IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 June 2023, accepted 14 June 2023, date of publication 16 June 2023, date of current version 21 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3286928

RESEARCH ARTICLE

Nested Block Based Double Self-Embedding Fragile Image Watermarking With Super-Resolution Recovery

NOVA RIJATI, (Member, IEEE), AND DE ROSAL IGNATIUS MOSES SETIADI, (Member, IEEE)
Department of Informatics Engineering, Dian Nuswantoro University, Semarang, Central Java 50131, Indonesia

Corresponding author: Nova Rijati (nova.rijati@dsn.dinus.ac.id)

This work was supported by the Ministry of Research and Technology National Research and Innovation Agency of Indonesia under Grant 076/E5/PG.02.00.PL/2023 and Grant 0014/LL6/PL/AL.04/2023.

ABSTRACT Self-recovery capability is challenging in developing fragile watermarking alongside authentication and tamper localization. In certain situations, authentication and tamper localization alone may not be sufficient. Information about the original condition of the damaged area is essential, particularly in forensic image analysis applications. This study proposes a nested block-based self-embedding method for fragile image watermarking. The data embedded in the cover image includes authentication and watermark bits based on the advanced least significant bit (LSB) method. The watermark bits are generated from the cover images, while the authentication bit is obtained through the SHA-512 operation. Authentication bit embedding is performed using a 2×2 block-based Morton pattern. Meanwhile, the watermark bit is embedded twice in different locations within 4×2 and 2×4 blocks, alternating with the Morton pattern inside the 4×4 block using the Zigzag pattern. This approach better preserves the watermark information when tampering occurs over a large area. However, embedding the watermark twice requires more space, necessitating a resize operation before embedding. During the recovery stage, the resized watermark is enhanced using the Feature Super-resolution CNN (FSRCNN) technique. The proposed method demonstrates good imperceptibility quality, with a PSNR value exceeding 40dB and an SSIM exceeding 0.98. Moreover, the proposed method effectively detects and localizes tampering, achieving a True Positive Rate (TPR) of over 95% and a False Positive Rate (FPR) of less than 1% for a watermarked image with 50% tampering. Additionally, the proposed method exhibits outstanding recovery capabilities, resulting in a PSNR of more than 36dB for images with 50% tampering.

INDEX TERMS Fragile image watermarking, image authentication, double self-embedding, super-resolution recovery, nested block-based embedding.

I. INTRODUCTION

Authentication, tamper detection, and localization in digital images are essential. This can prove the image's authenticity and even detect hoaxes due to the manipulation of digital images. Particularly due to the increasing number of digital image transactions, many of which require this level of protection. Watermarking is a technique for securing text, audio, video, and specifically images in this study. This is similar to steganography, but watermarking focuses more on copyright protection or authentication, tamper localization, and recovery purposes. Several watermarking methods are based on their purpose, such as robust and fragile [1], [2], [3], [4], [5]. Robust watermarking is commonly used for copyright protection. While the fragile watermarking method is designed to be able to perform digital image authentication, tamper detection, and even image recovery [1], [4], [5], [6]. Fragile watermarking requires a watermark that is very sensitive to image modification [7] and can be generated from several random values. One of the commonly used fragile watermarking techniques is the hash algorithm, which uses a random value as the basis for calculating

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

the hash value, which is then used as a watermark in the image.

Studies have proposed fragile image watermarking algorithms, such as [8], [9], [10], and [11], [12], [13], [14], [15]. Which invisibly embed methods that can detect and localize tampering while providing good authentication. However, in some situations, the authentication and detection of modified areas may be insufficient. In certain forensic image analysis applications, it is necessary to have information about the original condition of the damaged area. Several watermarking algorithms have adopted the self-embedding method to address this challenge [7], [16], [17], [18], [19], [20], [21].

The information embedded in self-embedding watermarking is generally in the form of basic information or main features of the cover image so that, if the image is tampered with or manipulated, this information can be extracted to restore the cover image [7], [22]. But to be able to perform a good recovery requires sufficient information. However, the information must be limited to minimize the payload because the larger the payload, the greater the distortion effect [5], [22]. The main challenge in self-embedding watermarking is minimizing reference information but being able to generate watermarks with maximum quality.

The block-wise method has been widely applied in fragile image watermarking because it can increase the chance of recovering the manipulated area [16]. The block size used can vary, such as 2×2 [23], 2×4, 4×2 [16], 4×4 [6], [19], [24], and 32×32 [25]. It must be wise to choose the block size because it affects the performance results. Large block sizes can hide more recovery information, so it has better recovery capabilities in case of tampering. However, the large block size is less accurate in determining the tampered image area [8], [22].

The size of the tampering area also greatly affects the recovery ability. The larger the tampering area, the more difficult it is to recover the image properly. This study proposes a double self-embedding method that utilizes a block-wise nested technique and a combination of two embedding patterns to overcome this challenge. This method differentiates from dual watermarking, serving a more multi-purpose function [26], [27], [28]. Based on the problems in the background described above, the motivation for this study was to design a fragile watermarking method that has robust self-recovery and is capable of authentication with a high level of accuracy. Therefore this research focuses on double self-embedding to increase self-recovery and tampering localization capabilities by embedding the same two watermarks at different locations so that if tampering occurs at one location, then another location that contains a watermark without tampering can be selected for use as a recovery. But embedding a double watermark can affect the payload so that the watermark is resized to half of its original size. The resizing process certainly reduces the information's quality, so before it is used for recovery, watermark enhancement is carried out using the super-resolution convolutional neural network (SRCNN) method [29]. In addition, nested block techniques and mixed embedding patterns are proposed. It can be concluded that this research made several contributions, namely:

1. We apply double self-embedding on fragile watermarking to improve recovery ability on a wider tamper area.
2. We use FSRCNN-based image enhancement to watermark quality.
3. Propose a nested block embedding method combining two scanning patterns, where smaller blocks are used as authentication blocks to improve tamper localization accuracy.
4. Propose a method of tamper recovery, authentication, and localization without auxiliary information.

The remainder of this paper is organized into several sections. Section II, the study literature and hypotheses for elaborating ideas are presented. Section III presents a step-by-step explanation of the proposed method. Section IV describes the results and analysis of the method, and Section V contains conclusions.

II. PRELIMINARIES

A. LEAST SIGNIFICANT BIT (LSB)

LSB is a popular method in fragile image watermarking. This method replaces the last bit or LSB of the original image pixels with the bits from the watermark. In the fragile image watermarking method, if there is even a slight change in the original image, the watermark will be lost or damaged, so this method is suitable for applications that require a high level of security [6], [7], [21]. Literally, the LSB method uses only one bit, but in its implementation, more than one bit can be used. The more LSB bits used for embedding will increase the payload but result in greater distortion [12]. In research [6], 2LSB embedding or the equivalent of 2bits per pixel (BPP) consists of 1.75 BPP for watermark recovery information and 0.25 BPP for authentication. This method focuses more on recovering information and minimizes bit authentication information. This makes the authentication process less accurate. However, because it is implemented in RGB images, a combination of OR and hierarchical authentication operations are performed to improve accuracy.

Research [7] also used embedding on 2LSB and added auxiliary information to assist the embedding and extraction processes. This method is designed to be able to perform recovery and authentication. This method can recover around 10% of attacks in testing the content removal attack. Meanwhile, the average tamper detection rate is more than 99% of the average for all attacks. Other research [21] also uses the Pixel P Air-Wise method combined with Huffman code and absolute moment block truncation coding with 2LSB for information embedding. The advantage of this method is that it can produce a watermarked image with high imperceptible quality, around 46.8dB. In addition, this method is also designed to perform tamper detection and recovery. In the tests carried out, a maximum tamper attack of around

3.44% was carried out and could recover with a quality of 31.8dB on baboon images. But the tamper detection performance of this method only has an average accuracy of about 86%.

B. BLOCK WISE METHOD

Block-wise is one of the popular methods in the fragile watermarking method. This method divides the digital image into smaller blocks for embedding the watermark. The advantages of this method are robustness against attacks and localization precision. The block-wise method can detect pixel changes in each image block independently, making it more robust against attacks such as pixel changes, deletions, or pixel insertions intended to damage the image. Each image block is calculated to have an authentication value separately so that if a change occurs in a particular block, it can be easily identified which block has changed.

Several previous methods have also proposed block-wise based methods such as [8], [16], and [30]. Research [8] suggested a 2×2 block division for the watermark generation and embedding processes. This method is designed to perform tamper localization on various general and complex attacks but cannot perform recovery. With the block-wise 2×2 technique, this method has high tamper detection accuracy compared to larger blocks such as 4×4, 8×8 and 16×16.

Research [30], a 2×4 block was used with an embedded payload of 1.5 BPP. The method is designed not only to perform tamper localization but also to perform recovery. Basically, the recovery results of this method are not very excellent, but with the addition of a smoothing process, this method can recover from a wide range of attacks. Research [16] proposes a 2×4 block size using similar block sizes, but this research also compares it to a 4×2 block to choose a more optimal imperceptibility. In addition, this method can perform image recovery with up to 50% tampering.

C. SUPER-RESOLUTION CONVOLUTIONAL NEURAL NETWORKS (SRCNN)

CNN in image enhancement makes it possible to improve image quality by producing higher-quality and easier-to-interpret images. Image enhancement based on super-resolution (SR) is a form of CNN (SRCNN) to increase low to high-resolution images with better quality. CNN is used to learn helpful feature representation of image data by extracting important features from low-resolution images and learning how to build high-quality images based on these features. CNN used in super-resolution consists of several layers that can deepen the model's understanding of low-resolution images and strengthen important features.

One of the popular CNN models in super-resolution is Feature SRCNN (FSRCNN) [29]. The FSRCNN method redesigns SRCNN by adding a deconvolution layer (see Fig. 1). Thus, the quality can be better than the bicubic or SRCNN methods. The CNN method can be applied in the self-recovery process in fragile watermarking. Previous studies, such as [20] and [31], also implemented CNN in the recovery process. This is an opportunity to be developed and applied in self-recovery fragile watermarking.

Section II is divided into three sub-sections, namely II-A, II-B, and II-C, which have explained the important methods in each sub-section by reviewing the state-of-the-art (SOTA). These three things are important and interrelated to build a hypothesis. It can be concluded that LSB is a popular method and has proven suitable for fragile watermarking. Still, in this case, it is necessary to be wise in determining the payload and the number of LSB bits used because it affects the quality of imperceptibility. While the implementation of the block-wise method based on LSB also needs to be considered because this determines the authentication capabilities and security of the watermark bits, with block-wise size variations, of course, it can make embedding not skewed towards certain capabilities but can also excel at more than one capability, namely accuracy and embed space. Finally, it was explained that the super-resolution method improves the visual quality of images when enlarged in size, this is very useful for the self-recovery process and has been tested in several related SOTAs. Based on these literatures, a method is proposed that combines these methods, in more detail in Section III.

III. PROPOSED METHOD

This study proposes the LSB method with 2 BPP payloads embedded in the last 2 LSB. In addition, it uses a nested block-wise technique with a combination of two embedding patterns. Meanwhile, to improve the recovery process, it is combined with FSRCNN to improve its quality. A more detailed explanation of the proposed method is presented in several subsections below.

A. AUTHENTICATION AND WATERMARK BIT GENERATION

The input needed at this stage is the cover image and the sender's secret key. The secret key can be a text password or a digital signature file. The output at this stage is the watermark bits (*wb*) and the authentication bit (*aub*). The watermark will be an image generated using the bicubic method from the cover image. This watermark image will later be used as one of the inputs for recovery. Bicubic is an interpolation technique that produces smoother and higher-quality images when reducing the image size. The Bicubic works by calculating the pixel values of blocks around the interpolated pixels. Bicubic calculates a third-order polynomial that passes 16 neighboring pixels from the interpolated pixels because this study uses a 4×4 kernel [32], [33]. This method was chosen because it has relatively lighter and simpler computations. In more detail, the resizing steps with the bicubic algorithm are as follows

1. Determine the size of the resized image. In this case, it is a quarter of the size of the original image because it will be embedded twice in the cover image.

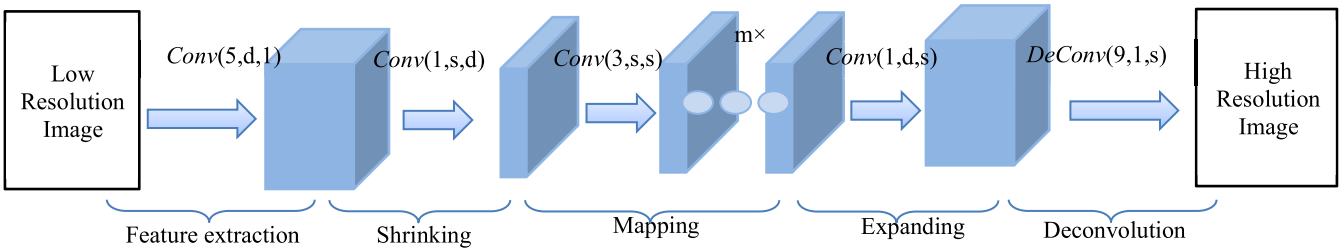

FIGURE 1. FSRCNN structure [29].

2. Calculate the values of Δx and Δy using Eq. (1).

$$\Delta x = (w-1)/(w'-1)$$
$$\Delta y = (h-1)/(h'-1) \quad (1)$$

where w and h are the width and height of the original image, and w' and h' are the width and height of the resized image.

3. For each pixel (x', y') in the resized image, calculate the pixel coordinates that match the original image using Eq. (2).

$$x = x' \times \Delta x$$
$$y = y' \times \Delta y \quad (2)$$

4. Determine the 4×4 pixel kernel around the pixels (x, y) in the original image.
5. Calculate the third-order polynomial coefficients for each pixel in the kernel using the bicubic interpolation technique.
6. Calculate the pixel intensity at position (x', y') in the resized image using Eq. (3).

$$f\left(x', y'\right) = \sum_{i=0}^{3}\sum_{j=0}^{3} a_{i,j} xi^j yj^i \quad (3)$$

where f $\left(\mathrm{x}', \mathrm{y}'\right)$ is the pixel intensity at the position $\left(\mathrm{x}', \mathrm{y}'\right)$ on the resized image, ai,j is the third-order polynomial coefficient calculated by bicubic interpolation technique, $xi = max(0, 1 - |x' - i|)$, and $yi = max(0, 1 - |y' - j|)$, x' and y' are pixel coordinates in the resized image, i and j are pixel indexes in the 4×4 pixel kernel around (x', y') in the original image.

7. Repeat steps 3-6 for each pixel to resize the image.
8. Perform scrambling on the resized image using Arnold transform. Use Eq. (4) to perform Arnold transform.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ M \quad (4)$$

where Arnold transform is performed for several iterations, resized image dimension is $M \times M$, a, and b are integers as parameters.

9. Get the watermark image w, and convert into binary form to watermark bit (wb).

Meanwhile, the *aub* is generated from the private key inputted by the sender, and the SHA-512 hash operation is performed. Because the length of the hash output wants to be extended as needed with the following steps:

1. Set *aub* from the hash data using an SHA-512 algorithm.
2. Convert the hash data to a character array and store it in *cAuth*.
3. Initialize an empty string variable *tempAuth*.
4. Loop through the *cAuth* data by pairs of 2 bytes, and for each pair:
   a. Hash the pair using the same algorithm used in step 1.
   b. Convert the resulting hash to a character array.
   c. Append the character array to the *tempAuth* variable.
5. Initialize another empty string variable *fAuth*.
6. Loop through the *tempAuth* data by chunks of 7 bytes, and for each chunk:
   a. Hash the chunk using the same algorithm used in step 1.
   b. Convert the resulting hash to a character array.
   c. Append the character array to the *fAuth* variable, as long as the *fAuth* variable length is less than the number of pixel/8.
7. Convert the first number of pixel/8 characters of the *fAuth* variable to binary format.
8. Reshape the binary data (*aub*) into a row vector with the length of the same number of pixels.

B. NESTED BLOCKS EMBEDDING

At the embedding stage, the cover image, *wb*, and *aub* are required for input. The embedding is carried out using the LSB method with a combination of two patterns, namely zigzag and Morton, based on nested blocks. The purpose of this stage is to get a safe pattern on 2LSB to store *aub* and double *wb*, so that later it can be more accurate in tamper localization and improve self-recovery processes. As an illustration, you can see Fig. 2.

In detail, the embedding stage illustrated in Fig. 2 is described as follows:

1. Delete the two LSBs in the cover image (I). In this process, the last two LSBs will be zero. For example, the following:

Original Pixel Value	Binary Value
149	1 0 0 1 0 1 0 1
After deleting two LSB	Binary Value
148	1 0 0 1 0 1 0 0

2. Divide the cover image into four parts of the same size, see Fig. 2.

3. Take the first part, then do a 4 × 4 zigzag scanning pattern.
4. Divide the 4 × 4 block into two parts with a size 2 × 4 for odd sequences and 4 × 2 for even arrangements. Embed the *wb* on the second LSB according to the Morton pattern order in Fig. 2
5. Based on step 4, attach the *aub* to the LSB with a block size 2 × 2 according to the Morton pattern order in Fig. 2.
6. Repeat steps 3 to 5 until all blocks in the first part are pinned. Each part of the cover image will be embedded with half of the watermark image for the record.
7. Repeat steps 3 to 6 for the second, fourth, and third parts, and then the two watermark images will be completely embedded in the cover image.
8. Watermarked image (I') is obtained.

For the record, because there are double *wb*, half of the *wb* embedded in part 1 is embedded in part 4, and the *wb* in part 2 is half embedded in part 3.

C. WATERMARK EXTRACTION AND TAMPER LOCALIZATION

Extraction in the proposed method can be done blindly. The required inputs are the cover image and secret key. While the resulting output is a watermark image for recovery, tamper localization (if not authentic). In detail, the extraction stages are presented as follows:

1. Read the watermarked image, and divide it into four large parts like the embedding step.
2. Input the secret key, then perform a hash operation to generate *aub*.
3. Extract *aub* (*aub*′) and *wb*, respectively on the LSB and LSB of the two watermarked images according to the embedding pattern on each part.
4. Compare the corresponding *aub* and *aub*′ in each 2 × 2 block. If one of the bits is not the same, mark it with a block value of 1, and for a block that is exactly the same, mark it with a value of 0.
5. On the other hand, since there are double *wb*, compare the *wb* of each part. Choose authentic *wb* based on authentic 2 × 2 blocks. If the two *wb*'s are not authentic based on the block, perform hierarchical authentication of the *wb* bits based on the appropriate *aub* bits, and arrange them based on the bits that are close to authentic. As an illustration, to get authentic pixels *wb* see Fig. 3.
6. Repeat steps 3, 4, and 5 until all blocks are inspected and a tamper localization (*mt*) matrix is formed, and *wb*′ is obtained as extracted watermark bit.
7. If all the pixels of the mt matrix are 0, then the watermarked image can be declared authentic.
8. Group every eight *wb*′ as the extracted watermark image (*w*′) pixel value, then reshape it into a matrix with the size of a quarter of the cover image part.

D. SUPER-RESOLUTION RECOVERY

This stage aims to improve self-recovery results. Super-resolution was required because of the reduced watermark, which needed to be restored to a better quality. The input necessary at this stage is a tampered watermarked image, *mt*, and *w*', while the output is a recovered image (*ri*). In more detail, the steps at this stage are:

1. Perform an inverse Arnold transform operation on the extracted watermark using Eq. (5), where the parameters and the number of iterations used must be the same.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} mod\ M \tag{5}$$

2. Enlarge ×4 on w' using FSRCNN so the size of w′ becomes the same as the cover image.
3. Find tampered areas on the watermarked image based on *mt* guidance. The tampered area is marked with a value of 1 in the mt matrix.
4. Replace the tampered pixel value with the appropriate pixel w' value
5. After all tampered pixels are replaced with a recovered watermark image, get a recovered cover image.

IV. RESULTS AND ANALYSIS

Several standard images from SIPI [32] were used to test the proposed fragile watermarking method at this stage. As for the super-resolution process with FSRCNN, we added the Bossbase [34] dataset for the learning process, but in this case, this is not discussed in detail because FSRCNN is just being implemented. First, the watermarked image is measured by the peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM). These two assessment tools are used to determine the quality of the proposed method's imperceptibility. PSNR is calculated using Eq. (6), while SSIM uses Eq. (7). Both of these measurement tools are measurement tools that require a reference so that the original cover image is compared with the watermarked image. The greater the PSNR value indicates, the smaller the ratio of embedded noise that distorts the image. The SSIM value close to 1 is the better SSIM value, and conversely, close to 0. The better SSIM indicates that the image structure is identical to the original image.

$$PSNR = 20log_{10}\left(\frac{max}{\sqrt{\frac{1}{WH}\sum_{x=1}^{W}\sum_{y=1}^{H}\left(C_{xy}-S_{xy}\right)^2}}\right) \tag{6}$$

$$SSIM = \frac{\left(2\mu_C\mu_S+(p_1D)^2\right)\left(2\sigma_{CS}+(p_2D)^2\right)}{\left(\mu_C^2+\mu_S^2+(p_1D)^2\right)\left(\sigma_C^2+\sigma_S^2+(p_2D)^2\right)} \tag{7}$$

where C is the cover image, S is the watermarked image, W is the width of the image, H is the height of the image, μ is of luminance intensity, σ is the standard deviation of contrast, p_1 and p_2 are stabilizing parameters with values 0.01 and 0.03, respectively, D is the dynamic range of pixel value.

Based on the PSNR results presented in Table 1, it can be recognized that the imperceptibility quality is not the best. However, the entire image is over 40dB, which means that the imperceptibility quality is excellent [5]. In addition, the SSIM value presented in Table 1 also produces excellent values,

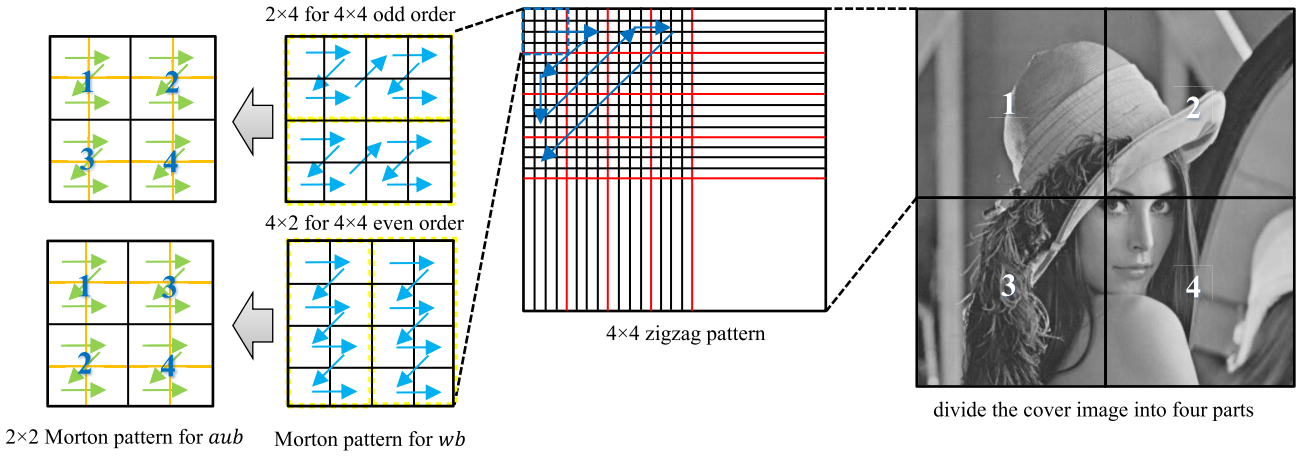

FIGURE 2. Proposed nested blocks embedding patterns.

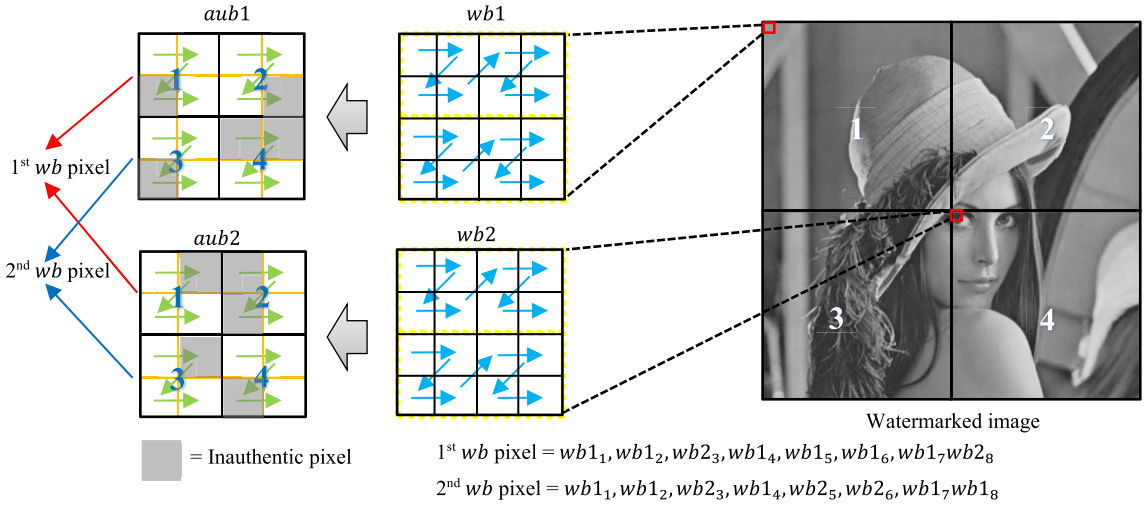

FIGURE 3. Watermark bits extraction and checking technique to select authentic bits.

TABLE 1. PSNR and SSIM results and comparison of watermarked image.

Image	Method	PSNR (dB)	SSIM
Lena	Method [16]	38.35	0.9260
	Method [21]	46.80	-
	Method [17]	39.77	-
	Proposed	40.89	0.9859
Airplane	Method [16]	38.35	0.9382
	Method [21]	46.80	-
	Proposed	40.78	0.9847
Baboon	Method [21]	46.80	-
	Method [17]	39.86	-
	Proposed	40.82	0.9864
Sailboat	Method [16]	38.38	0.9380
	Proposed	40.85	0.9856

with overall results above 0.98. The SSIM value is very close to 1 and is classified as excellent. Besides the imperceptibility quality with PSNR and SSIM, in Fig. 5, the results of the watermarked image, original cover image, watermarked, and histogram are presented. The histogram indicates imperceptibility, where the histogram between the cover image and the watermarked image is increasingly identical, indicating that the embedding effect does not significantly affect the histogram quality. As shown in Fig. 5, the histogram between the cover and watermarked images is visually similar to the number of overlapping bins histograms.

Tamper detection ability and localization are more important in fragile image watermarking. The evaluation metrics commonly used in the tamper detection of fragile watermarking are the True Positive Rate (TPR) and the False Positive Rate (FPR). TPR is the ratio between the number of watermarks that are detected as true (true positive) compared to the number of watermarks that should be detected as true (true positive) in a tampered image. In other words, TPR measures how well the fragile watermarking tamper detection system detects changes in an image marked with

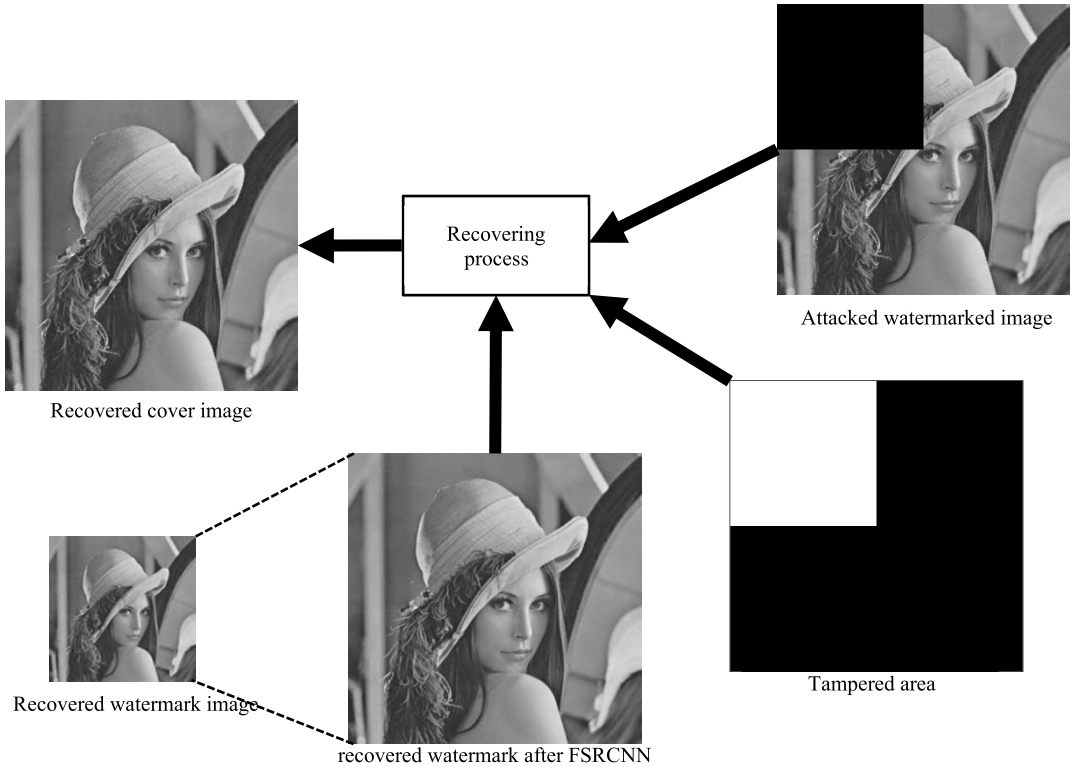

FIGURE 4. Self-recovery scheme.

a watermark. Meanwhile, FPR is the ratio between the number of incorrectly detected as modified (false positives) and the number of watermarks that should not be detected as modified (true negatives). High TPR results indicate that the system can detect most changes in images marked with watermarks, while low FPR results mean that the system can minimize errors in identifying images that have not changed tampered images. Fig. 6, 7, 8, and 9 present samples from the tampering test performed, while Table 2 presents the results of TPR and FPR measurements. Fig. 6, 7, 8, and 9 show samples of tampering from various attacks such as content removal, object removal, collage, and crop. The percentage of tampering varies from less than 1% to 50%. But visually, it appears that the recovery results are excellent. This is due to the double self-embedding watermark performance. The localization of the small tamper area results in Fig. 6 and 7 can reach ≈100% for TPR and ≈0% for FPR. In Fig. 8 and 9, the TPR is 97.89% and 95.56%, and the respective FPR values are 0.01% and 0.78%.

The results presented in Table 2 show that the resulting TPR and FPR values are outstanding. The proposed method can perform tamper localization with very high accuracy. The TPR value can be more than 95%, and the FPR is less than 1%, see Table 3. The recovery capability is also relatively stable, with tampering reaching 50%. The recovery quality can be more than 36 dB. The difference in recovery quality

TABLE 2. Average TPR, FPR, and Recovery results after tampering.

Tampering Rate	TPR	FPR	PSNR Recovery
5%	99.97%	0.00%	40.55dB
10%	99.78%	0.08%	40.38dB
15%	99.37%	0.19%	40.19dB
20%	98.97%	0.23%	39.91dB
25%	98.25%	0.31%	39.56dB
30%	97.91%	0.38%	39.10dB
35%	97.54%	0.42%	38.24dB
40%	96.94%	0.57%	37.88dB
45%	96.31%	0.64%	37.17dB
50%	95.54%	0.78%	36.68dB

TABLE 3. Comparison of tamper detection and localization with previous method.

Method	Tampering Rate Range	TPR (%)	FPR (%)
Method [21]	0.6-3.44%	≈ 79-96	≈ 0.04-0.18
Method [16]	<=10%	-	0%
Method [15]	<5%	>97%	<0.5%
Proposed	5-50%	95.54-99.97%	0.78-0.0%

at 5% to 50% tampering is only 3.87dB, see Table 4. With a tampering rate of 50%, the proposed method is superior in recovery quality [16], [17]. This is caused by a combination of embedding double watermarks and super-resolution

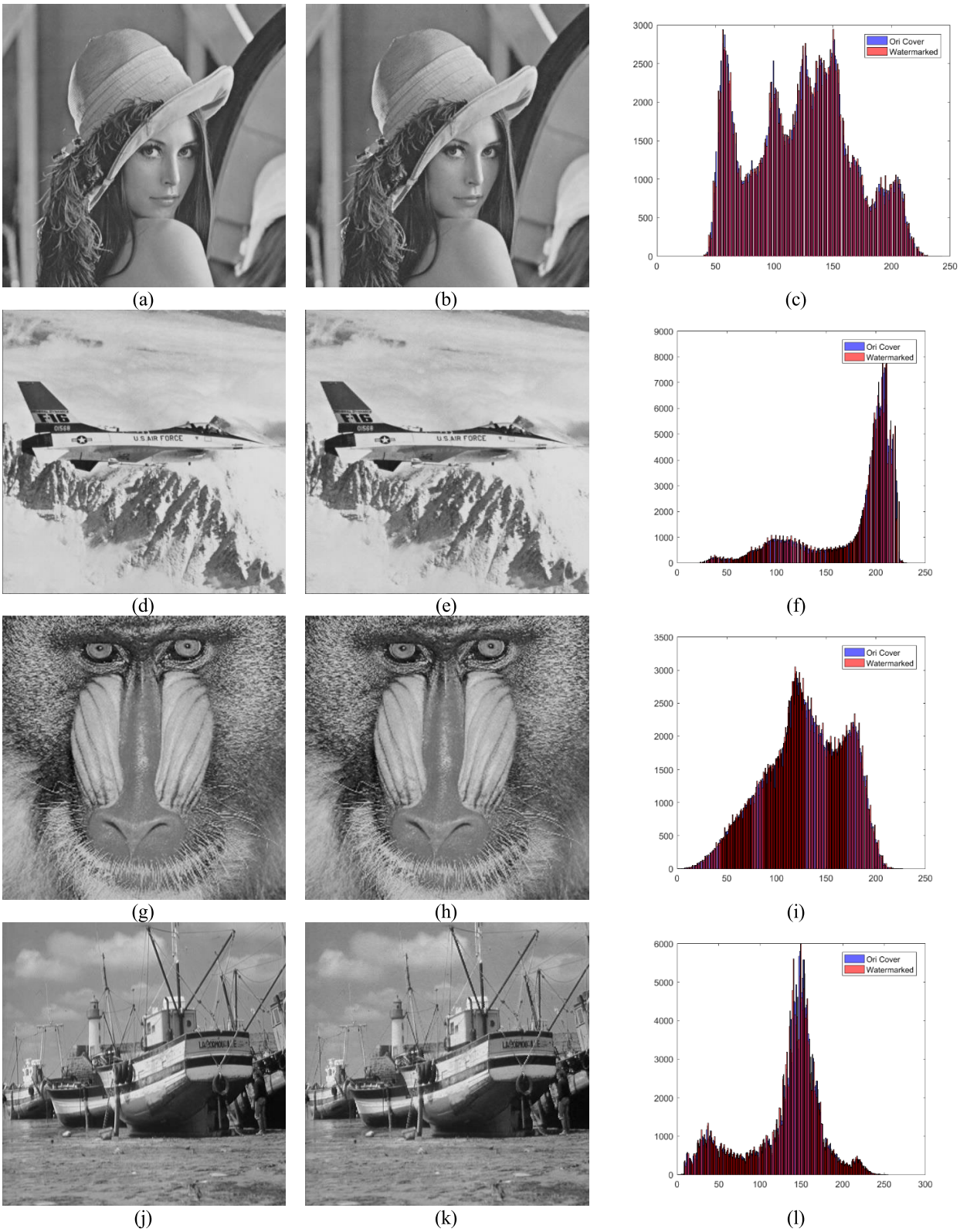

FIGURE 5. Results of Watermarking Scheme {(a, d, g, j) Original cover image, (b, e, h, k) Watermarked image, (c, f, I, l) Histogram of both}.

techniques. As additional evidence, an ablation study was carried out especially to find out how significant the effect is with and without super-resolution for the recovery stage. The proposed method without super-resolution is replaced

FIGURE 6. Sample of content removal attack ≈ 0.47% {(a) watermarked image, (b) tampered image, (c) tampered area, (d) restored image}.

FIGURE 7. Sample of collage attack ≈ 1.69% {(a) watermarked image, (b) tampered image, (c) tampered area, (d) restored image}.

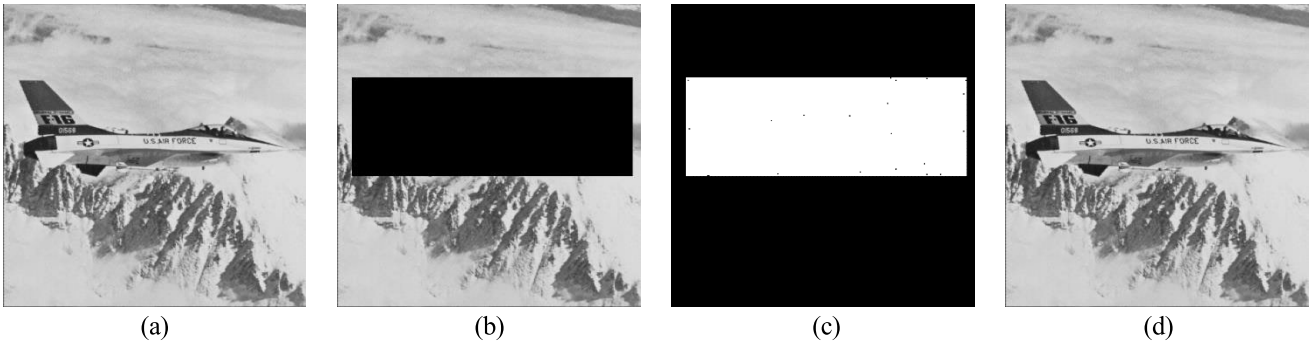

FIGURE 8. Sample of object removal attack ≈ 30.17% {(a) watermarked image, (b) tampered image, (c) tampered area, (d) restored image}.

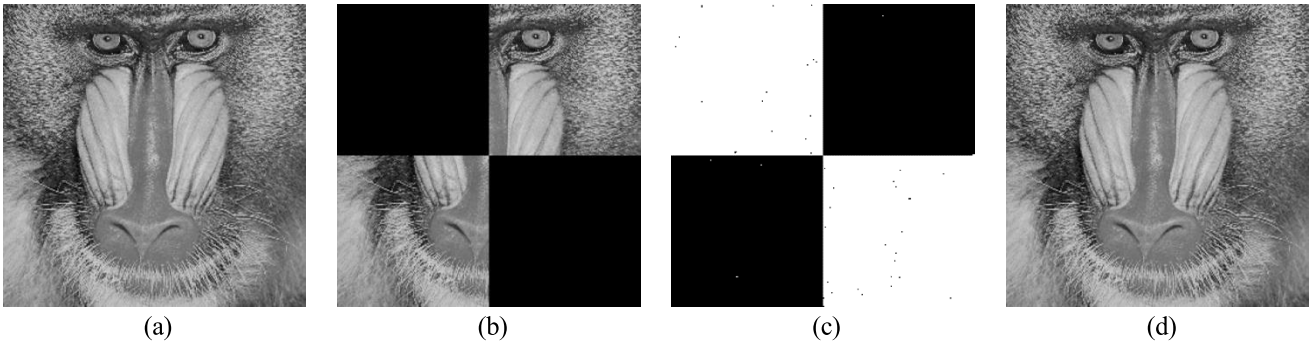

FIGURE 9. Sample of crop attack 50% {(a) watermarked image, (b) tampered image, (c) tampered area, (d) restored image}.

by the standard bicubic method. The test results are presented in Table 5, showing that super-resolution significantly affects the self-recovery stage with a PSNR difference of around 5dB.

TABLE 4. Comparison of recovery quality with previous method.

Method	Tampering Rate Range	PSNR Range	Diff PSNR
Method [17]	5-50%	≈ 35-47dB	≈ 12dB
Method [21]	0.6-3.44%	≈ 32-42dB	≈ 10dB
Method [16]	10-50%	≈ 32-43dB	≈ 11dB
Proposed	5-50%	36.78-40.55dB	3.87dB

TABLE 5. Average recovery quality results after tampering with and without super-resolution.

Tampering Rate	PSNR with SR	PSNR without SR
5%	40.55dB	35.89dB
10%	40.38dB	35.22dB
15%	40.19dB	34.63dB
20%	39.91dB	34.01dB
25%	39.56dB	33.71dB
30%	39.10dB	33.17dB
35%	38.24dB	32.52dB
40%	37.88dB	31.67dB
45%	37.17dB	30.89dB
50%	36.68dB	30.13dB

V. CONCLUSION

This study proposes a fragile watermarking method with a double self-embedding technique to perform authentication, tamper localization, and recovery. The consequence of a double watermark is magnifying and can affect the quality of imperceptibility. Because of this, the watermark needs to be reduced. However, a smaller size results in a reduced watermark quality and can affect the quality of the recovery. Then use image enhancement on the watermark using FSRCNN. In this way, the proposed method can maintain recovery quality even in a relatively large tamper area. Two watermarks can be checked, and one can choose which is more authentic. To improve the security of embedding watermarks, a nested block-wise embedding technique is used with a combination of zigzag and Morton and Arnold transform patterns on the watermark before embedding. The test results prove that the proposed method can work well for the authentication, tamper detection, and recovery processes. Payload is proven to be able to produce an excellent performance. In future research, this method can be combined with the autoencoder method to generate watermarks.

REFERENCES

[1] L. Rakhmawati, W. Wirawan, and S. Suwadi, "A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability," *EURASIP J. Image Video Process.*, vol. 2019, no. 1, Dec. 2019, doi: 10.1186/s13640-019-0462-3.

[2] C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "Robust and imperceptible image watermarking by DC coefficients using singular value decomposition," in *Proc. 4th Int. Conf. Electr. Eng., Comput. Sci. Informat. (EECSI)*, Sep. 2017, pp. 1–5, doi: 10.1109/EECSI.2017.8239107.

[3] O. F. A. Adeeb and S. J. Kabudian, "Arabic text steganography based on deep learning methods," *IEEE Access*, vol. 10, pp. 94403–94416, 2022, doi: 10.1109/ACCESS.2022.3201019.

[4] N. R. N. Raj and R. Shreelekshmi, "A survey on fragile watermarking based image authentication schemes," *Multimedia Tools Appl.*, vol. 80, no. 13, pp. 19307–19333, May 2021, doi: 10.1007/s11042-021-10664-y.

[5] D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, "Digital image steganography survey and investigation (goal, assessment, method, development, and dataset)," *Signal Process.*, vol. 206, May 2023, Art. no. 108908, doi: 10.1016/j.sigpro.2022.108908.

[6] J. Molina-Garcia, B. P. Garcia-Salgado, V. Ponomaryov, R. Reyes-Reyes, S. Sadovnychiy, and C. Cruz-Ramos, "An effective fragile watermarking scheme for color image tampering detection and self-recovery," *Signal Process., Image Commun.*, vol. 81, Feb. 2020, Art. no. 115725, doi: 10.1016/j.image.2019.115725.

[7] G. Su, C. Chang, and C. Lin, "Effective self-recovery and tampering localization fragile watermarking for medical images," *IEEE Access*, vol. 8, pp. 160840–160857, 2020, doi: 10.1109/ACCESS.2020.3019832.

[8] N. R. Neena and R. Shreelekshmi, "Fragile watermarking scheme for tamper localization in images using logistic map and singular value decomposition," *J. Vis. Commun. Image Represent.*, vol. 85, May 2022, Art. no. 103500, doi: 10.1016/j.jvcir.2022.103500.

[9] N. Rijati, D. R. I. M. Setiadi, and P. N. Andono, "Fragile image watermarking based on bidiagonal SVD-LSB for tamper detection and localization," *Int. J. Intell. Eng. Syst.*, vol. 15, no. 6, pp. 315–324, 2022, doi: 10.22266/ijies2022.1231.30.

[10] P. Lefèvre, P. Carré, C. Fontaine, P. Gaborit, and J. Huang, "Efficient image tampering localization using semi-fragile watermarking and error control codes," *Signal Process.*, vol. 190, Jan. 2022, Art. no. 108342, doi: 10.1016/j.sigpro.2021.108342.

[11] Z. Xia, W. Zhang, H. Duan, J. Wang, and X. Wei, "Fragile watermarking scheme in spatial domain based on prime number distribution theory," *Multimedia Tools Appl.*, vol. 81, no. 5, pp. 6477–6496, Feb. 2022, doi: 10.1007/s11042-021-11704-3.

[12] M. Hussan, S. Gull, S. A. Parah, and G. J. Qureshi, "An efficient encoding based watermarking technique for tamper detection and localization," *Multimedia Tools Appl.*, Mar. 2023, doi: 10.1007/s11042-023-15039-z.

[13] E. Akhtarkavan, B. Majidi, and A. Mandegari, "Secure medical image communication using fragile data hiding based on discrete wavelet transform and A5 lattice vector quantization," *IEEE Access*, vol. 11, pp. 9701–9715, 2023, doi: 10.1109/ACCESS.2023.3238575.

[14] P. Singh and S. Agarwal, "An efficient fragile watermarking scheme with multilevel tamper detection and recovery based on dynamic domain selection," *Multimedia Tools Appl.*, vol. 75, no. 14, pp. 8165–8194, Jul. 2016, doi: 10.1007/s11042-015-2736-9.

[15] C.-C. Lin, T.-L. Lee, Y.-F. Chang, P.-F. Shiu, and B. Zhang, "Fragile watermarking for tamper localization and self-recovery based on AMBTC and VQ," *Electronics*, vol. 12, no. 2, p. 415, Jan. 2023, doi: 10.3390/electronics12020415.

[16] E. Gul and S. Ozturk, "A novel pixel-wise authentication-based self-embedding fragile watermarking method," *Multimedia Syst.*, vol. 27, no. 3, pp. 531–545, Jun. 2021, doi: 10.1007/s00530-021-00751-3.

[17] D. Singh, S. K. Singh, and S. S. Udmale, "An efficient self-embedding fragile watermarking scheme for image authentication with two chances for recovery capability," *Multimedia Tools Appl.*, vol. 82, no. 1, pp. 1045–1066, Jan. 2023, doi: 10.1007/s11042-022-13270-8.

[18] L. Huang, D. Kuang, C.-L. Li, Y.-J. Zhuang, S.-H. Duan, and X.-Y. Zhou, "A self-embedding secure fragile watermarking scheme with high quality recovery," *J. Vis. Commun. Image Represent.*, vol. 83, Feb. 2022, Art. no. 103437, doi: 10.1016/j.jvcir.2022.103437.

[19] M. Jana, B. Jana, and S. Joardar, "Local feature based self-embedding fragile watermarking scheme for tampered detection and recovery utilizing AMBTC with fuzzy logic," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 10, pp. 9822–9835, Nov. 2022, doi: 10.1016/j.jksuci.2021.12.011.

[20] H.-C. Wu, W.-L. Fan, C.-S. Tsai, and J. J.-C. Ying, "An image authentication and recovery system based on discrete wavelet transform and convolutional neural networks," *Multimedia Tools Appl.*, vol. 81, no. 14, pp. 19351–19375, Jun. 2022, doi: 10.1007/s11042-021-11018-4.

[21] C.-C. Lin, S.-L. He, and C.-C. Chang, "Pixel P air-wise fragile image watermarking based on HC-based absolute moment block truncation coding," *Electronics*, vol. 10, no. 6, p. 690, Mar. 2021, doi: 10.3390/electronics10060690.

[22] F. Tohidi, M. Paul, and M. R. Hooshmandasl, "Detection and recovery of higher tampered images using novel feature and compression strategy," *IEEE Access*, vol. 9, pp. 57510–57528, 2021, doi: 10.1109/ACCESS.2021.3072314.

[23] A. Aminuddin and F. Ernawan, "AuSR1: Authentication and self-recovery using a new image inpainting technique with LSB shifting in fragile image watermarking," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5822–5840, Sep. 2022, doi: 10.1016/j.jksuci.2022.02.009.

[24] C.-F. Lee, J.-J. Shen, Z.-R. Chen, and S. Agrawal, "Self-embedding authentication watermarking with effective tampered location detection and high-quality image recovery," *Sensors*, vol. 19, no. 10, p. 2267, May 2019, doi: 10.3390/s19102267.

[25] E. Gul and S. Ozturk, "A novel hash function based fragile watermarking method for image integrity," *Multimedia Tools Appl.*, vol. 78, no. 13, pp. 17701–17718, Jul. 2019, doi: 10.1007/s11042-018-7084-0.

[26] S. Sharma, J. J. Zou, and G. Fang, "A dual watermarking scheme for identity protection," *Multimedia Tools Appl.*, vol. 82, no. 2, pp. 2207–2236, Jan. 2023, doi: 10.1007/s11042-022-13207-1.

[27] H. M. Al-Otum, "Dual image watermarking using a multi-level thresholding and selective zone-quantization for copyright protection, authentication and recovery applications," *Multimed. Tools Appl.*, vol. 81, pp. 25787–25828, Mar. 2022, doi: 10.1007/s11042-022-11920-5.

[28] P. Khare and V. K. Srivastava, "A novel dual image watermarking technique using homomorphic transform and DWT," *J. Intell. Syst.*, vol. 30, no. 1, pp. 297–311, Sep. 2020, doi: 10.1515/jisys-2019-0046.

[29] C. Dong, C. C. Loy, and X. Tang, "Accelerating the super-resolution convolutional neural network," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9906. Springer-Verlag, 2016, pp. 391–407. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-46475-6_25, doi: 10.1007/978-3-319-46475-6_25.

[30] R. Sinhal, I. A. Ansari, and C. W. Ahn, "Blind image watermarking for localization and restoration of color images," *IEEE Access*, vol. 8, pp. 200157–200169, 2020, doi: 10.1109/ACCESS.2020.3035428.

[31] M. Rezaei and H. Taheri, "Digital image self-recovery using CNN networks," *Optik*, vol. 264, Aug. 2022, Art. no. 169345, doi: 10.1016/j.ijleo.2022.169345.

[32] K. Singla, R. Pandey, and U. Ghanekar, "A review on single image super resolution techniques using generative adversarial network," *Optik*, vol. 266, Sep. 2022, Art. no. 169607, doi: 10.1016/j.ijleo.2022.169607.

[33] J. Sun, J. Sun, Z. Xu, and H. Y. Shum, "Image super-resolution using gradient profile prior," in *Proc. 26th IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2008, pp. 1–8, doi: 10.1109/CVPR.2008.4587659.

[34] P. Bas, T. Filler, and T. Pevný, "Break our steganographic system': The ins and outs of organizing BOSS," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6958. Springer, 2011, pp. 59–70. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-24178-9_5, doi: 10.1007/978-3-642-24178-9_5.

NOVA RIJATI (Member, IEEE) received the bachelor's degree from the Mathematics Department, Universitas Diponegoro, Semarang, in 1995, the master's degree in informatics engineering from STTIBI, Jakarta, in 2001, and the Ph.D. degree in intelligent electrical and informatics technology from Institut Teknologi Sepuluh Nopember, Surabaya, in 2021. She is currently with the Informatics Department, Universitas Dian Nuswantoro, Semarang, Jawa Tengah, Indonesia. Her research interests include computer science, artificial intelligence, and data mining. She is also an IAENG Member.

DE ROSAL IGNATIUS MOSES SETIADI (Member, IEEE) received the bachelor's degree from the Department of Informatics Engineering, Soegijapranata Catholic University, Semarang Indonesia, in 2010, and the master's degree from the Department of Informatics Engineering, Dian Nuswantoro University, Semarang, Indonesia, in 2012. He is currently a Lecturer and a Researcher with the Faculty of Computer Science, Dian Nuswantoro University, Semarang, Indonesia. He has authored or coauthored more than 140 refereed journals and conference papers indexed by Scopus. His research interests include watermarking, steganography, image encryption, cryptography, and image recognition. He is one of the academic editors of the *Security and Communication* journal and *Journal of Computer Networks and Communications* (Hindawi) and one of the editorial board in the *Technology, Education, Management, Informatics* (TEM) journal. He is also a reviewer of more than 50 Scopus-indexed journals.