A Secure Image Authentication Scheme for Tamper Detection and Recovery

Te-Yu Chen[§] Min-Shiang Hwang[†] Jinn-Ke Jan[‡]

Department of Computer Science & Information Engineering[†]
Asia University
500, Liufeng Rd., Wufeng Dist., Taichung 41354,
Taiwan (R.O.C.)
Email: mshwang@asia.edu.tw
Fax: 886-4-23608845

Department of Computer Science and Engineering[‡]
National Chung Hsing University
250, Guoguang Rd., South Dist., Taichung 40227,
Taiwan (R.O.C.)

Department of Information Networking Technology[§]
Hsiuping Institute of Technology
11, Gongye Rd., Dali Dist., Taichung 41280,
Taiwan (R.O.C.)

May 23, 2011

[†]Corresponding Author: Prof. Min-Shiang Hwang

A Secure Image Authentication Scheme for Tamper Detection and Recovery

Abstract

In recent decades, many watermarking schemes for tamper detection and tampered image recovery have been proposed. However, most of these schemes suffered from several kinds of attacks due to the lack of considering security issues. In this paper, an improved and elaborately designed scheme is proposed after the drawbacks of these schemes are analyzed and discussed. The proposed scheme outperforms the other schemes in terms of the sensitivity to the alteration in the protected image as well as the resistibility to the well-known attacks, such as the counterfeit attack, the disturbing attack, and the leakage of the secret key. In addition, the watermarked images and the recovered images generated by the proposed scheme demonstrate competent qualities.

Keywords: Image authentication; Tamper detection and recovery; Watermarking.

1 Introduction

Due to the rapidly advancing computer software and hardware technologies, more and more applications of digital images have been developed and widespread. Coming in as digital files, digitalized images can be conveniently stored, modified, duplicated, and transmitted; however, along with all the convenience, there comes many security threats as well. Therefore, copyright protection and authentication on digital works deserve a lot of attention. From the viewpoint of a digital image creator or legal owner, a particular mechanism for the protection of the intellectual property rights needs to be established in order to prevent the work from being distributed without their permission [7, 20, 33].

From the viewpoint of a receiver, on the other hand, a particular design for integrity verification needs to be established to prevent the item from being tampered without proper authorization [17, 24, 25, 32].

Watermarking is the art of imperceptibly embedding some information into the original work while getting it more or less modified as a result. Because there is a limit to the sensitivity of human beings' sensory organs such as the eyes and the ears, we would experience difficulty telling the subtle differences made to multimedia works. Hence, watermarking can be considered as a satisfactory solution to the security issues for digital images.

As for the taxonomy of image watermarking, there are several categorizations for a variety of watermarking schemes [5, 23]. First of all, in terms of the domain of watermarking, schemes can be classified as either spatial domain watermarking schemes [3, 12, 13, 16, 17, 21, 28, 29] or transformed domain watermarking schemes [10, 11, 27, 34]. The former embeds the watermark by directly modifying the pixels' values of an image, while the latter usually embeds the watermark in the coefficients after performing certain transformation such as DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform), and DWT (Discrete Wavelet Transform) [8]. The spatial domain scheme gains the advantage on computational efficiency, while the transformed domain scheme gets the upper hand on robustness. On the other hand, in accordance with the application purpose, watermarking schemes can be categorized as either fragile watermarking schemes [4, 14, 15] or robust watermarking schemes [22, 27, 34]. As the names imply, the watermark embedded by a fragile watermarking scheme is sensitive to any modification. In other words, the embedded watermark will be destroyed if any unauthorized modification to the watermarked image takes place. Hence the goals of fragile watermarking are to verify the integrity and even to locate the tamper and to recover the image. On the contrary, embedding by a robust watermarking scheme, the watermark

hidden inside the watermarked image should be able to survive attacks done to the watermarked image, which means that a decent robust watermarking scheme is adequate to be adopted for the copyright or ownership protection.

Since a fragile watermarking scheme is used to indicate whether an image suffers from unauthorized modification, the ability of recovery from tampered image has attracted more and more attentions during the recent decade [2, 3, 12, 13, 21, 29].

Generally speaking, the terminology is described as follows. Before any processing, the image, needed to be protected with nothing embedded in it, is referred to as the cover image or the original image. Then, the information later embedded in the cover image is called the watermark, and the image with the watermark embedded in it is called the watermarked image. A watermarking scheme for tamper detection and recovery consists of two phases, namely the watermark embedding phase and the authentication phase which can be further partitioned into the tamper detection and tampered image recovery phase. The majority of watermarking schemes for tamper detection and recovery nowadays are performed on the spatial domain in which some LSBs (least significant bits) are replaced by the watermark in the watermark embedding phase. Then, in the authentication phase, if the watermarked image never underwent any malicious modification, then the watermarked image can pass the verification procedure. Otherwise, the malicious modification will be detected and the image can be further recovered from alteration.

An admissible watermarking scheme for tamper detection and recovery should satisfy the following criteria:

C1: Ability of tamper detection. Unauthorized modification to watermarked images should be detected by the scheme.

C2: Ability of tamper recovery. The scheme should be able to detect unauthorized modification on images and to recover them from

the tampered ones.

C3: Imperceptibility on watermarked images and high quality on recovered images.

C4: Resistant to known attacks. The scheme should be as robust as it could to the well-known attacks, such as the counterfeit attack, the disturbing attack, and the leakage of the secret key.

Several watermarking schemes designed for tamper detection and recovery have been proposed recently. Lin et al. proposed a block-based hierarchical digital watermarking method for image tamper detection and recovery in 2005 [13]. The checksum and the intensity of blocks are adopted to examine the tamper and to recover images respectively, while the precision of tamper detection and localization both achieved 100% in their experimental results. However, Chang et al. demonstrated that Lin et al.'s scheme is not secure enough in 2008 [2]. Two kinds of attacks, i.e., the four-scanning attack and the blind attack, were therefore raised to tamper a watermarked image without being detected. In 2007, a color image watermarking scheme for tamper detection and recovery was proposed by Wang and Chen [29]. They claimed that the scheme can effectively thwart the collage attack and the vector quantization attack. However, we found out that this scheme still suffers the counterfeit attack, the disturbing attack, and the leakage of the secret key. In 2008, Lee and Lin proposed a dual watermark scheme for image tamper detection and recovery [12]. Their design maintains two copies of a watermark for each block in the image, thus providing a second chance for block recovery in case one of the watermarks is destroyed. Hence, a 90% tampered image can be recovered to a recognizable image with the PSNR=20dB. Nevertheless, the large amount of space assigned for storing the recovery information decreases the space of verification information, thus restricting the scheme's robustness. Lee and Lin's scheme therefore suffers many kinds of attacks, such as the counterfeit

attack, the disturbing attack, and the leakage of the secret key. During the same year, Park et al. proposed a watermarking scheme for tamper detection and recovery [21] as well. In their scheme, owner's binary logo is also involved in the watermark and embedded into the image in addition to the verification information and the recovery information. Unfortunately, we found that Park et al.'s scheme cannot resist against the counterfeit attack, the disturbing attack, and the leakage of the secret key. In summary, this paper aims to tackle the above-mentioned security drawbacks and proposes a novel and efficient image watermarking approach for temper detection and recovery.

The rest of this paper is organized as follows. In Section 2, Park et al.'s scheme is reviewed and the weakness of their scheme is demonstrated accordingly in Section 3. Our improved scheme is then proposed in Section 4, while the analysis of our proposed scheme is presented in Section 5. Finally, the conclusions are drawn in Section 6.

2 Review of Park et al.'s Scheme

In this section, Park et al.'s scheme will be reviewed. First of all, the original image is divided into N non-overlapping blocks with a size of 4×4 pixels for each block. The blocks are then rearranged using a secret key K. The permutated blocks can be represented as $B = \{b_i | i = 1, 2, \cdots, N\}$. The permutation function is not explicitly indicated in their paper, so it is reasonable to suppose that a common well-known transformation, such as $X' = (K \times X \bmod N) + 1$, is adopted. In the following subsections, we will introduce Park et al.'s scheme in accordance with the following phases: the watermarking embedding, tamper detection, and tampered image recovery phase.

2.1 The Watermark Embedding Phase

The watermark of Park et al.'s scheme is composed of the verification code, the recovery code, and the owner code. Let $VC = \{vc_i | i = 1, 2, \cdots, N\}$ be the

set of the verification code, where vc_i is the verification code of the block b_i, which is set to 11-bit long. For the block b_i, the variance value va_i of the 16 pixels is firstly computed by using their 6 most significant bits (MSBs); then vc_i can be generated by the equation: $vc_i = (va_i \bmod 2^{11}) \oplus ID$, where ID is the identification of the image.

Let $RC = \{rc_i | i = 1, 2, \cdots, N\}$ be the set of the recovery code, where the 20-bit long rc_i is the recovery code of block b_i. To generate rc_i, the block b_i is further divided into four non-overlapping sub-blocks with size of 2×2 pixels. After the averaged values of 4 pixels in each sub-block are computed, rc_i can be generated by concatenating the 5 MSBs of the average values for each sub-block.

Let $OC = \{oc_i | i = 1, 2, \cdots, N\}$ be the set of the owner code, where the one-bit long oc_i is the ith pixel value of the owner's binary logo, after being permutated with the secret key K.

Using the verification code (VC), the recovery code (RC), and the owner code (OC), the watermark of Park et al.'s scheme can be generated as $W = \{w_i | w_i = rc_{i+1} || vc_i || oc_i, i = 1, 2, \cdots, N\}$. Note that, in order to preserve the capability of recovery, the watermark of a block involves the recovery code of its succeeding block in the block mapping order. The watermark of the last block b_N therefore should be $w_N = rc_1 || vc_N || oc_N$.

After generating the watermark for the target image, the watermark can be embedded into blocks one by one. For a block b_i, the 2 least significant bits (LSBs) of each pixel in b_i is replaced by the watermark, w_i, in the embedding procedure. Once the watermark embedding for each block has been completed, these blocks are permuted in the reverse manner by employing the secret key K and the watermarked image is generated accordingly.

2.2 The Tamper Detection Phase

To authenticate an image, the image is first divided into N non-overlapping blocks each with the size of 4×4 pixels. The blocks are then rearranged by applying the secret key K. The permutated blocks can be represented as $B = \{b_i | i = 1, 2, \cdots, N\}$. The following procedures are performed to verify whether a block has been tampered. For a block b_i, the watermark is extracted from its 2 LSBs of each pixel. The extracted watermark which is of 32 bits is further decomposed into the verification code, the recovery code, and the owner code. Let the extracted verification code, the extracted recovery code, and the extracted owner code be denoted as vc_i, rc_{i+1}, and oc_i, respectively. Then, the inherent verification code of b_i is computed as: $vc'_i = (va_i \bmod 2^{11}) \oplus ID$, where va_i is the variance value of b_i's 16 pixels computed using their 6 MSBs and ID is the identification of the image. The integrity of the block b_i can be indicated by comparing vc_i with vc'_i. After detecting all the blocks, the detection result of the image is generated as $D = \{d_i | d_i = 0, \text{if} vc_i = vc'_i; d_i = 1, \text{if} vc_i \neq vc'_i; i = 1, 2, \cdots, N\}$. If all the elements of D are 0, then there will not be any block being tampered; therefore, this image is correctly authenticated. Otherwise, those blocks corresponding to the elements with their values being equal to 1 in D are tempered and the recovery procedure should be performed for recovering this image.

2.3 The Tampered Image Recovery Phase

According to the structure of the watermark, the recovery information of a block is embedded in its preceding block in the permuted order. Therefore, in order to recover a tampered block, the extracted recovery code from its preceding block is necessary. For a block b_i with its corresponding detection indicator d_i being 1, the recovery procedure is performed as follows. The recovery code rc_i is firstly obtained from the extracted watermark to recover

the block b_i. For each sub-block of b_i, its recovery information which is of 5 bits is further decomposed from rc_i. Then each pixel in the sub-block is retrieved by assigning the five decomposed bits to its 5 MSBs and setting its 3 LSBs all to 0. After all of the 4 sub-blocks are revived, the recovery for the block is completed thereafter.

If there are some elements with the consecutive indices presented to the same value 1 in the detection result D, the recovery procedure would not work properly except for the first corresponding block. Since the block in which the recovery information is embedded is also being tampered; the suspicious recovery information therefore cannot be used to recovery the corresponding tampered block. In this case, there are some holes which are not regained in the image after the recovery procedure. To retain an approximate image, particular image processing technique can therefore be employed to patch these holes.

3 The Weaknesses of Park et al.'s Scheme

Park et al.'s scheme cannot resist against the counterfeit attack, the disturbing attack, and the leakage of the secret key. In the following, the details of how these attacks gain their purposes will be demonstrated.

3.1 The Counterfeit Attack

An image authentication scheme cannot resist against the counterfeit attack if an adversary can tamper or generate a significant watermarked image without being detected. In Park et al.'s scheme, the verification code vc_i for the block b_i is computed by $vc_i = (va_i \bmod 2^{11}) \oplus ID$, where ID is the identification of the image and va_i is the variance of pixels in the block. Hence, an adversary can tamper any pixel value at his/her will, and compute the new variance to derive a new verification code. Then the adversary can modify the watermark by replacing the old verification code with the new one. It is obvious that

the block tampered by this way will pass the tamper detection of Park et al.'s scheme, therefore the adversary can tamper any block by using the same way. Finally, a tampered image will be generated without being detected by Park et al.'s scheme. Moreover, the owner's logo extracted from the tampered image does agree fully with the original one, because non owner bit is changed during the tampering procedure.

In addition to the preceding counterfeit attack which directly forges each block, there are various kinds of counterfeit attacks deserved to be examined further [9], such as the cut-and-paste attack [1], VQ attack [9], and collage attack [6]. The cut-and-paste attack [1] happens when an adversary collects some legitimate watermarked images, which are of the same size and protected by the same watermark and the same secret keys, and cuts blocks from these collected images and pastes them together to form a forged image. The cut-and-paste attack is successful if the forged image is falsely verified as legitimate. In general, the scheme in which each block is watermarked independently without containing any contextual information usually suffers from the cut-and-paste attack [1, 9]. The adoption of the owner code slightly gives Park et al.'s scheme immunity against this kind of attack. Owing to the identity of an image being regarded as public, an adversary can easily replace the old identity with an intended one by performing exclusive-or operations in Park et al.'s scheme. After replacing the identity, this forged image cannot be detected as being tampered by checking the verification code. However the cut-and-paste will disorder the owner code and therefore be detected by checking the owner code. Nevertheless, if the owner code of the forged image is further replaced by that of a legitimate watermarked image while preserving their corresponding spatial locations, the forged image would completely pass the verification procedure of Park et al.'s scheme. Consequently, Park et al.'s scheme cannot resist against this kind of attacks.

In the VQ attack, the adversary should have a collection of legitimate watermarked images and construct the VQ code book from the blocks of the collected images. The VQ attack is performed similarly to the cut-and-paste attack except that the blocks, which will be pasted to form the forged image, are selected from the VQ code book constraining with the approximate visual appearance. If an adversary takes the identity of the image as well as the owner code into consideration, Park et al.'s scheme cannot totally thwart the VQ attack. The reason is similar to why Park et al.'s scheme cannot resist against the cut-and-paste attack.

The collage attack is also similar to the cut-and-paste attack except that the spatial location of the cut block is maintained to be the same as that of the pasted block, thus it is obvious that Park et al.'s scheme will suffer from the collage attack. Suppose that an adversary has collected a number of legitimate images watermarked by Park et al.'s scheme, all of these images are of the same size and protected with the same owner code and the same secret key. After replacing the old identity with the intended one by performing exclusive-or operations, the forged image can be generated by combining blocks from collected legitimate images while preserving their relative spatial locations the same with the forged image. Because the order of the owner code is kept unchanged, the forged image therefore passes the verification procedure of Park et al.'s scheme.

3.2 The Disturbing Attack

The disturbing attack happens when an adversary can elaborately disturb the pixels to trouble the tamper detection procedure of an image authentication scheme. Usually, if a watermarked image is altered by such attack, this tampered image is easily visible to human perception; nevertheless, it will pass the tamper detection procedure. The disturbing attack is also referred as the blind attack in [2].

If an image is tampered by modifying the pixels' values while keeping the variance of the pixels in each block unchanged, the tampered image would pass the detection procedure of Park et al.'s scheme. The variance of a set of values, x_1, x_2, $\cdots$, x_n, is defined as var $= \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})$, where $\bar{x}$ is the mean of all values. The method that changes the values of x's while keeping the variance unchanged can be used to perform this kind of attack in Park et al.'s scheme. There are many ways holding this property, such as a constant being added to or subtracted from all values in the set, or arbitrarily interchanging the values of x's with each other. Because Park et al.'s scheme computes the variance using only the 6 MSBs, an adversary can tamper a block by adding or subtracting a constant to or from the 6 MSBs of each pixel in a block and keeping the 2 LSBs unchanged. An adversary also can arbitrarily interchange the 6 MSBs of each pixel in a block. Through this method, an adversary can tamper an image without being detected.

If Park et al.'s scheme is further improved by encrypting the watermark, none of the encrypted watermark bits in a block alone indicates the verification code, the recovery code, and the owner code instead of bit-by-bit meaning. Such improvement makes an adversary infeasible to modify the verification code in the encrypted watermark without the decryption key. However, this improved scheme still suffers from the disturbing attack since it is unnecessary to modify any verification code in the disturbing attack.

3.3 The Compromise of The Permutation Secret Key K

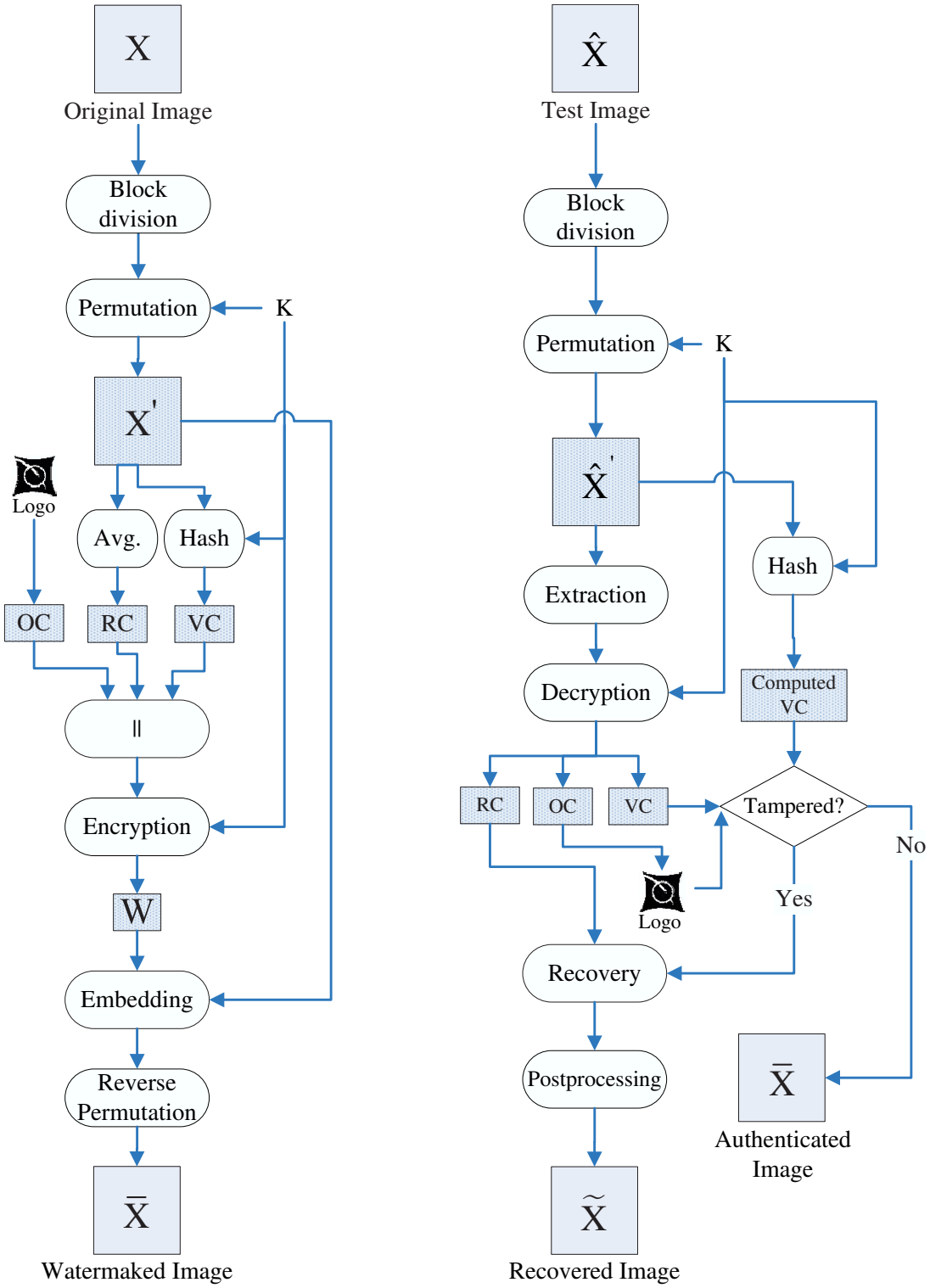
Another important role concerning the security in Park et al.'s scheme is the secret key K which is used to permute the blocks of an image and the pixels of the owner's logo. Although the permutation mechanism is not explicitly demonstrated in Park et al.'s paper, some public transformation, such as $X' = (K \times X \bmod N) + 1$, should be adopted to generate the block mapping. The following will show how an adversary can compromise the secret key K.

This attack is similar to the traditional dictionary attack. A dictionary is first generated by collecting all the verification codes embedded in blocks of the watermarked image. In Park et al.'s scheme, the recovery code of a block is embedded into another block according to the permutation. Based on the observation, the adversary can compute the corresponding recovery code rc_i for a specific block b_i; and then the adversary can search the dictionary to find out the dubious records from the constructed dictionary. If only one record is searched, the adversary can adopt the correlation to compute the secret key K according to the transformation. Otherwise, if the searched dubious correlations are more than one, the adversary will obtain some candidates for the secret key K computed from the transformation. The adversary should select another block and perform the above searching procedure. After collecting enough information, the secret key K can be uniquely determined. Once the secret key K is compromised, the adversary can carry out any attack on his/her own will. This type of attack is similar to the four-scanning attack referred in [2].

4 The Proposed Scheme

In this section, an improved image authentication scheme for tamper detection and recovery is proposed. Similar to most of the related schemes, the proposed scheme is composed of the watermark embedding as well as the tamper detection and recovery phases. The framework of our proposed scheme is illustrated in Figure 1.

For the image authentication schemes with the capabilities of tamper detection and recovery, the design of watermark is the most important part and the other attached mechanisms which are very similar in almost all the schemes can be intuitively deduced. We will therefore concentrate on how the watermark of our scheme is designed in detail for the following description.



(a): The watermark embedding process (b): The tamper detection and recovery process

Figure 1: The framework of our proposed scheme

4.1 The Watermark Embedding Phase

In our proposed scheme, the original image is divided into N non-overlapping blocks which are of the size 2×2 pixels for each. The blocks are rearranged using the following mapping function:

$$X' = [f(X) = K \times X \bmod N] + 1,$$

where X and X' are the original and the mapped block indices, respectively. N is the number of blocks in the image, K is a secret key which could be any of the primes while not being the factors of N. Let $B = \{b_i | i = 1, 2, \cdots, N\}$ be the blocks after being rearranged using the mapping function and the secret key K. The watermark of our design is constructed by three components: the verification code (VC), the recovery code (RC), and the owner code (OC).

The verification code is denoted as $VC = \{vc_i | i = 1, 2, \cdots, N\}$, in which vc_i being of 6 bits is the verification code of block b_i. A hash function, $h(\cdot)$, is employed to generate the verification code. In practice, the hash function can be designed by adapting checksums, fingerprinting algorithms, or cryptographic hash functions, such as the MD5 or SHA hash functions [18, 19, 26]. For security reasons, adopting the SHA hash function is suggested. The choice of an appropriate hash function is actually a trade-off between security level and computational complexity. For block b_i, the verification code vc_i can be obtained from the equation: $vc_i = h(p_{i1}||p_{i2}||p_{i3}||p_{i4}||i||K||ID)$, where p_{i1}, p_{i2}, p_{i3}, and p_{i4} are the values of 4 pixels setting their 3 LSBs to 0 in the block b_i, K is the secret key, and ID is the identity of this image. If the output of the adopted hash function is longer than 6 bits, the hash value is further divided into multiple segments in which the length of each segment is 6 bits. The verification code is therefore modified as the value which is generated by performing the exclusive-or on all the segments.

The recovery code is denoted as $RC = \{rc_i | i = 1, 2, \cdots, N\}$, in which rc_i being of 5 bits is the recovery code of block b_i. The recovery code rc_i is the 5

MSBs of the average intensity of 4 pixels in the block b_i.

The owner code is denoted as $OC = \{oc_i | i = 1, 2, \cdots, N\}$, in which oc_i being of 1 bit is the ith pixel value of the owner's binary logo.

After the verification code (VC), the recovery code (RC), and the owner code (OC) are computed, the watermark can be constructed as $W = \{w_i | w_i = E_K(rc_{i+1}||vc_i||oc_i), i = 1, 2, \cdots, N-1; w_i = E_K(rc_1||vc_i||oc_i), i = N\}$, where E_K is represented as a symmetric encryption function with the secret key K. For the implementation consideration, the symmetric encryption function could be any one of the well-known symmetric encryption algorithms, such as the DES, IDEA, Blowfish, RC5, or AES [26]. Furthermore, owing to the 12 bits length of watermark in a block, the symmetric encryption function should be performed in the CFB (Cipher Feedback) mode or OFB (Output Feedback) mode [26] to meet the limited length. Note that in order to preserve the recovery ability, the watermark of a block involves the recovery code of its succeeding block in the block mapping; consequently, the watermark of the last block b_N should be $w_N = E_K(rc_1||vc_N||oc_N)$.

Once the watermark for the image has been prepared, the watermark can be embedded into blocks one by one. For a block b_i, the watermark w_i is embedded into b_i by replacing 3 LSBs of each pixels in b_i with w_i. After the watermark embedding for each block is completed, these blocks are permuted in the reverse manner by employing the secret key K and the watermarked image is generated correspondingly.

4.2 The Tamper Detection Phase

To authenticate an image, the given image is first divided into N non-overlapping blocks of size 2×2 pixels. These blocks are then rearranged using the secret key K. Let the permutated blocks be represented as $B = \{b_i | i = 1, 2, \cdots, N\}$. The following procedures are performed to examine whether a block has been altered or not. For a block b_i, the watermark is extracted from its 3 LSBs

of each pixel. The extracted watermark which is of 12 bits is then decrypted using the secret key K. The verification code, the recovery code, and the owner code can be further retrieved according the proper position of the bit presentation from decrypted watermark. Let the extracted verification code, the extracted recovery code, and the extracted owner code be denoted as vc_i, rc_{i+1}, and oc_i, respectively. Then, the inherent verification code of b_i is computed as: $vc'_i = h(p_{i1}||p_{i2}||p_{i3}||p_{i4}||i||K||ID)$, where p_{i1}, p_{i2}, p_{i3}, and p_{i4} are the values of 4 pixels setting their 3 LSBs to 0 in the block b_i, K is the secret key, and ID is the identity of this image. The same as described in the previous section, if the output of the adopted hash function is longer than 6 bits, the hash value would be further processed to obtain the 6-bit verification code.

The integrity of the block b_i can be indicated by comparing vc_i with vc'_i. After all the blocks have been examined, the detection result of the image is generated as $D = \{d_i | d_i = 0, \text{if} vc_i = vc'_i; d_i = 1, \text{if} vc_i \neq vc'_i; i = 1, 2, \cdots, N\}$. That is, $d_i = 0$ indicates that b_i is authenticated, whereas $d_i = 1$ indicates that b_i is tampered. If all the elements of D are 0, then no block will be tampered; therefore, this image is authenticated. If certain elements of D are not 0, then those blocks corresponding to the elements whose values are equal to 1 in D are tampered so the recovery procedure should be performed further for recovering this image.

4.3 The Tampered Image Recovery Phase

If there are some blocks being detected as tampered, the tampered image recovery procedure should be invoked to revive theses blocks. The recovery information of a block is embedded in its preceding block in the permuted order according to the design of the watermark. Hence, the tampered block could be recovered to the original ones approximately by extracting the recovery code from its preceding block in the permuted order. For a block b_i whose corresponding detection indicator d_i is 1, the recovery procedure could be

performed as follows. The recovery code rc_i which is of 5 bits is extracted first. Three 0's are padded to the end of rc_i to form an 8-bit value for recovery. All the pixel values are replaced with this 8-bit value and the recovery for the block b_i is completed thereafter.

If there are some elements with the consecutive indices having the same value 1 in the detection result D, the recovery procedure does not work except for the leading corresponding block. The questionable recovery information therefore cannot be used to recovery the corresponding tampered block because the block employed to embed the recovery information is also be tampered. If this situation happens, there are some blocks which are tampered but could not be recovered would be presented in the image after the previous recovery procedure. The remaining unrecovered blocks could be revived with the pixels surrounding them by employing some image processing technique.

5 Analysis of Security and Quality

In this section, we evaluate and discuss several aspects of the proposed image authentication scheme for tamper detection and recovery. First, the security issues of our scheme are analyzed in detail. Then, the qualities of the watermarked and recovered images are evaluated.

5.1 Security Analysis

In the following subsection, we deliberate on the security of our proposed scheme, while the analysis proves that our proposed scheme is secured against the well-known attacks, such as the counterfeit attack, the disturbing attack, and the leakage of the secret key.

5.1.1 The counterfeit attack

The reason why the counterfeit attack gains its purpose successfully can be concluded that the generation and embedding of the verification code can be performed by anyone. Therefore, any adversary can forge a block without being detected by computing the corresponding verification code and replace it with the original one. In order to prevent our proposed scheme from suffering this type of attack, the generation of the verification code which is $vc_i = h(p_{i1}||p_{i2}||p_{i3}||p_{i4}||i||K||ID)$ in our scheme involves a secret key K. Without the secret key K, no one can compute a correct verification code. Moreover, the adoption of hash function makes our scheme very sensitive to any change to a block. Comparing with the other approaches, such as the intensity, the variance, and the exclusive-or, the hashing value of pixels is more easily affected by any alteration. Hence the detection ability of our proposed scheme is more precise than other schemes. Furthermore, it is infeasible for any adversary to forge a valid watermark since it is protected by encrypting with a secret key.

The elaborate design of the verification code also makes the cut-and-paste attack [1], VQ attack [9], and collage attack [6] not executable in our proposed scheme. The employ of the block index in the verification code prevents the cut-and-paste attack and VQ attack. If an adversary further takes the positions of blocks into consideration and generates a forged image in which the spatial positions of blocks are preserved, this trickery would still be exposed because the identity of the image is involved in the verification code. Moreover, if the adversary tries to replace the identity with an intended one, this attempt would be defeated because neither the valid verification code nor the valid watermark can be generated without the secret key. Therefore, the collage attack is also defeated by our proposed scheme.

5.1.2 The disturbing attack

The disturbing attack happens when the pixel values can be tampered while keeping the verification code of the tampered pixels unchanged. This kind of attack is frequently found in the image authentication schemes which employ the intensity, the variance, or the exclusive-or to generate their verification code. An adversary can easily adjust the pixel values to meet the unchanged intensity, variance, or exclusive-or value. However, the disturbing attack is thwarted by our elaborate design of the verification code. A hash function is employed to generate the verification code in our proposed scheme. According to the property of hash function, it scarcely finds out any collision in which the same hash value is produced from two different inputs in a hash function. Hence, it is infeasible for an adversary to tamper any pixel value while preserving the verification code unchanged. The disturbing attack is hardly performed in our proposed scheme as a result.

5.1.3 The leakage of the secret key

In order to recover a tampered block, the recovery information is embedded into another block in most image authentication schemes for tamper recovery. A secret key, which is used to generate the block mapping, is highly related to the robustness of a scheme and should be carefully protected. However, since the recovery information is embedded directly using its plaintext form in almost all the other schemes, such as [12, 13, 21, 29], the mapping correlation would therefore be revealed by comparing the computed recovery information with the extracted one. An adversary can proceed to apply the revealed mapping correlations to determine the secret key in these schemes. In order to prevent the leakage of the secret key, the mapping correlation of blocks could not be revealed. Hence, the watermark is further encrypted before it is embedded in our proposed scheme. Anyone can neither retrieve the recovery

information concealed in the encrypted watermark, nor find out the mapping correlation of blocks to determine the secret key. Consequently, our scheme is robust to the leakage of the secret key.

5.1.4 The cropping attack

The cropping attack happens when some marginal rows or/and columns of blocks are removed from the watermarked image. Those schemes which are designed only to confirm the validity for each individual block cannot resist to the cropping attack, since those schemes are not aware of the vanished blocks. However, the proposed scheme is resistant to the attack in which some blocks are removed from the image. In our design, the owner's binary logo is distributed over each block. Therefore, the disappearance of any block will be detected immediately from the retrieved owner's binary logo.

5.1.5 Remarks about the collision of the verification code

In our design, the verification code for each block is derived by the following steps: First, to hash the concatenation of the pixel values, the block index, the secret key, and the image identity. Second, to divide the hashed value into multiple segments which being of 6 bits for each. Finally, perform exclusive-or (XOR) on all of the segments to obtain a 6-bit verification code. It is foredoomed to collision by mapping a large domain which includes the pixel values, the block index, the secret key, and the image identity into a small co-domain which is 6 bits long. If any attacker can tamper the pixel values while preserving the corresponding verification code unchanged, the attacker has performed the counterfeit attack successfully. Therefore, the condition of collision should be taken into serious consideration. Fortunately, a secret key K is involved in the computation of the verification code in our design. None

attacker can get the knowledge about the secret key K. Accordingly, the only way for an attack to counterfeit a valid block, in which the pixel values are different from an intended one while their verification codes are the same, is by blindly guessing. The probability for the attacker to make a correct guessing on one block is only $1/2^6$ owing to the length of a verification code is 6-bit long. Consequently, the probability for an attacker to perform this kind of attack which takes advantage of the collision of the verification code is low enough to be negligible.

Another situation, which also results from the collision of the verification code, deserves to be considered since some blocks could have the same watermark in an image. If an attacker examines all the blocks of an image and finds out some blocks have the same watermark, he/she can arbitrarily interchange theses blocks and the tampered image won't be detected by our verification. However, this situation happens with a negligible probability because these blocks should have the same verification code, the same owner code, as well as the same recovery code succeeded to their corresponding blocks in the mapping with the secret key K. Furthermore, this attack can be deterred by performing the following steps in order to confirm the consistency of the recovery information.

1. Obtain the recovery code rc_{i+1} from the block b_i.
2. Compute the recovery code rc'_{i+1} of the block b_{i+1}.
3. Compare rc_{i+1} with rc'_{i+1}.

By putting the supplementary verification for each block together with our verification procedure, our scheme is resistant to this type of attack.

From the above analysis, it is convinced that our proposed scheme can resist to these known attacks. The comparisons of the robustness against to

these attacks between our scheme and the related schemes are shown in the upper part of Table 1. According to the comparisons, our scheme has shown obvious robustness compared to the related schemes.

Table 1: Functionality comparisons among all the related schemes

Schemes/Criterion	Ours	[13]	[29]	[12]	[21]
Robustness					
Resistance to counterfeit attack	Yes	No	No	No	No
Resistance to cut-and-paste attack	Yes	Yes	Yes	No	Yes*
Resistance to VQ attack	Yes	Yes	Yes	No	Yes*
Resistance to collage attack	Yes	Yes	Yes	No	No
Resistance to disturbing attack	Yes	No	No	No	No
Resistance to leakage of the secret key	Yes	No	No	No	No
Resistance to cropping attack	Yes	Yes	No	No	Yes
Factors concerning the image quality					
Block size	2×2	4×4	2×2	2×2	4×4
Detection granularity	2×2	4×4	2×2	2×2	4×4
Recovery granularity	2×2	2×2	2×2	2×2	2×2
Recovery intensity	5 bits	6 bits	5 bits	5 bits	5 bits
Wmk Embedding	3 LSBs	2 LSBs	3 LSBs	3 LSBs	2 LSBs
* : Certain mechanism should be additionally adopted to resist the attack.					

5.2 The Quality Analyzes on The Watermarked and Recovered Images

5.2.1 The Quality of Watermarked Image

In the literature, almost all the recent watermarking schemes for tamper detection and recovery are block-wise and designed in the spatial domain. That is, these schemes divide an image into blocks and replace the least significant bits of pixels in each bock with the watermark. The replacement may introduce some amounts of distortion. Therefore, the quality of the watermarked image fully depends on the number of the LSBs which are replaced with the watermark in a pixel. The following theorem generally analyzes the quality of the watermarked image generated by these schemes.

Theorem 5.1 *The PSNRs of the watermarked images generated by replacing 2 LSBs or 3 LSBs of each pixel with the watermark is 44.15 dB or 37.92*

dB, respectively. Furthermore, if the optimal LSB replacement is adopted, the PSNRs will be improved to be 46.36 dB or 40.73dB for 2 LSBs or 3 LSBs replacement, respectively.

Proof. The PSNR of the watermarked image generated by replacing 3 LSBs of each pixel with the watermark is first analyzed. Let the image have the dimension of $m \times m$, and let x_{ij} and y_{ij}, $0 \leq i, j \leq m-1$, be the pixel values of the cover image and watermarked image, respectively. The mean square error (MSE) is defined as $MSE = \left(\frac{1}{m^2}\right) \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} (x_{ij} - y_{ij})^2$. Because only the 3 LSBs may be different in each corresponding pixels, both the pixel values x_{ij} and y_{ij}, can be translated to x'_{ij} and y'_{ij} for simplifying the evaluation of the MSE, where $x'_{ij} = (x_{ij} \bmod 2^3)$ and $y'_{ij} = (y_{ij} \bmod 2^3)$. Therefore, the values of x'_{ij} and y'_{ij} can be regarded as two random variables X and Y, both uniformly distributed in the sample space $\{0, 1, \cdots, 7\}$. The MSE can be evaluated as the expected value of $(X-Y)^2$, and the result value can be obtained as 10.5.

$$\begin{aligned} MSE &= E((X-Y)^2) \\ &= \left(\frac{1}{m^2}\right) \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} (x_{ij} - y_{ij})^2 \\ &= \left(\frac{1}{m^2}\right) \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \left(x'_{ij} - y'_{ij}\right)^2 \\ &= 10.5 \end{aligned}$$

Accordingly, the PSNR can be computed as

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} dB = 10 \log_{10} \frac{255^2}{10.5} dB = 37.92 dB.$$

If the optimal LSB replacement [30] is adopted, the MSE can be reduced to 5.5 and the PSNR is improved to be 40.73dB consequently. The PSNR of the watermarked image generated by replacing 2 LSBs of each pixel with the watermark can be derived by a similar way, and the value will be 44.15dB and 46.36 dB depending on whether the optimal LSB replacement is adopted or not. This completes the proof. *Q.E.D.*

In our scheme, the watermarked image is generated by replacing 3 LSBs of the original image with the watermark for each pixel. Therefore, the PSNR of the watermarked image of our scheme is concluded to be about 40.73dB from Theorem 5.1.

5.2.2 The Quality of Recovered Image

Once an image is tampered, the tampered block will be detected and localized in the tamper detection procedure. In the recovery procedure, the recovery information embedded in the image will be retrieved and contributed to revive the tampered block. There are three main factors highly affecting the quality of the recovered image, described as follows.

The first one is the detection granularity. The detection procedures of all the related schemes were performed in a block-wise manner and designed to determine whether a block is tampered by comparing the computed verification code with the embedded one of the block. The detection granularity is then defined as the size of a block which the detection procedure estimates whether this block is tampered. Therefore, the larger the detection granularity is, the lower the detection precision is. In addition, the recovery procedure is triggered by the result of the detection procedure. Even if only a single pixel in a block is tampered, the whole block will be treated as infected and be restored by the recovery information. In the situation where only some scattered pixels are tampered, like the salt and pepper noise, the quality of the recovered image will be dramatically degraded if a large detection granularity is adopted. The detection granularity is 2×2 in our proposed scheme. As shown in Table 1, the detection granularity of our scheme is smaller than those of some related schemes. Our scheme therefore gains a higher detection precision and a better quality for the recovered image.

The second factor is the similarity between the recovery information and the original block. The more knowledge of the original block is stored in

the recovery information, the higher quality of the recovered image will be obtained. However, in order to preserve the quality of watermarked image, the allocated space for the watermark is limited, and the recovery information is constrained accordingly. All the proposed schemes design their recovery information by taking some most significant bits (MSBs) after averaging the pixel values in a block and using this value to recover all the pixels of the block in the situation that the block is detected as being tampered. The number of MSBs which are gathered to form the recovery information for each block is defined as the recovery intensity, while the size of the block is defined as the recovery granularity. Therefore, the more bits of the recovery intensity are, the higher quality of the recovered image will be obtained. In our approach, there are 5 MSBs taken as the recovery information for each block and the block size is 2×2, i.e., the recovery intensity is 5 bits and the recovery granularity is 2×2. From the comparisons shown in in the lower part of Table 1, our proposed scheme competes with the related schemes in this view-point.

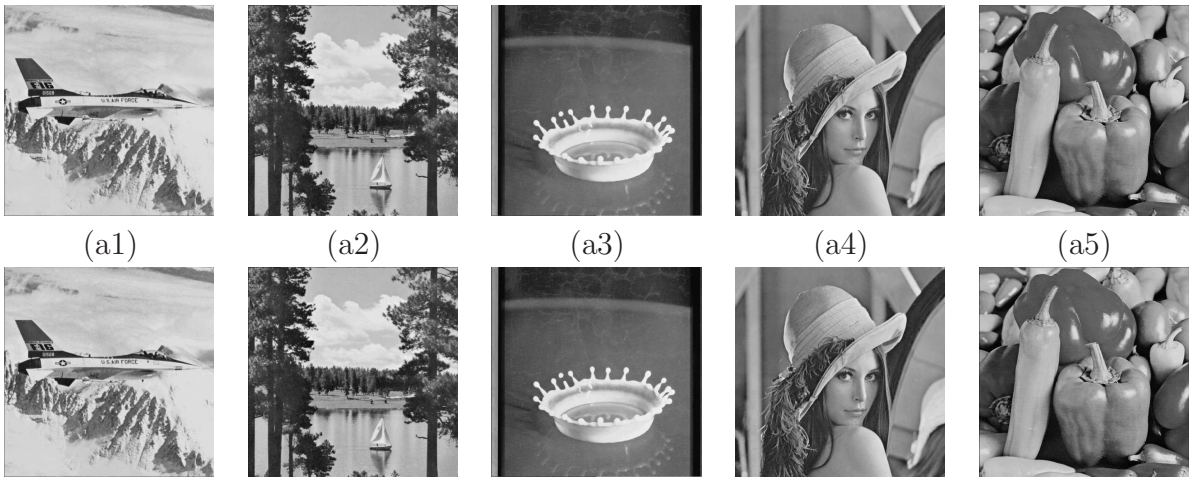
The third main factor affecting the quality of the recovered image is the block mapping function which determines the location where the recovery information of a block is embedded. If the block, say A, which holds the recovery information of a tampered block, say B, is also tampered unfortunately, the recovery information of block B, which is stored in block A, is dirty and could not be used to revive block B. Though block B can be recovered by the average intensity of its neighboring blocks, however, this circumstance will degrades the recovered images. In general, if a block is tampered, it is highly possible that its surrounding blocks are tampered as well. For this reason, the recovery information of a block should be embedded far from the block. Therefore, the mapping function is important to the quality of the recovered image. The block mapping function, i.e., $X' = [f(X) = K \times X \bmod N] + 1$, which is also adopted by most of the related schemes [12, 13, 29], satisfies this requirement.

Hence, the quality of the recovered images is comparable to those of the related schemes from this viewpoint.

The factors concerning the qualities of recovered images among all the related schemes are summarized in the lower part of Table 1. Comparing with the other related schemes, our proposed scheme is competent from the analysis of these factors.

5.3 Experimental Results

In this section, the experimental results of our proposed scheme are illustrated. We implemented our method in MATLAB. To verify our method, five images with size 512×512 shown in Figure 2(a1)$\sim$(a5) were chosen from the USC-SIPI Image Database [31].



(a1) (a2) (a3) (a4) (a5)

(b1) (b2) (b3) (b4) (b5)

Figure 2: The original and watermarked images. (a1)$\sim$(a5): the original images, Airplane, Sailboat, Splash, Lenna, and Pepper, arranged from left to right; (b1)$\sim$(b5): the corresponding watermarked images generated by the proposed scheme.

The watermarked images generated by our proposed scheme are shown in Figure 2(b1)$\sim$(b5), and the PSNRs of the watermarked images are listed in Table 2. It is obvious that the watermarked images are visually indistinguishable from their corresponding original images. In our scheme, the watermark is embedded in the 3 LSBs of each pixel. According to the theoretical analysis

in previous section, the PSNR will approximately be 37.92 dB. As shown in Table 2, the PSNRs of the watermarked images are all close to but slightly better than the theoretical value, due to the fact that the extreme situations which degrade the PSNR happen rarely in natural images. Therefore, it is reasonable to obtain the resulted PSNRs.

Table 2: The PSNRs of the watermarked images

Images	Airplane	Sailboat	Splash	Lenna	Pepper
PSNR(in dB)	38.31	38.21	38.39	38.62	38.44

As shown in Figure 3, some experiments have been made to validate the proposed scheme. First, the image "Splash" is adopted. The watermarked image "Splash" is shown in Figure 3(a1). As shown in Figure 3(b1), the tampered image is manipulated by attaching some white drops to the outside of the splash. The detection result is shown in Figure 3(c1). It is clear that the tampered region can be correctly localized. Figure 3(d1) is the recovered image of Figure 3(b1). To make a comparison between the recovered image, shown in Figure 3(d1), and the watermarked image, shown in Figure 3(a1), the PSNR of 48.93 dB indicates that it is well recovered.

In Figure 3(b2), the watermarked image "Sailboat" shown in Figure 3(a2) is tampered by inserting an F16 which is cut from another watermarked image "Airplane". Figure 3(c2) presents the detection result in which the tampered region is localized. The image recovered from Figure 3(b2) is illustrated in Figure 3(d2) with an image quality of 43.32 dB.

Figure 3(a3) is the watermarked image "Lenna". In Figure 3(b3), Lenna's face is covered with a black rectangle. Figure 3(c3) shows the detection result. The recovered image is illustrated in Figure 3(d3) with PSNR being 39.41 dB. Although all of Lenna's facial features disappeared, the proposed scheme restored the tampered image well.

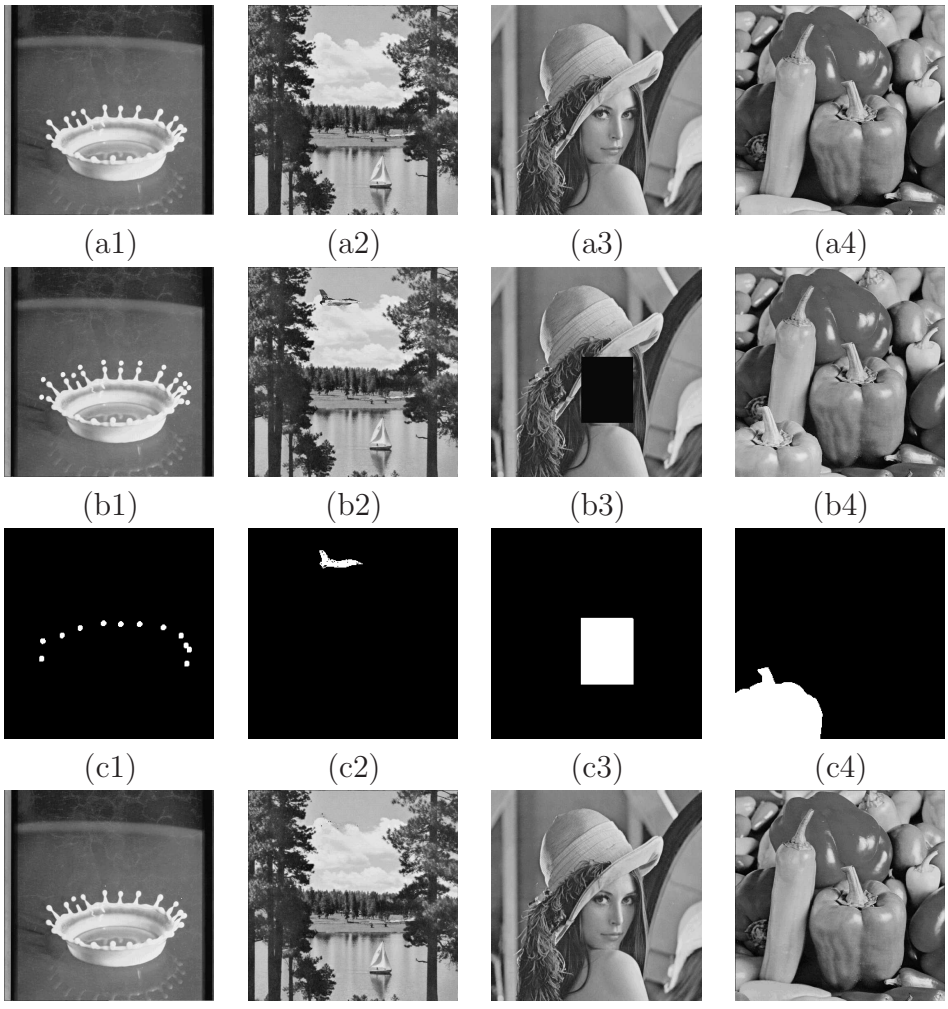


Figure 3: Tamper detection and recovery results. (a1)∼(a4): the watermarked images; (b1)∼(b4): the tampered images; (c1)∼(c4): the detection results; (d1)∼(d4): the recovered images.

As shown in Figure 3(b4), the modification made to the watermarked image "Pepper" shown in Figure 3(a4) is done by copying the bell pepper at the center and pasting it to the bottom-left corner of the image. The detection result and the recovered image are illustrated in Figure 3(c4) and Figure 3(d4), respectively. The PSNR value of the recovered image is 35.31 dB. The tampered region is well detected and recovered.

6 Conclusions

In this paper, a more secured watermarking scheme for tamper detection and recovery is proposed. This proposed scheme not only discovers any unauthorized modification and restore the image, but also preserves high image qualities which are comparable to the related schemes regardless of the watermarked images or the recovered images. Under the assumption that the watermarking algorithm is open, our proposed scheme is the only one that can resist against the most well-known attacks. The verification and recovery information play important roles in an image authentication scheme for tamper detection and recovery. The verification information is used to detect whether the image suffers from being altered. The design principle of the verification information mainly concentrates on how to make it sensitive enough to detect any alteration. In this research, we found that employing a hash function for the generation of the verification information is an effective way to strengthen the capability of temper detection. The recovery information is used to recover the image once it has been altered, and the design principle of the recovery information mainly concentrates on how to make it greatly resemble in the correspondent block. Moreover, both the verification and recovery information should not appear as plaintext in the image for the security considerations. Hence, we concluded that the approach with the watermark protected by encryption demonstrated successful results in avoiding security

threats.

In addition, the longer the watermark is, the more information about the verification and recovery can be maintained. Therefore, a longer watermark generally results in more accurate tamper detection and a better quality on recovered image. However, the length of the watermark should be constrained for guaranteeing the watermarked image from serious distortion. Hence, how to simultaneously enhance the precision of tamper detection and the quality of the recovered image while preserving the quality of the watermarked image should be taken into consideration in the future research.

References

[1] P. S. L. M. Barreto, H. Y. Kim, and V. Rijmen. Toward a secure public-key blockwise fragile authentication watermarking. In *International Conference on Image Processing*, volume 2, pages 494–497. IEEE, October 2001.

[2] C. C. Chang, Y. H. Fan, and W. L. Tai. Four-scanning attack on hierarchical digital watermarking method for image tamper detection and recovery. *Pattern Recognition*, 41(2):654–661, 2008.

[3] C. C. Chang, Y. S. Hu, and T. C. Lu. A watermarking-based image ownership and tampering authentication scheme. *Pattern Recognition Letters*, 27(5):439–446, 2006.

[4] C. C. Chang, P. Y. Lin, and J. C. Chuang. Fragile watermarking scheme for digital image authentication using pixel difference. *The Imaging Science Journal*, 55(3):140–147, 2007.

[5] J. B. Feng, I. C. Lin, C. S. Tsai, and Y. P. Chu. Reversible watermarking: Current status and key issues. *International Journal of Network Security*, 2(3):161–171, 2006.

[6] J. Fridrich, M. Goljan, and N. Memon. Further attacks on Yeung-Mintzer fragile watermarking scheme. In *SPIE Conference on Security and Watermarking of Multimedia Contents*, volume 3971, pages 428–437, San Jose, California, January 2000.

[7] G. Voyatzis and I. Pitas. Protecting digital-image copyrights: A framework. *IEEE Computer Graphics and Applications*, 1:18–24, 1999.

[8] R. C. Gonzalez and R. E. Woods. *Digital Image Processing*. Prentice Hall, 3rd edition, 2008.

[9] M. Holliman and N. Memon. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes. *IEEE Transactions on Image Processing*, 9(3):432–441, 2000.

[10] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin. A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression. *IEEE Transactions on Circuits and Systems for Video Technology*, 13(8):776–786, 2003.

[11] X. Kang, W. Zeng, and J. Huang. A multi-band wavelet watermarking scheme. *International Journal of Network Security*, 6(2):121–126, 2008.

[12] T. Y. Lee and S. D. Lin. Dual watermark for tamper detection and recovery. *Pattern Recognition*, 41(11):3497–3506, 2008.

[13] P. L. Lin, C. K. Hsieh, and P. W. Huang. A hierarchical digital watermarking method for image tamper detection and recovery. *Pattern Recognition*, 38(11):2519–2529, 2005.

[14] C. S. Lu and H.-Y.M Liao. Multipurpose watermarking for image authentication and protection. *IEEE Transactions on Image Processing*, 10(10):1579–1592, 2001.

[15] H. Lu, R. Shen, and F. L. Chung. Fragile watermarking scheme for image authentication. *Electronics Letters*, 39(12):898–900, 2003.

[16] H. C. Lu, Y. P. Chu, and M. S. Hwang. New steganographic method of pixel value differencing. *Journal of Imaging Science and Technology*, 50(5):424–426, 2006.

[17] Z. M. Lu, C. H. Liu, and H. Wang. Image retrieval and content integrity verification based on multipurpose image watermarking scheme. *International Journal of Innovative Computing Information and Control*, 3(3):621–630, 2007.

[18] NIST. Secure hash standard. *http://csrc.nist.gov/publications/fips*, 2002. FIPS PUB 180-2.

[19] NIST. The keyed-hash message authentication code (HMAC). *http://csrc.nist.gov/publications/fips*, 2008. FIPS PUB 198-1.

[20] J.J.K. O'Ruanaidh, W.J. Dowling, and F.M. Boland. Watermarking digital images for copyright protection. In *IEE Proceedings on Image and Signal Processing*, volume 143, pages 250–256, August 1996.

[21] Y. Park, H. Kang, K. Yamahuchi, and K. Kobayashi. Watermarking for tamper detection and recovery. *IEICE Electronics Express*, 5(17):689–696, 2008.

[22] S. Pereira and T. Pun. Robust template matching for affine resistant image watermarks. *IEEE Transactions on Image Processing*, 9(6):1123–1129, 2000.

[23] B. Pfitzmann. Information hiding terminology. In R. Anderson, editor, *Proceedings of First International Workshop on Information Hiding*, volume 1174 of *Lecture Notes in Computer Science*, pages 347–350, Berlin, 1996. Springer.

[24] C. Rey and J. L. Dugelay. A survey of watermarking algorithms for image authentication. *EURASIP Journal on Applied Signal Processing*, 2002(6):613–621, 2002.

[25] J. J. Shen and P. W. Hsu. A fragile associative watermarking on 2D barcode for data authentication. *International Journal of Network Security*, 7(3):301–309, 2008.

[26] William Stallings. *Cryptography and Network Security*. Prentice Hall, 4th edition, 2006.

[27] S. Suthaharan and S. Sathananthan. Transform domain technique: robust watermarking for digital images. In *Proceedings of the IEEE Southeastcon 2000*, pages 407–412, April 2000.

[28] C. M. Wang, N. I. Wu, C. S. Tsai, and M. S. Hwang. A high quality steganographic method with pixel-value differencing and modulus function. *Journal of Systems and Software*, 81(1):150–158, 2008.

[29] M. S. Wang and W. C. Chen. A majority-voting based watermarking scheme for color image tamper detection and recovery. *Computer Standards and Interfaces*, 29(5):561– 570, 2007.

[30] R. Z. Wang, C. F. Lin, and J. C. Lin. Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognition*, 34(3):671–683, 2001.

[31] A. Weber. The USC-SIPI image database. *The Signal and Image Processing Institute of the University of Southern California. Available at: http://sipi.usc.edu/database/*, 1977.

[32] C. C. Wu, M. S. Hwang, and S. J. Kao. A new approach to the secret image sharing with steganography and authentication. *The Imaging Science Journal*, 57(3):140–151, 2009.

[33] N. I. Wu, C. M. Wang, C. S Tsai, and M. S Hwang. A certificate-based watermarking scheme for coloured images. *The Imaging Science Journal*, 56(6):326–332, 2008.

[34] K. S. Yoo and W. H. Lee. Classification-based image watermarking using wavelet DC components. *The Imaging Science Journal*, 58(2):105–111, 2010.