 產生驗證碼 ac 和 ac_2 (兩者差別在於 ac_2 多放入一個數字 32 當成 hash function 的種子碼)，公式如下式(5)式(6) (preshared value 是雙方約定的雜湊參數，預設為 32)，將驗證碼嵌入藍色和紅色通道，以目前的 r, b 為座標，r 為 row，b 為 column，並在參考表中以此座標查找對應位置，接著尋找參考表中值為 ac 或 ac_2 且離該對應位置最近的位置，並記錄此位置的座標，假設找到的座標為 (r', b') ，將像素中的 (r, b) 替換成 (r', b') ，分別對這兩種驗證碼進行嵌入測試，並計算 r, b 的變化量，將 (r, b) 和 (r', b') 視為座標即可計算歐幾里得距離，取變化量較小者作為最終嵌

入的驗證碼，並將此結果記在 extra_table 內，因為只有兩種可能，因此透過布林陣列即可記錄(0 代表嵌入 ac，1 代表嵌入 ac_2)。

這時灰階值會被更改，為了達成灰階不變性，必須透過式(2)調整綠色通道，假設 g' 為 0 到 255 ，嵌入工作就完成了，反之則必須進入無法維持灰階不變性的處理。

$ac = hash(gv,\ i,\ j)$，i,j 為當前像素索引 (5)

$ac_2 = hash(gv, i, j, \text{preshared value})$ (6)

- 無法維持灰階不變性的處理 :

  以下分為兩種情況，分別是 $g' > 255$ 以及 $g' < 0$

  a. $g' > 255$:

     將 g' 透過以下公式折返

     $$g' = 510 - g' \quad (7)$$

  b. $g' < 0$:

     將 g' 透過以下公式折返

     $$g' = -g' \quad (8)$$

雖然這麼做會更使灰階值和原本不同，沒辦法像 Hong 的論文達成完全的灰階不變性，但真正的灰階值會存在參考表中，透過像素的紅色和藍色通道即可取出，在沒有被篡改的情況下可以還原灰階圖。

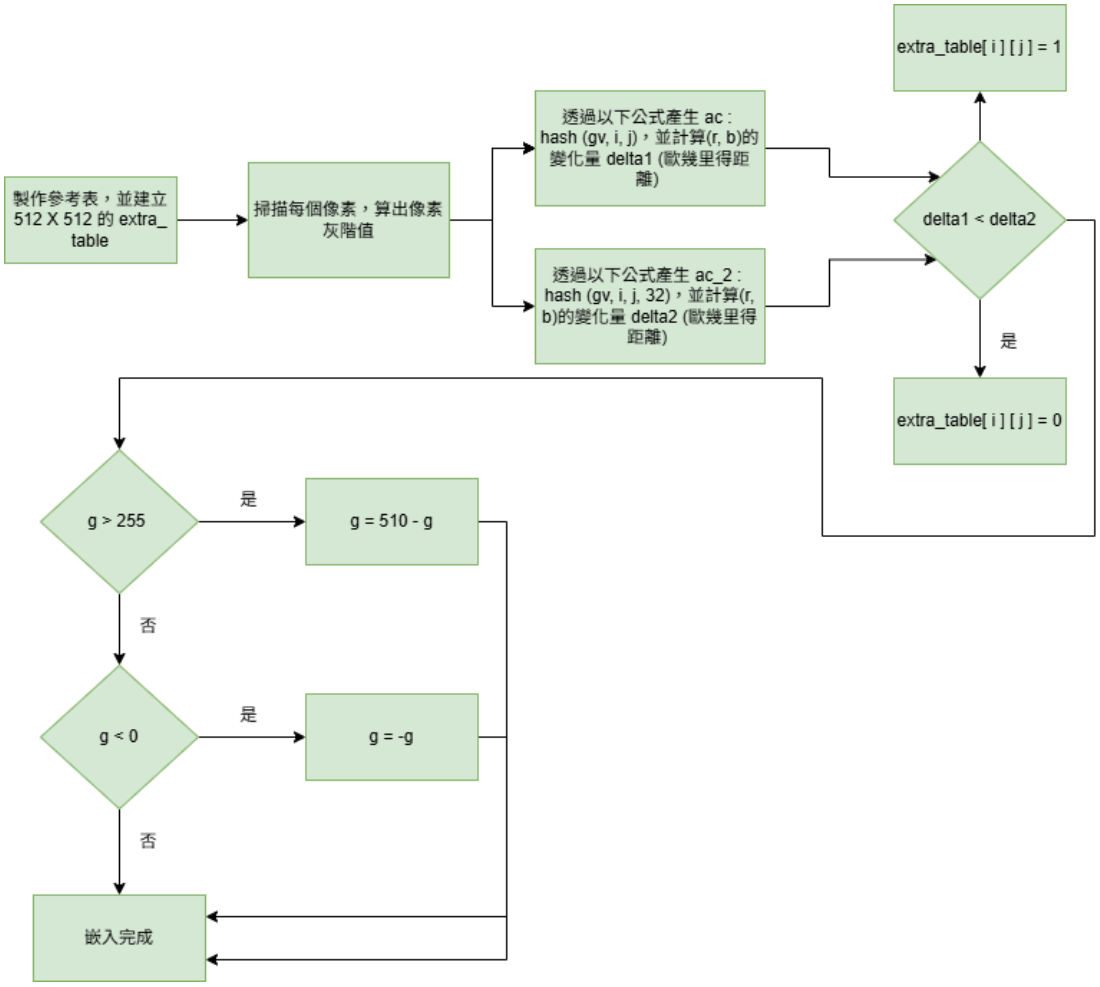


figure 4: 傳送方驗證碼嵌入流程圖

- **以下為接收方的介紹：**

  首先對每個像素迭代，算出灰階值後，透過 extra_table 內的值決定要透過式(5)還是式(6)算出驗證碼 ac'，透過 (r, b) 取出 ac ，檢查 ac' 是否等於 ac，如果是代表沒有被篡改，但如果不同就要進一步判斷，因為有可能是被篡改，也可能是因為折返時調整了 g 導致灰階值改變，進而造成驗證碼不相同。

  折返分為兩種情況：

  a. 如果 g > 128 表示有可能是因為 g 超過 255 而進行折返，因此透過式(7)將 g 折返回去。
  b. 如果 g <= 128 表示有可能是因為 g 小於 0 而進行折返，因此透過式(8)將 g 折返回去。

  g > 128 是一種簡單的劃分，實際上會折返的情況多半在 g 接近邊界(0 或 255)。

  上面兩種情況會執行其中一種，接著重新計算灰階值並放入 hash function，如果算出來的驗證碼和 ac' 相同表示沒有被篡改，否則就是有被篡改。

六、 系統實現與實驗：

- **實驗方法：**

  本研究採用 USC-SIPI 影像資料庫中的經典圖片進行測試，包括：Baboon、Jet、Sailboat、House、Peppers 以及 Splash ，每張圖片皆是尺寸為 512×512 像素的彩色影像，我們首先透過加密前後的圖片計算 Peak Signal-to-Noise Ratio (PSNR) ，PSNR 是一種計算圖片品質的指標，超過 30dB 以後人眼難以分辨，PSNR 的公式如下：

$$PSNR = 10 \cdot \log_{10}\left(\frac{255^2}{MSE}\right) \quad (9)$$

  其中

$$MSE = \frac{1}{m * n}\sum_{i=1}^{m}\sum_{j=1}^{n}|I(i,j) - I'(i,j)|^2 \quad (10)$$

  其中 I 為原始影像的像素值，I' 為修改後的影像的像素值。

比較處理前後的灰階圖差異，接著用程式模擬篡改過程，例如：在 Lena 頭上放一朵花，檢查圖片是否被篡改，同時計算偵測率 (被檢測出篡改的像素數量除以受更改的像素總量)。

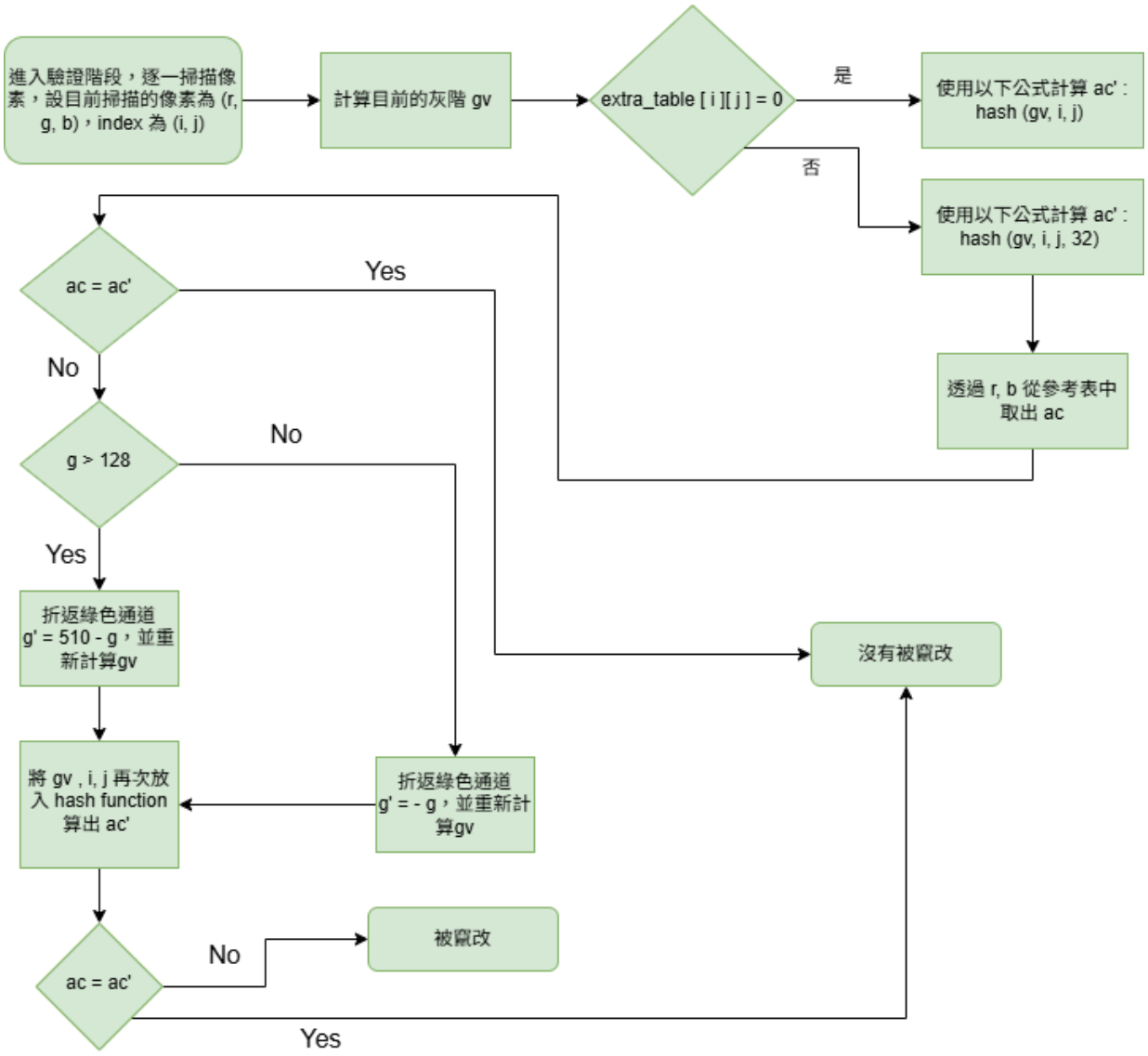


figure 5: 接收者驗證流程圖

figure 6: 測試影像

- **實驗結果：**

  以下為本篇文章的實驗數據和 Hong 等人在 2020 [1]和 2023 [2]的比較，每張圖片的每個像素皆嵌入 8 位元的驗證碼，可以看到除了 Tiffany 以外，本篇提出的方法 PSNR 皆在 37 左右，Outlier 指的是 unsolvable case，也就是無法嵌入完整的 8 位元，只能嵌入 2 位元的情況，此定義出自 Hong 的論文，由於我們的方法不須硬性規定像素的灰階值相同，因此必定可以嵌入 8 位元的驗證碼，Outlier 皆為 0

	Hong's_method (2020)		Hong's_method (2023)		proposed	
Image	PSNR	Outlier	PSNR	Outlier	PSNR	Outlier
Baboon	33.01	73	34.80	11	37.94	0
house	32.85	414	34.63	7	35.98	0
Jet	33.01	153	34.81	0	37.94	0
Lena	32.91	11	34.82	0	37.92	0
Peppers	33.00	7492	36.18	6	37.92	0
Sailboat	33.00	615	36.84	3	37.94	0
Splash	33.04	5441	35.94	0	37.72	0
Tiffany	31.71	24328	35.21	7	37.93	0

figure 7：本篇文章提出的方法的影像品質和 Hong 等人的論文比較

	Hong's method (2020)		Hong's method (2023)		Proposed	
Picture	Tiffany	Peppers	Tiffany	Peppers	Tiffany	Peppers
Number of Tempered pixels	82838	46633	82838	46633	70375	21548
Percent of Tampering	31.60%	17.79%	31.60%	17.79%	26.84%	8.22%
Number of Detection	76122	41160	82447	46445	69841	21363
Detection rate	91.98%	88.26%	99.53%	99.60%	99.24%	99.14%

figure 8: 本篇文章提出的方法的偵測率和 Hong 等人的論文比較

七、 效能評估與成果：

為了檢測本實驗的效能提升，將此實驗與相關研究進行各項指標的對比。有別於其他相關研究本實驗的核心驗證碼經過參考表的輔助取代直接嵌入至低位元是否能有效提升圖片品質是本實驗的研究目的，從上方的圖片品質比較 (figure 7) 能直觀的看出確實有明顯的提升，提升的幅度約 6% (以 PSNR 為指標)，為了更加全面的了解本實驗與相關研究的差異，以及判斷圖像品質的提升是否是犧牲了其他指標換來的結果，以下是完整的比較:

	Hong's method (2020)	Hong's method (2023)	Proposed
Average_PSNR	33.87	35.63	37.66
Detection rate	90.12%	99.57%	99.47%
Average_Payload	1787316	2087243	2097152
Grayscale_invariance	complete	complete	approximate

figure 9: 本篇文章提出的方法和 Hong 等人的論文的各項指標比較

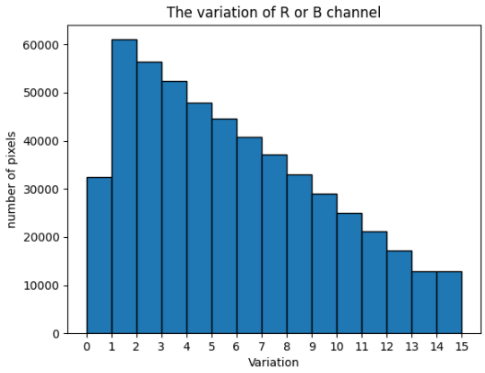
相較於 Hong's method (2020)，我們的各項數據幾乎都有大幅度的提升，而對比於 Hong's method (2023)，我們的影像品質(PSNR)也有了明顯的提升，雖然我們的 Payload 較 Hong's method (2023)多，但是因為我們的方法有折返的可能性，因此偵測率略低於 Hong's method (2023)，最後也是最重要的指標灰階不變性，雖然我們只有接近灰階不變性，但這只是因為折返的像素儲存於圖片時無法保持灰階不變性，但只需要透過參考表依然可以將灰階值復原，因此就灰階不變這個目的而言，我們的方法依然能夠達成。

以下為偵測篡改實驗，黑色部分是判定為未遭到篡改，白色則為遭到篡改，可以發現在 Lena 圖中嵌入(篡改)了一朵紅花，基本上明顯地被偵測出來，至於花朵中的黑色小點則是誤差

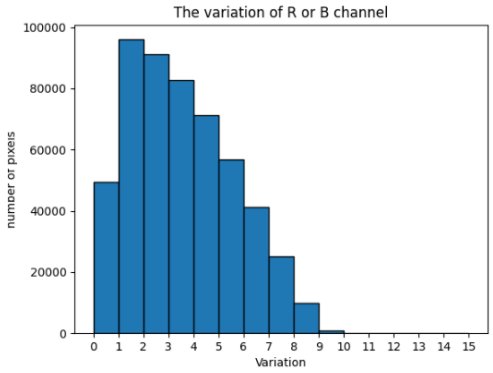
figure 10 偵測篡改圖像

為了檢測 APPM 嵌入法是否真的能夠有效減少嵌入驗證碼時造成的像素變化，我們記錄每個像素在嵌入驗證碼時紅色與藍色通道的變化量，並將其存入一個表格中，統計每個變化量（從 0 到 16）分別對應了多少個像素通道(一個像素有三個像素通道，但因為綠色通道變化較小，因此聚焦於紅色及藍色兩像素通道)，接著繪製成如下的直方圖，橫軸是 r 或 b 的變化量，縱軸是對應的像素量，因為是 r, b 合在一起算，因此每個直條加總最大值是 2x512x512。

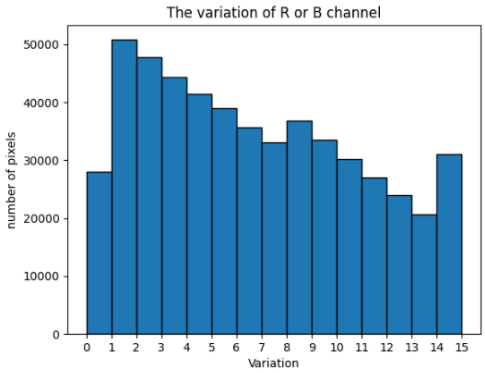
Lena_Hong(2020)



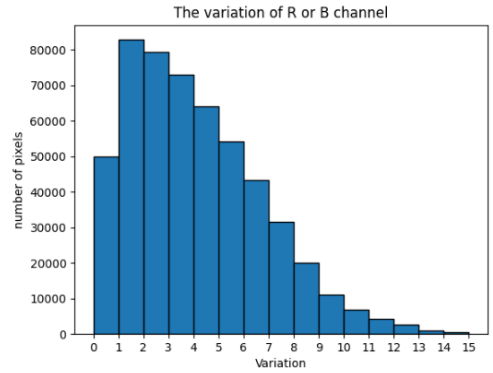
Lena_proposed



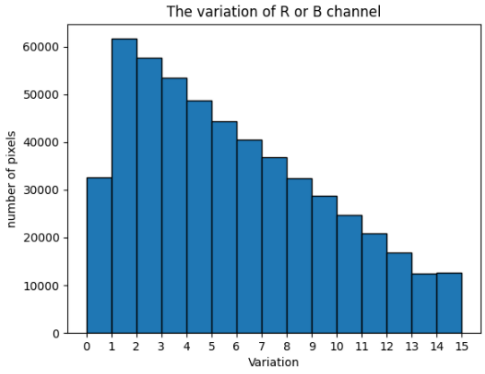
Tiffany_Hong(2020)



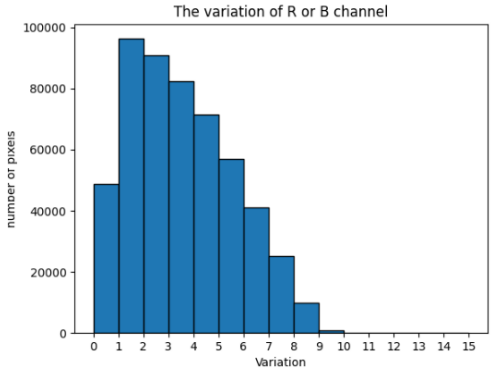
Tiffany_proposed



Sailboat_Hong(2020)



Sailboat_proposed



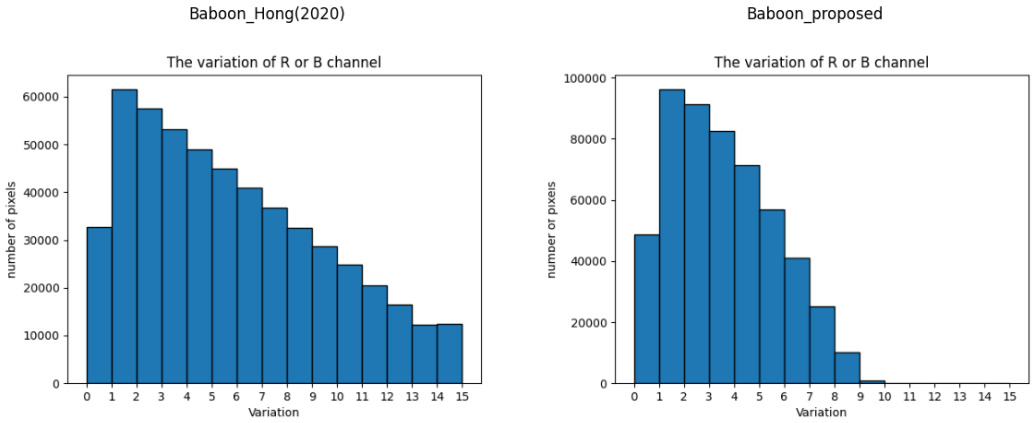


figure 11： 不同圖片下使用 Hong (2020) 和我們提出的方法所造成的像素變化量

與 Hong (2020)，我們的方法造成的變化量明顯較低，絕大部分的圖片變化量都沒有超過 10，即便是整體偏亮的 Tiffany，變化量較高的像素也很少，可以說明使用 APPM 嵌入法可以有效降低 r, b 變化量。

以下是本類別研究的最終目的灰階不變性，左上角為原圖的灰階圖，右上角為原圖的輪廓，左下角為由本研究嵌入驗證碼後的輪廓，右下角為單純嵌入驗證碼而未顧及灰階不變性的圖片輪廓，由此可知維持灰階不變性在邊緣偵測時能夠保持輪廓。

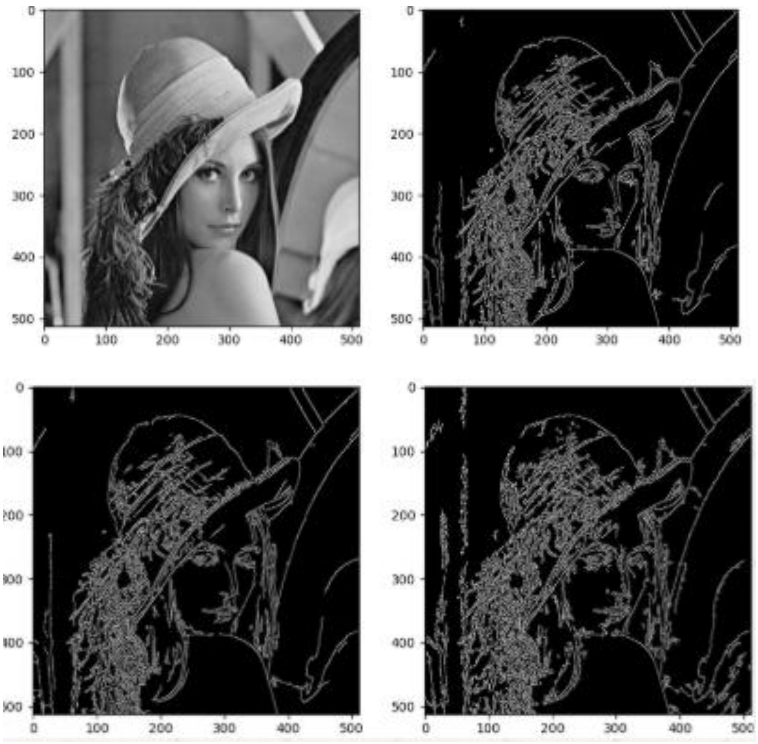


figure 12:比較原圖、灰階不變性嵌入法、未灰階不變性嵌入法的輪廓分析

八、 結論 ：

本研究成功實現一套基於 APPM 且具近似灰階不變性的彩色影像驗證，兼顧影像品質與篡改偵測能力。透過參考表輔助的驗證碼嵌入方式，有效降低像素變化量，提升影像品質，實驗顯示平均 PSNR 值可達 37 dB 以上，明顯優於既有方法。此外，本系統亦具備完整的驗證流程與高準確度之篡改定位能力，能應對各類圖像異動情境。雖然本方法在某些極端情況下無法完全維持灰階值，但透過折返設計，仍可從參考表中還原正確灰階資訊，實現功能上的灰階一致性。未來可進一步結合深度學習模型進行智慧驗證碼設計，提升系統於真實應用中的強健性與彈性。

九、 參考資料 ：

[1] Hong, W., Chen, J., Chang, P.-S., Wu, J., Chen, T.-S., & Lin, J. (2020). A Color Image Authentication Scheme With Grayscale Invariance. IEEE Access, 8, 3047270.

[2] X. Zhou, W. Hong, G. Yang, T.-S. Chen, J. Chen, “An Unsolvable Pixel Reduced Authentication Method for Color Images with Grayscale Invariance,” Journal of King Saud University - Computer and Information Sciences, Volume 35, Issue 9, 2023, 101726.

[3] Chao, R.-M., Wu, H.-C., Lee, C.-C., & Chu, Y.-P. (2009). A Novel Image Data Hiding Scheme with Diamond Encoding. EURASIP Journal on Information Security, 2009, Article ID 658047.

[4] W. Hong and T.S. Chen, “A Novel Data Embedding Method Using Adaptive Pixel Pair Matching,” IEEE Transactions on Information Forensics and Security, vol. 7,no. 1, pp. 176-184, 2012.