



ISO 9001 : 2008

TRƯỜNG ĐẠI HỌC TRÀ VINH  
**HỘI ĐỒNG KHOA HỌC**

**BÁO CÁO TỔNG KẾT**  
**ĐỀ TÀI NGHIÊN CỨU KHOA HỌC CẤP TRƯỜNG**

**KỸ THUẬT THỦY VÂN TRONG XÁC NHẬN**  
**BẢN QUYỀN SỐ**

Chủ nhiệm đề tài: **TS. NGUYỄN THÁI SƠN**  
Chức danh: **Giảng viên**  
Đơn vị: **Khoa Kỹ thuật và Công nghệ**

*Trà Vinh, ngày 02 tháng 08 năm 2017*



ISO 9001 : 2008

TRƯỜNG ĐẠI HỌC TRÀ VINH  
**HỘI ĐỒNG KHOA HỌC**

**BÁO CÁO TỔNG KẾT**  
**ĐỀ TÀI NGHIÊN CỨU KHOA HỌC CẤP TRƯỜNG**

**KỸ THUẬT THỦY VÂN TRONG XÁC NHẬN**  
**BẢN QUYỀN SỐ**

**Xác nhận của cơ quan chủ quản**

*(Ký, đóng dấu, ghi rõ họ tên)*

**Chủ nhiệm đề tài**

*(Ký, ghi rõ họ tên)*

**Nguyễn Thái Sơn**

*Trà Vinh, ngày 02 tháng 08 năm 2017*

## TÓM TẮT

Xác nhận bản quyền số thuận nghịch thu hút được nhiều sự quan tâm của các nhà khoa học do kỹ thuật này có khả năng khôi phục lại dữ liệu gốc của những ảnh mang tin mà không có bất kỳ thay đổi nào sau khi được xác nhận. Trong đề tài này, chúng tôi đưa ra một giải pháp xác nhận bản quyền số thuận nghịch mới dựa vào tiên đoán hình thoi và đánh giá độ phức tạp. Để đảm bảo chất lượng ảnh đã mang tin cao và đạt được độ chính xác cao trong kiểm tra giả mạo, đánh giá độ phức tạp được thực hiện trên mỗi điểm ảnh. Sau đó, những lỗi tiên đoán được tính toán dựa vào tiên đoán hình thoi cho việc giấu mã xác nhận. Kết quả thực nghiệm thể hiện rằng giải pháp đề xuất có khả năng khôi phục lại phiên bản gốc của ảnh chủ. Ngoài ra, giải pháp đề xuất còn đạt được các hiệu quả tốt hơn so với các giải pháp trước xét về mặt kiểm tra giả mạo và chất lượng ảnh.

Reversible image authentication attracts much attention of researchers since such technique has ability to reconstruct the original version of the host image losslessly after image authentication. In this paper, we propose a new reversible image authentication based on rhombus prediction and local complexity. To maintain good quality of stego images and to achieve high accuracy of tamper detection, the local complexity of each pixel is first evaluated, then, the prediction error is calculated by using rhombus prediction for embedding the authentication code. Experimental results demonstrated that the proposed scheme has ability to recover the original version of the host images. In addition, the proposed scheme obtains better performance than previous schemes in terms of tamper detection and image quality.

## MỤC LỤC

LỜI CẢM ƠN .....	7
PHẦN MỞ ĐẦU .....	8
1. Tính cấp thiết của đề tài .....	8
2. Tổng quan nghiên cứu.....	8
3. Mục tiêu.....	9
4. Đối tượng, phạm vi và phương pháp nghiên cứu.....	10
PHẦN NỘI DUNG .....	11
CHƯƠNG 1. Giải pháp đề xuất.....	11
CHƯƠNG 2. So sánh và đánh giá kết quả thực nghiệm của giải pháp mới được đề xuất	17
PHẦN KẾT LUẬN .....	25
TÀI LIỆU THAM KHẢO .....	26

## DANH MỤC BẢNG BIỂU

<b>Table 1.</b> Embedding capacity (bits) under different thresholds .....	17
<b>Table 2.</b> Visual quality (dB) under different thresholds .....	17
<b>Table 3.</b> Performance comparison of the proposed scheme and Lo and Hu's scheme for the tamper object A1 .....	20
<b>Table 4.</b> Performance comparison of the proposed scheme and Lo and Hu's scheme for the tamper object B1 .....	20
<b>Table 5.</b> Performance comparison of the proposed scheme and Lo and Hu's scheme for the tamper object C1 .....	21
<b>Table 6.</b> Performance comparison of the proposed scheme and Lo and Hu's scheme for the tamper object D1 .....	22
<b>Table 7.</b> Performance comparison of the proposed scheme with previous image authentication schemes .....	23

## DANH MỤC CÁC BIỂU ĐỒ, SƠ ĐỒ, HÌNH ẢNH

<b>Figure 1.</b> Flowchart of the embedding procedure .....	11
<b>Figure 2.</b> Illustration of the host image with black and white sets .....	12
<b>Figure 3.</b> Flowchart of the extracting procedure.....	14
<b>Figure 4.</b> The current processing block B with white color implying the legal block and with black color implying the tampered block.....	16
<b>Figure 5.</b> Six test images with the size of $512 \times 512$ .....	16
<b>Figure 6.</b> A1, B1, C1, and D1 are four tampered color objects. A2, B2, C2, and D2 are four corresponding grayscale objects. A3, B3, C3, and D3 are four corresponding tampered images.....	19

## LỜI CẢM ƠN

Tôi xin gửi lời cảm ơn chân thành và sự tri ân sâu sắc đối với trường Đại học Trà Vinh, đặc biệt là Khoa Kỹ thuật & Công nghệ của trường đã giành nhiều thời gian cho tôi thực hiện đề tài nghiên cứu khoa học tại Khoa. Đồng thời, nhà trường đã tạo cho tôi có cơ hội được tìm hiểu và áp dụng những kiến thức sâu rộng của khoa học máy tính vào một đề tài cụ thể. Qua thời gian thực hiện đề tài này tôi nhận ra nhiều kiến thức mới mẻ và bổ ích trong việc nghiên cứu và giảng dạy để giúp ích cho công việc hiện tại và sau này của tôi.

*Tôi xin chân thành cảm ơn!*

## PHẦN MỞ ĐẦU

### 1. Tính cấp thiết của đề tài

Với sự phát triển mạnh của đa phương tiện và mạng máy tính, dữ liệu số đã được dùng một cách rộng rãi để thay thế những dữ liệu được lưu trữ theo cách truyền thống. Khi dữ liệu số được truyền trên một kênh phổ thông như mạng Internet, những dữ liệu số này phải đối mặt với những sửa đổi, sao chép một cách không hợp pháp hay giả mạo từ những kẻ tấn công. Chính vì vậy, vấn đề bảo vệ sự an toàn và bảo mật của thông tin được lưu trữ hay được truyền đi trở thành một vấn đề rất quan trọng và cấp thiết. Điều này thu hút sự quan tâm đặc biệt của các nhà nghiên cứu trong nhiều lĩnh vực khác nhau. Nhiều giải pháp đã được đưa ra để giải quyết vấn đề này, như mã hoá thông tin (cryptography) [34-35] và thuỷ vân số (watermarking) [1-33]. Trong đó, thuỷ vân số được xem như một trong những giải pháp hứa hẹn nhất hiện nay. Thuỷ vân số là một phương pháp nhúng thông tin bí mật, ví dụ như logo của doanh nghiệp, vào dữ liệu đa phương tiện gốc, ví dụ như văn bản, hình ảnh, audio, và video, để tránh sự quan tâm của những kẻ tấn công (attackers) vào thông tin được nhúng. Vì vậy thuỷ vân số đảm bảo được sự an toàn của thông tin mật được nhúng. Thuỷ vân số có thể được phân loại dựa trên miền của dữ liệu gốc chứa tin, như miền không gian (spatial domain), miền tần số (frequency domain), miền nén (compression domain). Trong các năm gần đây việc mất an toàn thông tin diễn ra một cách mạnh mẽ hơn. Do đó, việc nghiên cứu và đề xuất các giải pháp thuỷ vân số mới với tính bảo mật cao hơn phần nào giúp giảm bớt sự tấn công của những người không được phép, điều này thu hút sự quan tâm của rất nhiều nhà nghiên cứu trong và ngoài nước.

### 2. Tổng quan nghiên cứu

Trong các năm qua, nhiều giải pháp thuỷ vân số cho ảnh số đã được giới thiệu trên thế giới. Năm 2008, Lee and Lin [1] đề xuất một kỹ thuật thuỷ vân số, giải pháp này không những có thể kiểm tra được vùng giả mạo trên ảnh đã được nhúng thông tin mật, mà còn có khả năng khôi phục dữ liệu gốc của khu vực đã bị giả mạo đó. Trong giải pháp của Lee and Lin, mỗi khối ảnh có thể được dùng để chứa dữ liệu mật và dữ liệu nén của hai khối ảnh khác. Năm 2010, Ahmed and Siyal [2] đưa ra một giải pháp thuỷ vân số để xác nhận ảnh dựa trên hàm băm (hash function). Giải pháp của Ahmed and Siyal đạt được tính bền vững (robustness) đối với một vài kiểu tấn công như: nén JPEG, lọc bỏ qua phần trầm (low-pass filtering) và lọc bỏ qua phần cao (high-pass filtering). Đến năm 2011, để chống lại những thay đổi bất hợp pháp trên ảnh nén lượng tử vector (vector quantization compressed image), Chuang and Hu [3] giới thiệu một phương pháp thuỷ vân số mới. Trong phương pháp này, hai tập của dữ liệu xác nhận được sử dụng để xử lý kiểm tra giả mạo và xác nhận với ảnh nén đã được cung cấp. Tuy nhiên, chất lượng của ảnh chứa tin còn thấp. Sau đó, năm 2013, để cải thiện những yếu kém trong giải thuật của



Chuang and Hu, Hu và cộng sự [4] đã đề xuất giải pháp thủy vân số mới cho ảnh số kết hợp với phương pháp nén BTC (block truncation code). Trong [4], mã xác nhận của khối ảnh sẽ được tạo ra từ mức lượng tử của ảnh nén. Sau đó, nhiều bản sao của mã xác nhận sẽ được giấu trong bản đồ bit (bit map) bằng phương pháp hoán vị (permutation operation). Năm 2014, chúng tôi [5] đã đề xuất một phương pháp thủy vân số mới trong việc bảo vệ toàn vẹn dữ liệu ảnh nén BTC. Để đạt được chất lượng ảnh tốt hơn, một bảng tham chiếu (reference table) được thiết lập và được dùng trong khi giấu những mã xác nhận. Vì vậy, chất lượng ảnh được cải thiện trong giải pháp của chúng tôi. Tuy nhiên, bằng cách dựa vào miền không gian và miền nén để giấu thông tin mật và áp dụng cho việc xác nhận nhưng thay đổi không hợp pháp trên ảnh số, đa số các giải pháp đã đề xuất [1-5] đều làm giảm đáng kể chất lượng của ảnh chứa tin mật, luôn nhỏ hơn 50 dB. Để nâng cao chất lượng của ảnh chứa tin, trong [6], Preda đã giới thiệu một giải pháp thủy vân số mới dùng trong xác nhận ảnh số trên miền tần số, cụ thể là sử dụng miền phép biến đổi sóng nhỏ rời rạc (discrete wavelet transform - DWT). Trong giải pháp này [6], thông tin mật được nhúng vào những hệ số được lựa chọn (selected coefficients) bằng phương pháp lượng tử trung bình (mean quantization), nhưng độ chính xác trong việc xác nhận ảnh bị giả mạo còn chưa cao. Cũng dựa vào miền DWT, Al-Otum [7] thực hiện kỹ thuật thay đổi hệ số DWT đã được lượng tử để giấu thông tin mật áp dụng cho việc xác nhận ảnh số. Giải pháp này đã giúp cải thiện được độ chính xác trong việc xác nhận khu vực giả mạo trên ảnh. Tuy nhiên, chất lượng ảnh đạt được bởi giải pháp của Al-Otum thì thấp hơn giải pháp của Preda. Trong cả 2 giải pháp này [6, 7], mặc dù chất lượng ảnh chứa tin đã được cải thiện, nhưng vẫn còn thấp (nhỏ hơn 70 dB). Vì thế, trong [8], chúng tôi áp dụng lớp hệ số DWT thứ hai (2nd DWT subbands) để giải quyết bài toán nâng cao chất lượng của ảnh chứa tin cũng như tăng độ chính xác trong việc xác nhận các khu vực trên ảnh bị giả mạo. Việc đạt được độ chính xác cao trong xác nhận những khu vực bị giả mạo trong dữ liệu số, như ảnh mức xám, cũng như đảm bảo được độ phân giải cao của dữ liệu số chứa tin thì được các nhà khoa học đặc biệt quan tâm và đề xuất cách giải quyết trong các kết quả gần đây.

### **3. Mục tiêu**

- Tìm hiểu đặc trưng của ảnh mức xám
- Nghiên cứu các giải pháp thủy vân số trên các miền không gian khác nhau
- Đề xuất được phương pháp thủy vân số mới có khả năng xác nhận những khu vực trên ảnh bị giả mạo.

- So sánh và đánh giá kết quả thực nghiệm của chúng tôi với các giải pháp đã được đề xuất trước .

#### **4. Đối tượng, phạm vi và phương pháp nghiên cứu**

4.1. **Đối tượng, địa điểm và thời gian nghiên cứu:** Xác nhận bản quyền số trên ảnh mức xám.

4.2. **Quy mô nghiên cứu:** Đề tài cấp trường thực hiện một năm trên tập ảnh mức xám.

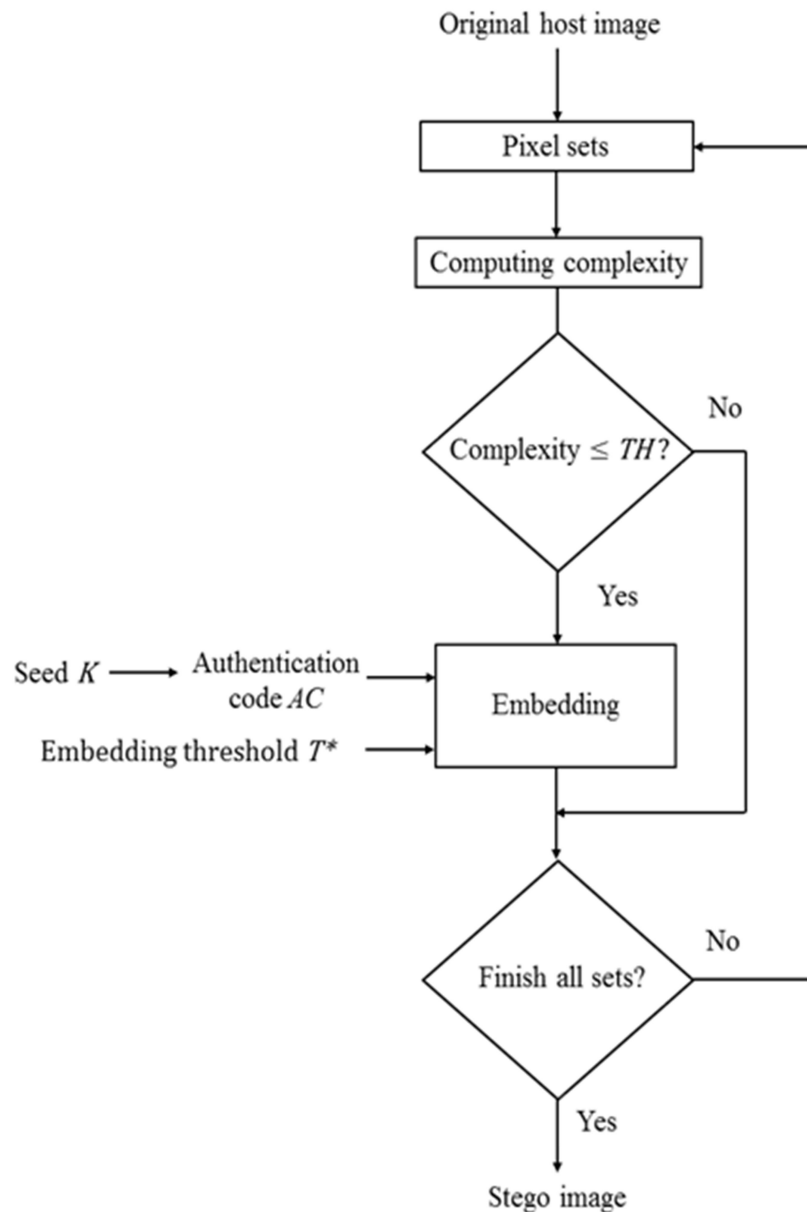
#### **4.3. Phương pháp nghiên cứu**

- Chúng tôi sẽ phân tích, đánh giá, tổng hợp các đặc điểm đặc trưng (feature point) trên ảnh mức xám
- Nghiên cứu các giải pháp thủy văn số trên miền tần số (frequency domain).
- Chọn lọc các ưu điểm để xây dựng một lý thuyết phù hợp cho các giải pháp thủy văn số mới trên miền tần số của ảnh xám.

## PHẦN NỘI DUNG

### CHƯƠNG 1. Giải pháp đề xuất

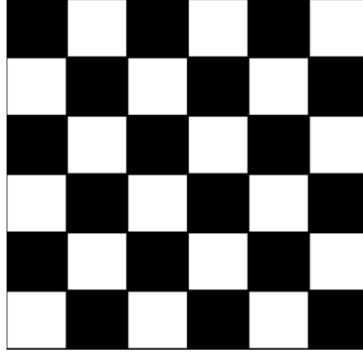
In this paper, a novel reversible image authentication scheme is proposed to protect the integrity of digital images. First, the authentication code is generated and embedded into the host image to generate a stego image. Then, if the stego image is suspected to be tampered, the proposed tamper detection algorithm can be used to detect whether or not the stego image is modified. Otherwise, if none of modified regions are encountered, the stego image can be recovered to its original version without any distortion. Figure 1 shows the flowchart of the proposed embedding procedure.



**Figure 1.** Flowchart of the embedding procedure

## 1. Image partition and authentication code generation

Assume that the host image  $I$  is a grayscale image with the size of  $W \times H$  pixels. Let  $I_{i,j}$  denotes the pixel at the  $i^{\text{th}}$  row and the  $j^{\text{th}}$  column in the host image. The image  $I$  is partitioned into two sets: black set  $S_B = \{I_{i,j}: i \equiv j \pmod{2}\}$  and white set  $S_W = \{I_{i,j}: I_{i,j} \notin S_B\}$ . Figure 2 illustrates the host image with two sets after image partition. The, an authentication code  $AC$  in the binary form is generated by pseudo random number generator (PRNG) with a seed  $K$ . Each bit of  $AC$  corresponds to each pixel in the host image. Therefore, there are totally  $W \times H$  bits in authentication code  $AC$ . By using the same seed  $K$ , PRNG can regenerate the same authentication code. Take the advantage of this property, we only record  $K$  in order to regenerate same authentication code for detecting the tampered region in the stego images.



**Figure 2.** Illustration of the host image with black and white sets

## 2. Embedding procedure

In this subsection, we describe how the authentication code bit is embedded into each pixel of the host image. As illustrated in Figure 1, for a given host image  $I$  with the size of  $W \times H$  and three parameters, including the seed  $K$ , the embedding threshold  $T^*$  and the complexity threshold  $TH$ , the authentication code is generated and embedded. The embedding algorithm consists of five main steps as followings.

**Step 1:** The host image  $I$  is partitioned into two sets of pixels, i.e., the black set  $S_B$  and the white set  $S_W$ .

**Step 2:** From left to right and up to bottom, for each pixel  $I_{ij}$  in the set  $S_B$ , the average value  $Avg$ , also called as the predicted value, and the *Complexity* are calculated according to four adjacent pixels in the set  $S_W$  by using Equations (1) and (2), respectively.

$$Avg = \left\lfloor \frac{I_{i,j-1} + I_{i-1,j} + I_{i,j+1} + I_{i+1,j}}{4} \right\rfloor, \quad (1)$$

$$\begin{aligned} & \text{Complexity} \quad (2) \\ & = \max(I_{i,j-1} - Avg, I_{i-1,j} - Avg, I_{i,j+1} - Avg, I_{i+1,j} \\ & \quad - Avg). \end{aligned}$$

Notice that if  $I_{i,j}$  is located at the corner or the boundary of the image, meaning that some adjacent pixels are missing. In other words,  $I_{i,j}$  does not have enough four adjacent pixels. In this scenario, the average value  $Avg$  and  $Complexity$  can be computed according to the rest of adjacent pixels.

Then, the local complexity of the current pixel  $I_{ij}$  is evaluated by comparing the value of  $Complexity$  with the predefined complexity threshold  $TH$ . If  $Complexity$  is less than or equal to  $TH$ , go to Step 3 for further processing. Otherwise, read the next black pixel and re-perform this step.

**Step 3:** Read the authentication code bit  $w$  from  $AC$  and embed it into  $I_{i,j}$  by using Equation (3).

$$d' = \begin{cases} d \times 2 + w & \text{if } -T^* \leq d \leq T^* \\ d - T^* & \text{if } -T^* > d \\ d + T^* + 1 & \text{if } T^* < d \end{cases}, \quad (3)$$

where  $d$  is the different value between the current black pixel and the average value, which is calculated as  $d = I_{i,j} - Avg$ , and  $T^*$  is the embedding threshold.

**Step 4:** The stego pixel  $I'_{i,j}$  is then calculated by using Equation (4).

$$I'_{i,j} = Avg + d'. \quad (4)$$

**Step 5:** Repeat Steps 2 to 4 until all of pixels in the black set  $S_B$  are embedded the authentication code completely.

According to the values of stego pixels of the black set  $S_B$ , the similar process is used to embed the authentication code into the pixels of the white set  $S_W$ . Eventually, the stego image is constructed by combination of stego pixels of the black set and the white set. It is notable that although the small value of pixels is modified for embedding the authentication code, the overflow/underflow problems also may be occurred during embedding process. Therefore, to avoid the overflow/underflow problems, each pixel should be considered by using Equation (5) before embedding process.

$$\begin{cases} 0 \leq P_{i,j} + 2d + 1 \leq 255 & \text{if } -T^* \leq d \leq T^* \\ P_{i,j} < 255 - T^* & \text{if } d > T^* \\ P_{i,j} \geq T^* & \text{if } d < -T^* \end{cases}, \quad (5)$$

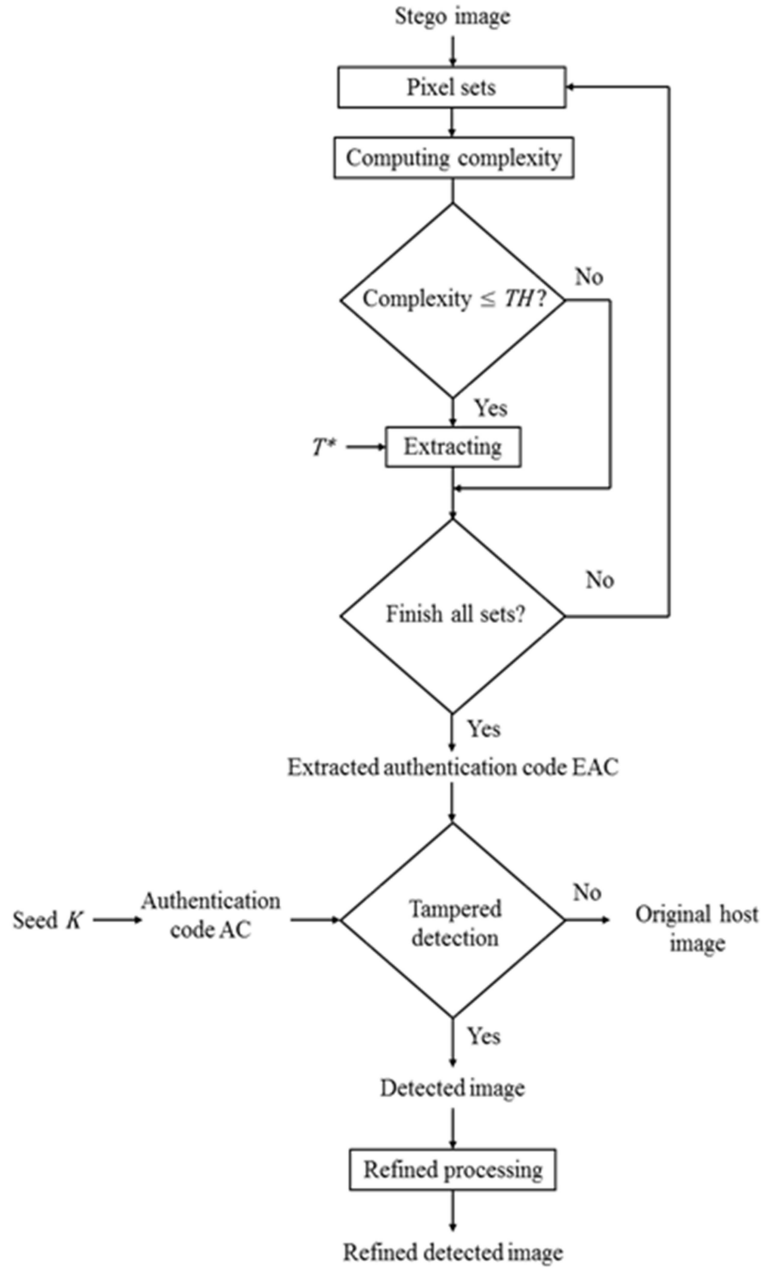
where  $T^*$  is a predefined embedding threshold. If  $I_{i,j}$  does not satisfy Equation (5), meaning that overflow/underflow is occurred if the pixel is used for embedding. Therefore, the location of  $I_{i,j}$ , is recorded and we leave it without embedding process.

To extract the authentication code successfully and to recover the host image losslessly, the side information should be required by the receiver during the extracting process. This side information consists of three parameters, i.e.,  $K$ ,  $TH$ ,  $T^*$ , and the overflow/underflow locations. To avoid the requirement of extra information, the proposed scheme preserves some

last rows of image  $I$  for transferring such side information by using the least significant bits (LSBs) replacement. Let these last rows be  $R$  and they do not use during embedding the authentication code. For reversibility reason, the LSBs of  $R$  are read to construct the bit sequence  $S_{LSB}^R$  in order to preserve space for the side information. Then, the bit sequence  $S_{LSB}^R$  is concatenated into the authentication code  $AC$ . Assume that the length of the side information is  $L$ , then, the bit sequence  $S_{LSB}^R$  is constructed by recording LSBs of  $round(\frac{L}{2 \times W})$  last rows in the  $W \times H$  image. If the embedding capacity of the proposed scheme in the current image is  $EC$ , the authentication code  $AC$  is generated with the length of  $\left[ EC - 2 \times round(\frac{L}{2 \times W}) \right]$  bits. Therefore, after the entire authentication code is embedded into the host image completely, the embedding procedure is used continually to embed the bit sequence  $S_{LSB}^R$  into the host image. Eventually, the side information is embedded into the LSBs of  $R$  by LSBs replacement. By doing so, no extra information is required in the proposed scheme.

### **2.3 Extracting procedure**

Once obtaining the stego image  $I'$ , if the receiver suspects that the image is tampered, he/she can use the extracting algorithm for verifying the tampered regions. If none of regions are modified; the image can be recovered to its original version for further processing. Figure 3 shows the flowchart of the extracting procedure.



**Figure 3.** Flowchart of the extracting procedure

The extracting algorithm can be divided into six main steps which are described as followings.

**Step 1:** Extract the side information, i.e., three parameters, i.e.,  $K$ ,  $TH$ ,  $T^*$ , and overflow/underflow locations, from LSBs of the region  $R$  in the stego image. Then, the authentication code  $AC$  is re-constructed by using PRNG with the seed  $K$ .

**Step 2:** Partition the stego image into two sets, the black set  $S_B$  and the white set  $S_W$ . According to the raster scan order as was done in the embedding algorithm, the authentication code is first extracted from the set  $S_W$ .

**Step 3:** For each pixel  $I'_{i,j}$  in  $S_W$ , the average value  $Avg$  and the complexity value  $Complexity$  are re-calculated by using Equations (1) and (2). Then, the complexity of  $I'_{i,j}$  is determined by comparing the value of  $Complexity$  with the complexity threshold  $TH$ . If  $Complexity$  is less than or equal to  $TH$ , meaning that this pixel was used to carry the authentication code bit, then, go to Step 4. Otherwise, read the next white pixel and re-perform this step.

**Step 4:** Calculate the different value as  $d' = I'_{i,j} - Avg$ . Then, the original different value  $d$  is re-constructed by using Equation (6).

$$d = \begin{cases} \lfloor \frac{d'}{2} \rfloor, & -2T^* \leq d' \leq 2T^* + 1 \\ d' + T^*, & d' < -2T^* \\ d' - T^* - 1, & 2T^* + 1 < d' \end{cases}, \quad (6)$$

where  $\lfloor \cdot \rfloor$  is floor function. If  $-2T^* \leq d' \leq 2T^* + 1$ , a authentication code bit  $w'$  can be extracted by Equation (7), and the original pixel can be reconstructed by using Equation (8).

$$w' = d' \bmod 2, \quad (7)$$

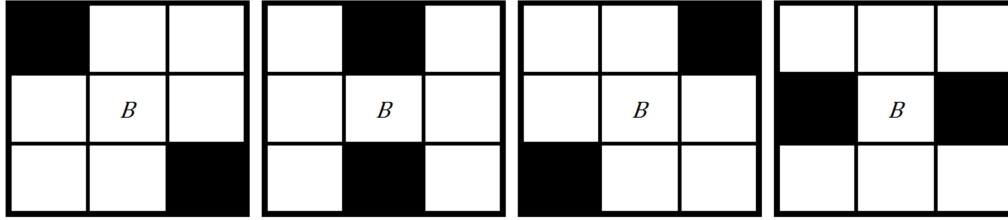
$$I_{i,j} = d + Avg. \quad (8)$$

**Step 5:** Steps 3 and 4 are performed repeatedly to extract all embedded authentication code  $EAC_W$  from the set  $S_W$ , and all the pixels in the set  $S_W$  are reconstructed losslessly. Based on the pixels in  $S_W$ , the similar process is used to extract the embedding authentication code  $EAC_B$  from the set  $S_B$ . Then, the embedded authentication code  $EAC$  is generated by combination of  $EAC_W$  and  $EAC_B$ . To detect the tampered regions, each bit  $w'$  in  $EAC$  is compared with the corresponding bit  $w$  in the authentication code  $AC$ . If  $w' = w$ , the corresponding pixel is not modified, and it is marked as a legal pixel. Otherwise, this pixel is marked as a tampered pixel. If none of tampered pixels is encountered, the original image  $I$  is restored according to two reconstructed sets,  $S_B$  and  $S_W$ . Otherwise, the image is divided into blocks with the size of  $4 \times 4$  pixels. For each block, if there are any tampered pixels, the block is marked as a tampered block. Otherwise, the block is marked as a legal block. Then, the detected image is generated by gathering all of the legal and tampered blocks.

**Step 6:** To improve the accuracy of the detected images, we use a refinement process. In this process, each legal block in the detected image is examined whether or not it belongs to one of the four cases in Figure 4. If a block belongs to one of these four cases, the block is changed to the tampered block. This process will be implemented repeatedly until none of blocks are changed to the tampered block. Eventually, the



refined detected image is obtained and the extracting procedure is terminated.



**Figure 4.** The current processing block  $B$  with white color implying the legal block and with black color implying the tampered block

## CHƯƠNG 2. So sánh và đánh giá kết quả thực nghiệm của giải pháp mới được đề xuất

In this section, we conducted various experiments to evaluate the performance of the proposed scheme. Six test images, i.e., “Airplane,” “Boat,” “Lena,” “Peppers,” “Tiffany,” and “Toys,” shown as Figure 5, are used in the experiment. Different values of the complexity threshold and the embedding threshold, i.e.,  $TH = 4, 8, \text{ or } 14$ , and  $T^* = 0, 1, 2, \text{ or } 3$ , are used for testing. Tables 1 and 2 provide embedding capacity and image quality under such different thresholds. As can be seen in Tables 1 and 2, if the larger values of  $TH$  and  $T^*$  are used, the higher embedding capacity and the lower image quality (PSNR) are obtained. The main reason is when the larger value of threshold is used; more pixels are selected for embedding the authentication code, resulting in the image is distorted significantly.



**Figure 5.** Six test images with the size of  $512 \times 512$

**Table 1.** Embedding capacity (bits) under different thresholds

	Images	$T^* = 0$	$T^* = 1$	$T^* = 2$	$T^* = 3$
$TH = 4$	Airplane	47466	107251	131727	142088
	Boat	26617	65909	88548	102571
	Lena	38251	89532	112646	123030
	Peppers	32444	78258	103224	117226
	Tiffany	35316	84044	109933	124994
	Toys	27504	67445	91021	107345
	<b>Average</b>	<b>34599</b>	<b>82073</b>	<b>106183</b>	<b>119543</b>
$TH = 8$	Airplane	52803	125447	162230	179508
	Boat	30486	80506	116011	138694
	Lena	47347	118457	157968	177213
	Peppers	41508	107144	149791	174817
	Tiffany	41592	105618	146986	171649
	Toys	32545	86736	126522	153313
	<b>Average</b>	<b>41046</b>	<b>103984</b>	<b>143251</b>	<b>165865</b>
$TH = 14$	Airplane	54520	131343	172332	193815
	Boat	32362	86633	126798	154196
	Lena	50757	128819	175107	199670
	Peppers	43661	114771	163370	193958
	Tiffany	43059	110546	156082	185070
	Toys	33670	90781	134223	165675
	<b>Average</b>	<b>43004</b>	<b>110482</b>	<b>154652</b>	<b>182064</b>

**Table 2.** Visual quality (dB) under different thresholds

	Images	$T^*=0$	$T^*=1$	$T^*=2$	$T^*=3$
$TH = 4$	Airplane	52.79	48.27	46.39	45.51
	Boat	53.55	48.29	45.73	44.39
	Lena	53.45	48.72	46.70	45.74
	Peppers	53.30	48.25	45.89	44.70
	Tiffany	52.81	47.76	45.35	44.07
	Toys	53.03	47.70	45.05	43.59
	<b>Average</b>	<b>53.15</b>	<b>48.16</b>	<b>45.85</b>	<b>44.66</b>
$TH = 8$	Airplane	51.85	46.95	44.71	43.57
	Boat	52.44	46.81	43.96	42.37
	Lena	52.09	46.96	44.61	43.46
	Peppers	51.82	46.38	43.74	42.36
	Tiffany	51.61	46.15	43.43	41.94
	Toys	51.98	46.24	43.32	41.68
	<b>Average</b>	<b>51.96</b>	<b>46.58</b>	<b>43.96</b>	<b>42.56</b>

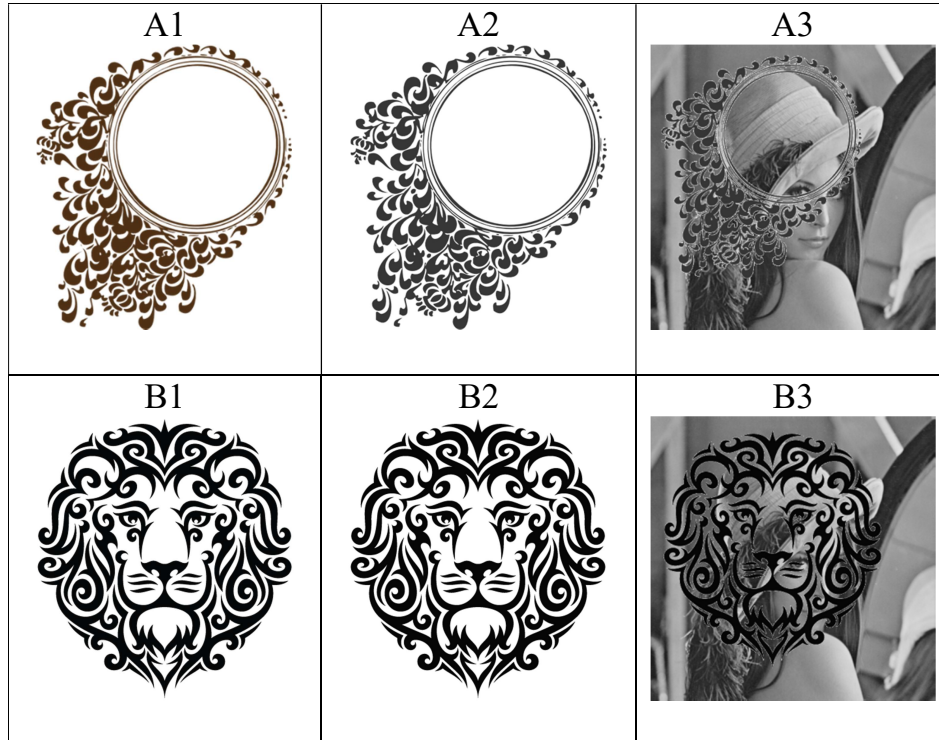
$TH$ 14 =	Airplane	51.42	46.33	43.88	42.54
	Boat	51.75	45.97	42.96	41.20
	Lena	51.51	46.24	43.71	42.38
	Peppers	51.37	45.81	43.04	41.50
	Tiffany	51.19	45.59	42.70	41.02
	Toys	51.58	45.75	42.71	40.94
	<b>Average</b>	<b>51.47</b>	<b>45.94</b>	<b>43.16</b>	<b>41.59</b>

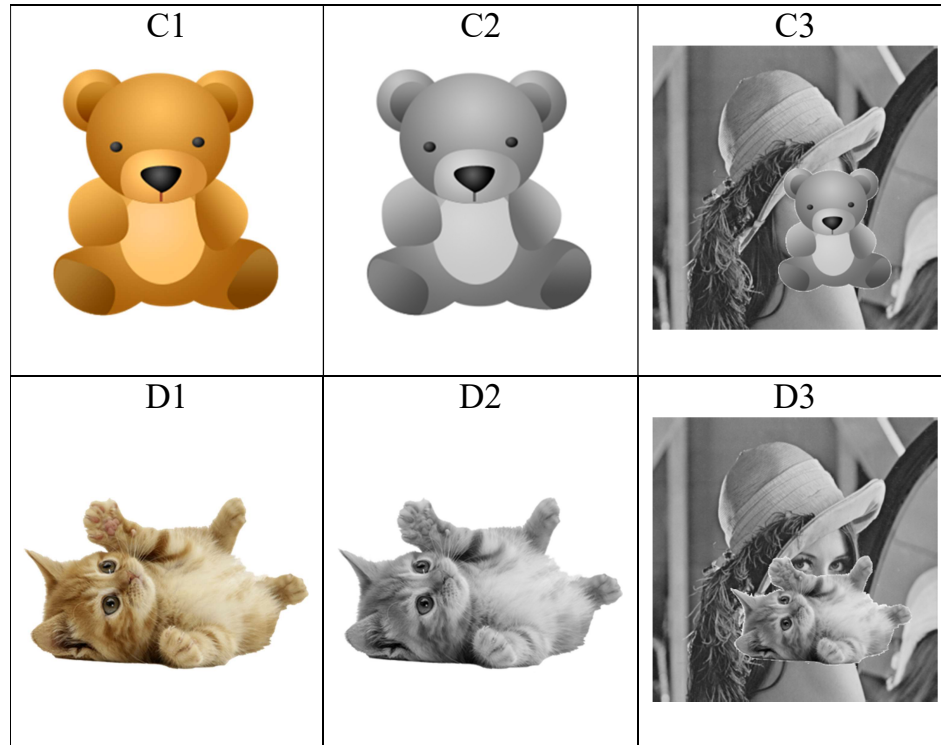
To estimate the accuracy of tamper detection, the normalized correlation coefficient (NCC) rate is used to measure the similarity between the detected image and the tampered image which is defined by:

$$NCC = \frac{\sum_{i=1}^H \sum_{j=1}^W [T_{i,j} - T_{mean}] [D_{i,j} - D_{mean}]}{\sqrt{(\sum_{i=1}^H \sum_{j=1}^W [T_{i,j} - T_{mean}]^2) (\sum_{i=1}^H \sum_{j=1}^W [D_{i,j} - D_{mean}]^2)}}, \quad (8)$$

where  $T$  is the binary form of the tampered object and  $T_{mean}$  is the mean value of all pixels in  $T$ .  $D$  is the detected image and  $D_{mean}$  is the mean value of all pixels in  $D$ .

For testing tamper detection, four different tampered color objects are converted to grayscale level and used in the proposed scheme as shown in Figure 6. Here, two first tampered color objects, A1 and B1, are very smooth image type with the complicated shape, C1 is the normal image type, and D1 is the complex one, respectively. In the experiment, to simulate tamper operation, the image “Lena” is embedded the authentication code. Then, each tampered object is added subsequently on the wall of the stego image “Lena” as shown in Figure 6.











**Figure 6.** A1, B1, C1, and D1 are four tampered color objects. A2, B2, C2, and D2 are four corresponding grayscale objects. A3, B3, C3, and D3 are four corresponding tampered images

To illustrate the superior performance of our scheme, we compared the proposed scheme with Lo and Hu's scheme [17] since their scheme achieved the reversibility as that of the proposed scheme. In Lo and Hu's scheme, the parameter  $p = 1$  or 2 is used because the similar results are obtained by their scheme for  $p \geq 2$ . For image "Lena", if  $p = 1$  is used, their scheme obtained the PSNR of 51.37 dB and the embedding capacity of 24,447 bits. If  $p = 2$  is used, their embedding capacity is improved further, up to 46,009 bits while the image quality decreases 2.54 dB. For a fair comparison, tampered objects are embedded into same location of the stego images in the proposed scheme and Lo and Hu's scheme, and the best results are used for comparison.

Tables (3)-(6) show the comparison results between the proposed scheme and Lo and Hu's scheme for different tampered objects. As can be seen in these tables, irrespective of tampered object is used for testing; the proposed scheme always provided the superior performance of image quality and accurate tamper detection to Lo and Hu's scheme. Especially, even for the complex tamper object, the proposed scheme also achieved more accuracy of tamper detection than that of Lo and Hu's scheme while ensuring good quality of the stego images. The main reason is that Lo and Hu's scheme is based on histogram shifting mechanism to embed the authentication code. This means that, in their scheme, more of the authentication code bits are embedded into the smooth region of the host image while fewer the







authentication code bits or none of them are embedded into the complex region. As a result, their scheme yielded low accuracy of tamper detection when some complex regions are modified. In contrast, to embed the authentication code, the proposed scheme divided the image into two sets of pixels. Accordingly, the high correlation of pixels in the host image is exploited for embedding the authentication code. By doing so, the authentication code is spread over the entire of the host image resulting in the high accurate tamper detection.

**Table 3.** Performance comparison of the proposed scheme and Lo and Hu’s scheme for the tamper object A1





	Detected images	Refined detected images
Lo and Hu’s scheme ( $p = 1$ , PSNR = 51.37)	 NCC = 0.474	 NCC = 0.613
Lo and Hu’s scheme ( $p = 2$ , PSNR = 48.83)	 NCC = 0.489	 NCC = 0.643
Proposed scheme ( $TH = 4$ , $T^* = 0$ , PSNR = 53.45)	 NCC = 0.684	 NCC = 0.697



**Table 4.** Performance comparison of the proposed scheme and Lo and Hu’s scheme for the tamper object B1

	Detected images	Refined detected images
--	-----------------	-------------------------







Lo and Hu's scheme ( $p = 1$ , PSNR = 51.37)	 NCC = 0.542	 NCC = 0.663
Lo and Hu's scheme ( $p = 2$ , PSNR = 48.83)	 NCC = 0.545	 NCC = 0.677
Proposed scheme ( $TH = 4$ , $T^* = 0$ , PSNR = 53.45)	 NCC = 0.834	 NCC = 0.841

**Table 5.** Performance comparison of the proposed scheme and Lo and Hu's scheme for the tamper object C1

	Detected images	Refined detected images
Lo and Hu's scheme ( $p = 1$ , PSNR = 51.37)	 NCC = 0.878	 NCC = 0.967
Lo and Hu's scheme ( $p = 2$ , PSNR = 48.83)	 NCC = 0.878	 NCC = 0.967

	NCC = 0.922	NCC = 0.970
Proposed scheme ( $TH = 4$ , $T^* = 0$ , PSNR = 53.45)	 NCC = 0.957	 NCC = 0.977

**Table 6.** Performance comparison of the proposed scheme and Lo and Hu’s scheme for the tamper object D1

	Detected images	Refined detected images
Lo and Hu’s scheme ( $p = 1$ , PSNR = 51.37)	 NCC = 0.642	 NCC = 0.902
Lo and Hu’s scheme ( $p = 2$ , PSNR = 48.83)	 NCC = 0.783	 NCC = 0.957
Proposed scheme ( $TH = 14$ , $T^* = 0$ , PSNR = 51.51)	 NCC = 0.820	 NCC = 0.958

To illustrate the superiority of the proposed scheme, we compared the proposed scheme to three previous image authentication schemes [15-17]. In this experiment, three grayscale tamper objects, i.e., B2, C2, and D2, are added on the wall of the stego image “Lena”. As shown in Table 7, the proposed scheme and the scheme in [17] both can recover the image to its original version losslessly. However, the average PSNR obtained by the

proposed scheme is slightly higher than that of the scheme in [17]. This is because the scheme [17] utilizes histogram-shifting algorithm to hide the authentication code in the host image. As a result, the more authentication bits are embedded, the larger distortion of the image will be. Conversely, before embedding the authentication code, the proposed scheme first evaluates the complexity of each pixel in the black set. Therefore, the pixels are the large complexity, which are not used for embedding because of the significant distortion. By doing so, the proposed scheme guaranteed the high image quality of stego images.

**Table 7.** Performance comparison of the proposed scheme with previous image authentication schemes

Schemes	Average NCC	Average PSNR (dB)	Average SSIM	Execution time (second)	Reversibility
Nguyen et al. [16]	0.812	40.58	0.9322	6.23	No
Hu et al. [15]	0.801	38.87	0.9262	7.16	No
Lo and Hu [17]	0.856	51.32	0.9784	3.43	Yes
Proposed	0.925	52.80	0.9981	4.21	Yes



## **PHẦN KẾT LUẬN**

In this paper, we propose a novel, reversible image authentication scheme based on rhombus prediction and local complexity for digital images. First, the host image is partitioned into two sets of pixels, i.e., black and white sets. Then, the rhombus prediction is used to select the smooth pixels in each set for embedding the authentication code while the complex pixels are kept unchanged during embedding process. By doing so, the authentication code is spread in the entire image, resulting in high accuracy of tamper detection and good image quality. Our experimental results demonstrated that the proposed scheme achieves good quality of stego images. In addition, the proposed scheme yields a high accuracy of tamper detection and reversibility. Also demonstrated in the experimental results, the proposed scheme provides better performance than previous scheme in terms of tamper detection and image quality.

## TÀI LIỆU THAM KHẢO

- [1] A. Swaminathan, M. Wu, K. J. R. Liu, “Digital image forensics via intrinsic fingerprints,” *IEEE Trans. Inf. Forens. Secur.*, vol. 2, no. 3, pp 101-117, 2008.
- [2] W. X. Tian, C. C. Chang, T. S. Nguyen, M. C. Li, “Reversible data hiding for high quality image exploiting interpolation and direction order mechanism,” *Digital Signal Processing*, vol. 23, no. 2, pp. 569-577, Mar. 2013.
- [3] H. Farid, “Exposing digital forgeries from JPEG ghosts,” *IEEE Trans Inf. Forens. Secur.*, vol. 4, no. 1, pp. 154-160, 2009.
- [4] S. Chen, H. Leung, “Chaotic watermarking for video authentication in surveillance applications,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 5, pp. 704-709, 2008.
- [5] C. C. Chang, T. S. Nguyen, C. C. Lin, “A blind reversible robust watermarking scheme for relational databases,” *Scientific World Journal (SWJ)*, volume 2013.
- [6] F. J Huang, J. W Huang, Y. Q. Shi, “New channel selection rule for JPEG steganography,” *IEEE Trans. Inf. Forens. Secur.*, vol. 7, no. 4, pp. 1181-1191, 2012.
- [7] P. W. Wong, N. Memon, “Secret and public key image watermarking schemes for image authentication and ownership verification,” *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1593-1601, 2001.
- [8] X. P. Zhang, S. Z. Wang, “Statistical fragile watermarking capable of locating individual tampered pixels,” *IEEE Signal Process. Lett.*, vol. 14, no. 10, pp. 727-730, 2007.
- [9] T. Y. Lee, S. F. D. Lin, “Dual watermark for image tamper detection and recovery,” *Pattern Recognition*, vol. 41, no. 11, pp. 3497-3506, 2008.
- [10] C. S. Chan, “An image authentication method by applying Hamming code on rearranged bits,” *Pattern Recognition Letters*, vol. 32, no. 14, pp. 1679-1690, 2011.
- [11] C. Qin, C. C. Chang, P. Y. Chen, “Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism,” *Signal Processing*, vol. 92, no. 4, pp. 1137-1150, 2012.
- [12] J. C. Chuang, Y. C. Hu, “An adaptive image authentication scheme for vector quantization compressed image,” *J. Vis. Commun. Image Represent.*, vol. 22, no. 5, pp. 440-449, 2011.
- [13] C. Qin, C. C. Chang, K. N. Chen, “Adaptive self-recovery for tampered images based on VQ indexing and inpainting,” *Signal Processing*, vol. 93, pp. 933-946, 2013.
- [14] Y. C. Hu, W. L. Chen, C. C. Lo, C. M. Wu, “A novel tamper detection scheme for BTC compressed images,” *Opto-Electronics Review*, vol. 21, no. 1, pp. 137-146, 2013.
- [15] Y. C. Hu, C. C. Lo, W. L. Chen, C. H. Wen, “Joint image coding and image authentication based on absolute moment block truncation coding,” *Journal of*

- Electronic Imaging*, vol. 22, no. 1, pp. 1-12, 2013.
- [16] T. S. Nguyen, C. C. Chang, T. F. Chung, "A tamper-detection scheme for BTC-compressed images with high-quality images," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 6, pp. 2005-2012, 2014.
- [17] C. C. Lo, Y. C. Hu, "A novel reversible image authentication scheme for digital images," *Signal Processing*, vol. 98, pp. 174-185, 2014.
- [18] T. S. Nguyen, C. C. Chang, N. T. Huynh, N. T. "A novel reversible data hiding scheme based on difference-histogram modification and optimal EMD algorithm," *Journal of Visual Communication and Image Representation*, vol. 33, pp. 389-397, 2015.
- [19] T. S. Nguyen, C. C. Chang, W. C. Chang, "High capacity reversible data hiding scheme for encrypted images," *Signal Processing: Image Communication*, vol. 44, pp. 84-91, 2016.
- [20] C. Qin, C. C. Chang, Y. H. Huang, L. T. Liao, "An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 23, no. 7, pp. 1109-1118, 2013.
- [21] C. Qin, C. C. Chang, G. Horng, Y. H. Huang, and Y. C. Chen, "Reversible data embedding for vector quantization compressed images using search-order coding and index parity matching," *Security and Communication Networks*, vol. 8, no. 6, pp. 899-906, 2015.
- [22] C. Qin, C.C. Chang, T.J. Hsu, "Reversible data hiding scheme based on exploiting modification direction with two steganographic images," *Multimedia Tools and Applications*, vol. 74, no. 15, pp. 5861-5872, 2015.