Reversible Watermarking: Current Status and Key Issues

Jen-Bang Feng[1], Iuon-Chang Lin[2], Chwei-Shyong Tsai[2], and Yen-Ping Chu[3]
(Corresponding author: Iuon-Chang Lin)

Institute of Computer Science, National Chung Hsing University[1],
250 Kuo Kuang Rd., Taichung, Taiwan 402, R.O.C. (Email: phd9213@cs.nchu.edu.tw)
Department of Management Information Systems, National Chung Hsing University[2],
250 Kuo Kuang Rd., Taichung, Taiwan 402, R.O.C. (Email: {iclin;tsaics}@nchu.edu.tw)
Computer Science and Information Engineering, Tynghai University[3],
Taichung, Taiwan, R.O.C. (Email: ypchu@thu.edu.tw)

(Invited Paper)

Abstract

Over the past few years a number of research papers about reversible watermarks has been produced. Reversible watermarking is a novel category of watermarking schemes. It not only can strengthen the ownership of the original media but also can completely recover the original media from the watermarked media. This feature is suitable for some important media, such as medical and military images, because these kinds of media do not allow any losses. The aim of this paper is to define the purpose of reversible watermarking, reflecting recent progress, and provide some research issues for the future.

Keywords: Copyright protection, reversible watermarking, security

1 Introduction

Digital watermarking has been widely used to protect the copyright of digital images. In order to strengthen the intellectual property right of a digital image, a trademark of the owner could be selected as a watermark and embedded into the protected image. The image that embedded the watermark is called a watermarked image. Then the watermarked image could be published, and the owner can prove the ownership of a suspected image by retrieving the watermark from the watermarked image. According to the retrieved results, we can determine the ownership of the suspected image. Generally, a practical and useful watermarking scheme has to meet the following requirements [26].

1) *Robustness:*
A watermarking scheme should resist destruction from standard image processing and malicious attacks. For example, watermarked images may be compressed before transmitting or storing it. Thus, the watermarked image has to survive the legitimate usage such as lossy compressions, conversions, resamples, and other non-malicious operations. On the other hand, the watermarked image may be incurred in several of the intentional or the unintentional attacks to try to remove the embedded watermark. A robust watermarking scheme has to ensure the retrieved watermark is recognized, when the image quality does not get seriously harmed. Without robustness, an embedded watermark can be removed easily even in a legal procedure, and is unable to be proven.

2) *Imperceptibility:*
A watermark can be embedded into an image as either visible or invisible. The visible watermark is perceptible and is just like noise. It mostly can be removed by a noise removing process. In order to decrease the risk of cracking, most of the proposed watermarking schemes are invisible. On the other hand, the quality of the watermarked image is also important. If the watermark embedding process seriously affects the quality of the watermarked image, the watermarked image will draw the attention of attackers or even lose its value. Therefore, the quality between the original image and the watermarked image should not be seriously degraded. The property is called imperceptibility.

3) *Readily Embedding and Retrieving:*
The watermark must be able to be easily and securely embedded and retrieved by the owner. Therefore, the overheads of embedding process and retrieving

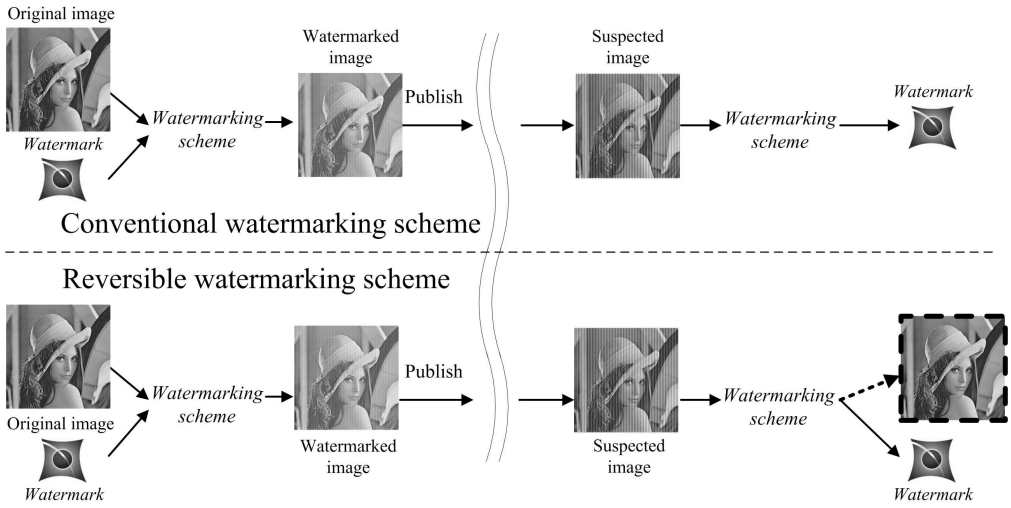


Figure 1: Flowcharts of conventional and reversible watermarking schemes

process should be limited in a reasonable range.

In recent years a special kind of digital watermarking is discussed widely, called reversible watermarking. It not only provides the protection of the copyright by embedding the assigned watermark into the original image but also can recover the original image from the suspected image. The retrieved watermark can be used to determine the ownership by comparing the retrieved watermark with the assigned one. Similar to conventional watermarking schemes, reversible watermarking schemes have to be robust against the intentional or the unintentional attacks, and should be imperceptible to avoid the attraction of attacks and value lost. Therefore, the reversible watermarking also has to satisfy all requirements of the conventional watermarking such as robustness, imperceptibility, and readily embedding and retrieving.

Except for these requirements, reversible watermarking has to grantify the following two additional requirements.

1) *Blind:*
Some of the conventional watermarking schemes require the help of an original image to retrieve the embedded watermark. However, the reversible watermarking can recover the original image from the watermarked image directly. Therefore, the reversible watermarking is blind, which means the retrieval process does not need the original image.

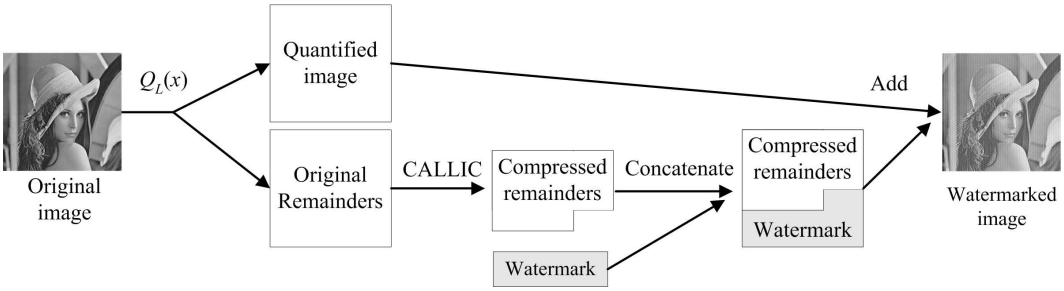
2) *Higher Embedding Capacity:*
The capable size of embedding information is defined as the embedding capacity. Due to the reversible watermarking schemes having to embed the recovery information and watermark information into the original image, the required embedding capacity of the reversible watermarking schemes is much more than the conventional watermarking schemes. The embedding capacity should not be extremely low to affect the accuracy of the retrieved watermark and the recovered image.

The procedure of conventional and reversible watermarking schemes can be illustrated by using the flowcharts in Figure 1. The steps of conventional watermarking and reversible watermarking are similar except there is an additional function to recover the original image from the suspected image. Therefore, the reversible watermarking is especially suitable for the applications that require high quality images such as medical and military images.

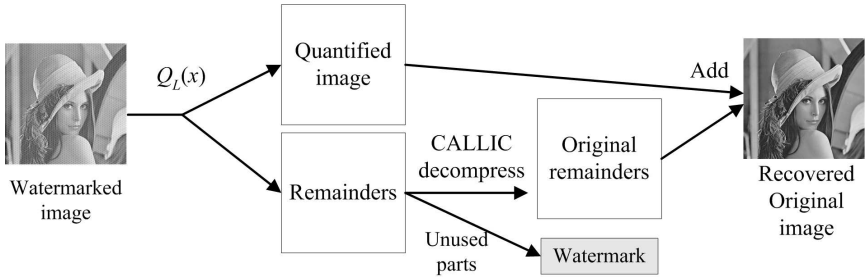
In addition, there are two research fields often connected with digital watermarking: data hiding (steganography) [9] and image authentication [7]. The purpose of data hiding is using the cover image to conceal and transmit the secret information. And the purpose of image authentication is to verify the received image whether it be tampered or not. In order to achieve the goals, the data hiding scheme should have a large embedding capacity to carry more secret information, and it has to be imperceptible to keep the secret undetectable. The image authentication schemes also require embedding some information into the protected image, and also has to keep the imperceptibility between the preprocess image and processed image.

As in the definition, the goals of the reversible watermarking are to protect the copyrights and can recover the original image. The robustness, imperceptibility, high embedding capacity, readily embedding and retrieving, and blind are the basic criterions of the reversible watermarking. A reversible data hiding scheme and a reversible image authentication scheme can be also defined as the schemes which can recover the original image from the embedded image. Schemes for digital images are focused in this paper since most of the reversible watermarking schemes are developed for digital images currently.

So far, there are several reversible watermarking schemes which have been proposed [1, 4, 8, 12, 14, 15, 16, 17, 18, 19, 23, 25, 28, 30, 34, 35, 36]. In order to introduce the current researches of reversible watermarking



(a) The embedding process



(b) The retrieving and recovering processes

Figure 2: The illustrations of Celik et al.'s lossless generalized-LSB data hiding scheme

clearly, we classify the reversible watermarking schemes into three classifications:

1) The schemes by applying data compression, such as [4, 5, 6, 10, 11, 12, 13, 14, 17, 30, 31].

2) The schemes by using difference expansion, such as [1, 2, 3, 19, 20, 21, 22, 23, 24].

3) The schemes by using histogram bin exchanging, such as [8, 18, 27, 28, 33, 34].

The detailed descriptions of the three types are introduced in Sections 2, 3, and 4, respectively. The features and comparisons are analyzed in Section 5. Some research issues are discussed in Section 6, and the conclusions are in Section 7.

2 Reversible Watermarking Schemes by Applying Data Compression

In order to recover the original image from the watermarked image, an intuitional strategy is to embed the recovery information into the original image. Except for the recovery information, we also have to embed the data of watermark into the original image. Therefore, the capacity of the embedded information is much more than the conventional watermarking schemes. In order to embed more data into the original image, a straight solution is to compress the embedding data. There are several watermarking schemes [4, 5, 6, 10, 11, 12, 13, 14, 17, 30, 31] applying data compression to reduce the size of embedding data. In this type of reversible watermarking schemes, we introduce a well-known scheme that was proposed by Celik et al. in 2005 [4]. The details of the embedding process of the scheme is described as follows.

1) Every pixel is quantified by using the following L-level scalar quantization, and the corresponding remainders are generated:

$$Q_L(x) = L \times \lfloor \tfrac{x}{L} \rfloor.$$

For example, allow the 4×4 block of original image be

$$H = \begin{pmatrix} 20 & 37 & 7 & 22 \\ 35 & 12 & 32 & 13 \\ 22 & 12 & 18 & 23 \\ 12 & 23 & 12 & 26 \end{pmatrix},$$

the watermark W be $\{10\,0010\,1011\}_2$, and the parameter $L = 5$. Then the quantified image is

$$Q = \begin{pmatrix} 20 & 35 & 5 & 20 \\ 35 & 10 & 30 & 10 \\ 20 & 10 & 15 & 20 \\ 10 & 20 & 10 & 25 \end{pmatrix},$$

and the remainders are

$$R = \begin{pmatrix} 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 3 \\ 2 & 2 & 3 & 3 \\ 2 & 3 & 2 & 1 \end{pmatrix}$$

.

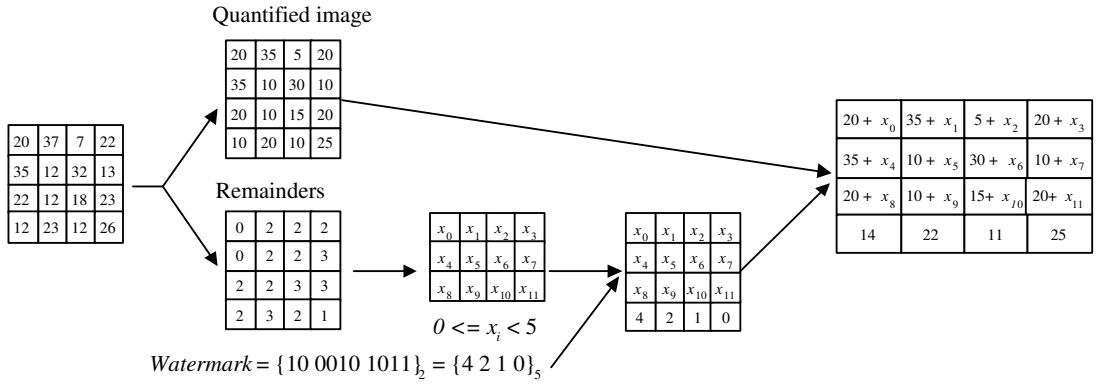


Figure 3: Example of Celik et al.'s lossless generalized-LSB data hiding scheme

2) Using adapted CALIC lossless compression algorithm [29, 32] to compress the remainders.

   Continue the former example, it is assumed that the 16 remainders are compressed to 12 digit data and denoted as $\{x_0, x_1, \ldots, x_{11}\}$. In the opposite direction, $\{x_0, x_1, \ldots, x_{11}\}$ can be decompressed to the original 16 remainders, too.

3) To concatenate the L-ary converted watermark information after the compressed remainders.

   For the same example, watermark W is converted from $\{10\ 0010\ 1011\}_2$ to $\{4\ 2\ 1\ 0\}_5$, and becomes $\{x_0, x_1, \ldots, x_{11}, 4, 2, 1, 0\}$.

4) The watermarked image is generated by adding the compressed data and the watermark to the quantified image. Finally, we gain the watermarked image

$$H' = \begin{pmatrix} 20+x_0 & 35+x_1 & 5+x_2 & 20+x_3 \\ 35+x_4 & 10+x_5 & 30+x_6 & 10+x_7 \\ 20+x_8 & 10+x_9 & 15+x_{10} & 20+x_{11} \\ 10+4 & 20+2 & 10+1 & 25+0 \end{pmatrix}$$

.

In the retrieving and recovering process, the first step of embedding process is applied again in the suspected image. The first twelve digits of the remainders can be decompressed to the 16 original remainders and the last four bits is the hidden watermark. Therefore, the watermark can be retrieved to verify the ownership and the original image can be recovered. The processes of this scheme is shown in Figure 2 and the example is shown in Figure 3.

Celik et al. also used this concept directly to propose an image authentication scheme [5] and data hiding scheme [6]. Except for Celik et al., Fridrich et al. [10, 11, 12, 13] also developed a serious of reversible schemes by applying data compression. Xuan et al. [30, 31] applied a similar concept to compress and replace the high and middle frequency data transformed by using wavelet transformation. Leest et al. [17] also proposed a similar scheme in this area.

However, the robustness of this type of reversible watermarking scheme is weak. Due to most data compression techniques which can not resist the distortions, any loss of the compressed data may crash the whole embedded data. Therefore, schemes belonging to this type lack robustness and are usually designed for data hiding or image authentication.

3 Reversible Watermarking Schemes by Using Difference Expansion

The second type of reversible schemes is using difference expansion to embed information. So far, several schemes [1, 2, 3, 19, 20, 21, 22, 23, 24] belong to this type. These schemes usually generate some small values to represent the features of the original image. Then, we expand (enlarge) the generated values to embed the bits of watermark information. The watermark information is usually embedded in the LSB parts of the expanded values. Then the watermarked image is reconstructed by using the modified values.

We introduce Tian's scheme [22] to describe the concept of this type. In Tian's scheme, an integer transformation is defined as

$$l = \lfloor \frac{(x+y)}{2} \rfloor, \tag{1}$$

where x and y are two adjacent pixels. The inverse integer transformation can be represented as

$$x' = l + \lfloor \frac{(h+1)}{2} \rfloor, \ and \tag{2}$$

$$y' = l - \lfloor \frac{h}{2} \rfloor, \tag{3}$$

where

$$h = x - y. \tag{4}$$

The processes of Tian's scheme are described as follows.

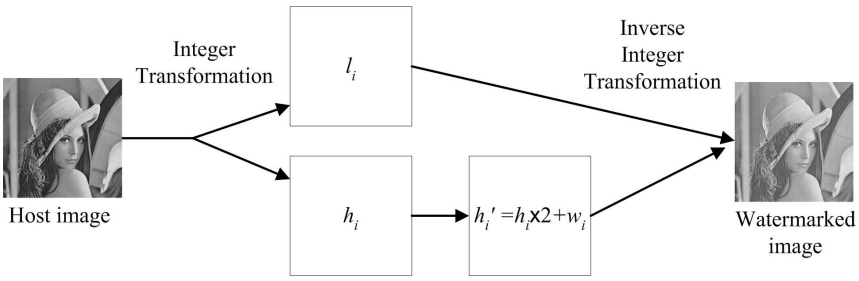


Figure 4: Flowcharts of the Tian's scheme

1) Calculating l_i and h_i for the i-th pair of pixels, denoted as $\{x_i, y_i\}$, by using Equations 1 and 4.

   For example, let x_0 and y_0 be 106 and 100. Then we have $l_0 = \lfloor \frac{(106+100)}{2} \rfloor = 103$ and $h_0 = 106 - 100 = 6$.

2) Calculating $h_i' = h_i \times 2 + w_i$, where w_i is the corresponding bit of watermark.

   Using the same example in the above. If $w_0 = \{0\}_2$, then $h_0' = 6 \times 2 + 0 = 12$. If $w_0 = \{1\}_2$, then $h_0' = 6 \times 2 + 1 = 13$.

3) The parameters l_i and h_i' are used to substitute for the parameter l_i and h_i in Equations 2 and 3 to get x_i' and y_i'.

   Continuity, if the embedded bit of watermark is 1, then $x_0' = l_0 + \lfloor \frac{(h_0'+1)}{2} \rfloor = 103 + \lfloor \frac{(13+1)}{2} \rfloor = 110$ and $y_0' = l_0 - \lfloor \frac{h_0'}{2} \rfloor = 103 - \lfloor \frac{13}{2} \rfloor = 97$. Similarly, if the embedded bit of watermark is 0, then $x_0' = l_0 + \lfloor \frac{(h_0'+1)}{2} \rfloor = 103 + \lfloor \frac{(12+1)}{2} \rfloor = 109$ and $y_0' = l_0 - \lfloor \frac{h_0'}{2} \rfloor = 103 - \lfloor \frac{12}{2} \rfloor = 97$.

4) Repeat the former steps until all pixel pairs are processed.

5) The watermarked image can be constructed by using each x_i' and y_i'.

In Tian's scheme, h represents the generated feature of the original image and it is expanded to embed information. The flowcharts of Tian's scheme is illustrated in Figure 4.

In the retrieval phase of this scheme, the corresponding pixel pairs are collected again and substituted in Equations 1 and 4. For example, suppose that $x_0' = 110$ and $y_0' = 97$, we get $l_0 = \lfloor \frac{(x_0'+y_0')}{2} \rfloor = \lfloor \frac{(110+97)}{2} \rfloor = 103$ and $h_0' = x_0' - y_0' = 110 - 97 = 13$. Extracting the least significant bit of $h_0' = 13 = \{1101\}_2$ and then we get the corresponding watermark bit $w_0 = 1$ and $h_0 = \lfloor \frac{13}{2} \rfloor = 6$. Finally the original pixels $x_0 = l_0 + \lfloor \frac{(h_0+1)}{2} \rfloor = 103 + \lfloor \frac{(6+1)}{2} \rfloor = 106$ and $y_0 = l_0 - \lfloor \frac{h_0}{2} \rfloor = 103 - \lfloor \frac{6}{2} \rfloor = 100$ are calculated from Equations 2 and 3.

However, embedding data in the expansions may cause overflow problems in this type. For example, suppose that $x = 200$ and $y = 10$, we get $l = 105$, $h = 190$, and $h' = 380$ or 381. The modified pixel value x' becomes $105 + \lfloor \frac{380}{2} \rfloor = 295$ or $105 + \lfloor \frac{381}{2} \rfloor = 295$. It is clear that the value is invalid. Therefore, a threshold to prevent the value from overflow is necessary. However, it causes another problem. For example, suppose that a threshold is 10 and $h_0 = 6$. Thus, h_0' may becomes $h_0' = 12$ or 13. In the retrieving phase, suppose that a value $h_0' = 12$ is received. There are two possible situations $h_0 = 6$ (embedded) or $h_0 = 12$ (not embedded). Therefore, we need additional information to determine whether the pair of pixels is embedded. Alattar [1] named the additional information the location map and embedded it back into the watermarked image.

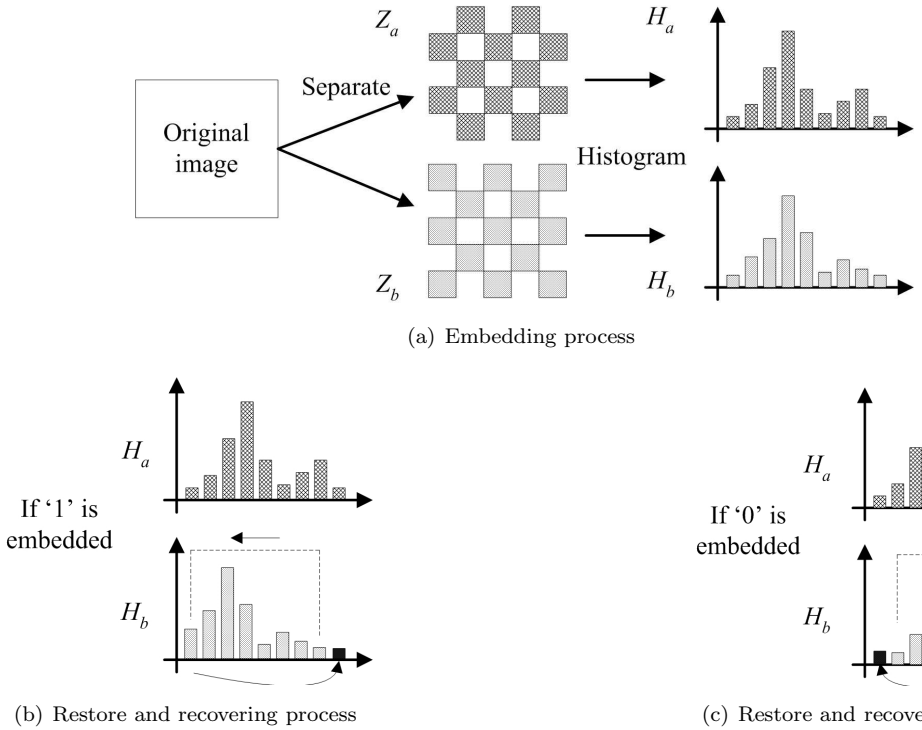
By elaborately design or location map, Alattar's scheme [1] uses different integer transformation considering all cases without exceptions. Zhang and Wang [36] directly use the integer wavelet transformation with difference expansion, and Thodi and Rodriguez [19, 20] apply the error prediction process of JPEG-LS and expand the predicted errors to embed information.

Most schemes of this type are pixel wise or block based in which loss of data doesn't affect the next one. However, the completeness of location map is destroyed, causing mismatching to all the latter pixels. Therefore, the schemes of this type are also fragile under attacks.

4 Reversible Watermarking Schemes by Using Histogram Bin Shifting

The former two types of reversible watermarking are not robust under image processing and distortions. In order to enhance the robustness of the reversible watermarking, the embedding target is replaced by the histogram of a block. There are several schemes [8, 18, 27, 28, 33, 34] belonging to this type. We introduce the Vleeschouwer et al.'s circular interpretation scheme [27] to wrok out the concept of this type. In Vleeschouwer et al.'s scheme, the original image is segmented into several blocks of the neighbor pixels, and the embedding processes are described as follows.

1) For each block B, we randomly separate B into two zones Z_a and Z_b, and calculate the two corresponding histograms of pixel values, H_a and H_b. For example,



(a) Embedding process

(b) Restore and recovering process

(c) Restore and recovering process

Figure 5: Example of Vleeschouwer et al.'s scheme

in Figure 5(a) it is assumed that an original image block is separated into two zones Z_a and Z_b and then two histograms H_a and H_b for pixel values in zones Z_a and Z_b are built, respectively.

2) If the corresponding bit of watermark is 1, we downgrade every bin in H_b except in shifting the lowest bin to the highest one. If the corresponding bit of watermark is 0, we upgrade the bins except in shifting the highest to the lowest one. The embedded results are shown in Figures 5(b) and 5(c), where the bins are shifted.

3) Repeat the former steps until all blocks are processed.

From the characteristics of the images, the neighboring pixels are usually similar to each other. Therefore, H_a and H_b should also be similar for most of the image blocks. In normal cases, it is assumed that the peak bin of Z_a and Z_b are the same.

In cases in which the highest and lowest bins are shifted to the other side may cause a huge distortion. For example, the white background may become black. Therefore, Vleeschouwer et al. [28] proposed an improved version of circular reversible watermarking scheme by using the bijective transformations shown in Figure 6. The improved bijective transformation shifts two bin regions at most and avoid the extreme distortion.

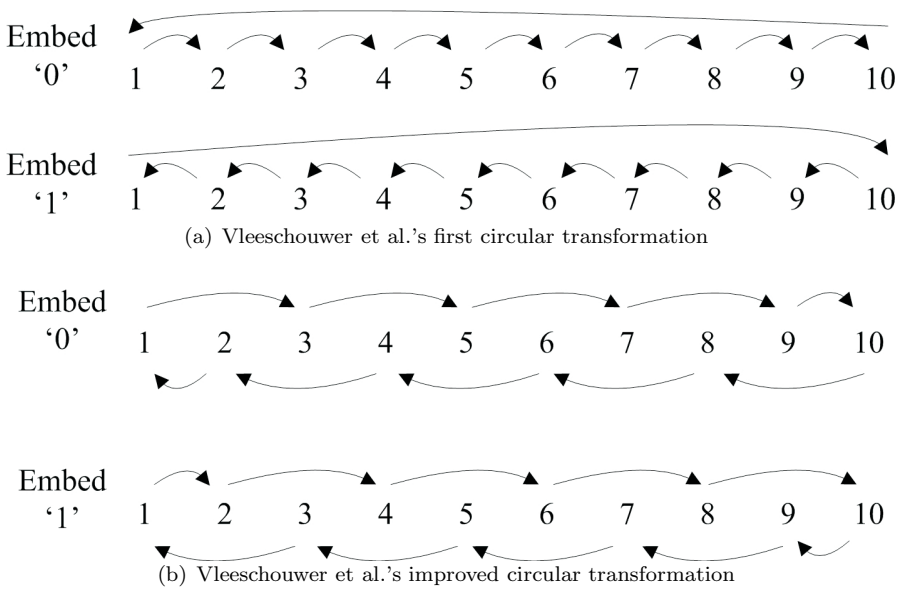
Some schemes [18, 30, 31] developed another histogram technique that embed information only in the peak bin pixels. Although these schemes need additional side information to retrieve the watermark and recover the original image, they provide a higher quality of the watermarked image. Yang et al. [33, 34] also proposed another histogram expansion model to increase the embedding capacity. Chang et al. [8] applied a similar idea to propose a reversible scheme for VQ compressed images.

Generally, most schemes in this type are block-based embedding and thus they have the ability to resist some attacks. The embedding capacity in this type is lower but the robustness is the major advantage of this type.

5 Discussions

In this section, we discuss the properties of the three types of reversible watermarking schemes. Usually, higher embedding capacity usually comes along with a higher distortion. Therefore, based on the watermarked images with the similar image quality, we compare the embedding capacity with the three types by using the three standard test images, "F-16", "Mandrill", and "Lena", as shown in Figure 7. The PSNR (Peaks of the Signal-to-Noise Ratio) is a popular index term to evaluate the difference between the pre-processing image and the post-processing image. A larger value of PSNR means that the watermarked image has a better quality, the difference between the original image and the watermarked image is imperceptible.

For a similar quality of watermarked images, the embedding capacity of the first type directly depends on the compression rate. The best experimental result of this type appears in Celik et al.'s scheme [4] of which the highest embedding capacity is 13% for F-16 image and



(a) Vleeschouwer et al.'s first circular transformation

(b) Vleeschouwer et al.'s improved circular transformation

Figure 6: Vleeschouwer et al.'s circular transformations

the lowest embedding capacity is 2.2% for Mandrill image with PSNR = 31.9 dB.

The embedding capacity of second type depends on the expanded data and the techniques of recording the location map. In Alattar's scheme [1], the capacity is 27% (2.17 bpp) for Lena image with PSNR = 31.78 dB and is 12% (0.98 bpp) for Mandrill image with PSNR = 30.19 dB. We found that the embedding capacity is relatively higher than the other types.

Due to the block-based properties, the embedding capacity of the third type is much lower than the other types. Except Yang et al.'s schemes [33, 34] reached about 4% for a sharpened Mandrill image with the PSNR value about 30 dB, other schemes in this type are almost lower than 1%.

The major operation of the first type is data compression. Thus, the complexity of the first type depends on the data compression techniques. In the second and the third types, there is no such complicated operation. Therefore, the complexity of the second type and the third type are relatively lower than the first.

As mentioned in Section 2, most compressed data can be decompressed only from complete data. Therefore, the schemes in the first type have to apply the additional techniques like spread-spectrum, error-correction, or other methods to enhance robustness. Unfortunately, these techniques will decrease the embedding capacity in the first type. Therefore, this additional technique must be worth the sacrifice, and the schemes are not robust against image processes and attacks.

Although a partial distortion will not affect undamaged regions in the schemes of the second type, the location map must correctly indicate the embedding cases. Any loss of the location map will mess up the latter verifications. Therefore, the situation is similar to the former one, and the second type is not robust.

The schemes in the third type only need to recognize the correct bins for the watermarked pixels. For this reason, the retrieved results are still correct with a slight distortion that doesn't force the pixel away from the original bin.

From the above discussions, we found that the schemes in the first and second types do not provide any robustness. Only the schemes in the third type meets the requirement of robustness, and it can completely achieve the requirements of the reversible watermarking.

6 Research Issues

It is clear from the comparisons in Section 5 that the embedding capacity and the robustness are the two major challenges of reversible watermarking. Furthermore, many of the conventional watermarking schemes are embedding watermarks in frequency domains. In general, the advantages of embedding watermarks in frequency domains are naturally resisting some attacks, immuned to several destruction, or others. But the existing reversible watermarking schemes did not fully utilize the advantages. Therefore, we provide the following three research issues.

1) Providing a higher embedding capacity.
   Although capacity is indeed not the necessary requirement of watermarking schemes, but higher capacity is one of the ultimate goals. There's still room for reversible watermarking schemes to improve this terminology.

2) Providing a higher robustness.
   The reversible watermarking schemes using histogram bin shifting can resist several attacks, but

(a) F-16 (b) Mandrill (c) Lena

Figure 7: Three standard test images

the requirements for realistic applications are strict with more challenges.

3) Use the advantage of frequency domains.
We thought it could be an opportunity to raise the practicability by this direction.

7 Conclusions

In this paper, the reversible watermarking schemes are defined and introduced. In order to work out the features of reversible watermarking schemes, we particularly classified the existing reversible watermarking schemes into three types. They are the schemes which apply data compression, by using difference expansion, and the schemes by using histogram bin shifting. The three types are analyzed and compared to introduce the current status of reversible watermarks.

In the schemes by applying data compression, a proper design of compression method is important. The existing schemes belong to this type lacking robustness because the applied compression methods can not resist the distortions. The formula to produce the difference and the techniques to handle location map are still under development in reversible watermarking schemes by using difference expansion. The schemes belong to this type are also weak in robustness because the destroyed location map will cause mismatching. The type of histogram bin shifting is different from the previous two types with robustness. Reversible watermarking schemes are still in development and have dramatically potential possibilities. From this paper, we hope to provide an overall introduction of reversible watermarking, and give a proper cause to commence the research in this fascinating area.

References

[1] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Transactions on Image Processing*, vol. 13, no. 8, pp. 1147–1156, Aug. 2004.

[2] A. M. Alattar, "Reversible watermark using difference expansion of quads," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 3, pp. 377–80, Montreal, Canada, May 2004.

[3] A. M. Alattar, "Reversible watermark using difference expansion of triplets," in *Proceedings of the IEEE International Conference on Image Processing*, vol. 1, pp. 501–504, Catalonia, Spain, Sept. 2003.

[4] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-lsb data embedding," *IEEE Transactions on Image Processing*, vol. 14, no. 2, pp. 253–266, Feb. 2005.

[5] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Localized lossless authentication watermark (LAW)," in *International Society for Optical Engineering*, vol. 5020, pp. 689–698, California, USA, Jan. 2003.

[6] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding," in *Proceedings of the International Conference on Image Processing*, pp. 157–160, NY, USA, Sept. 2002.

[7] C. C. Chang and I. C. Lin, "Remarks on fingerprint-based remote user authentication scheme using smart cards," *ACM Operating Systems Review*, vol. 38, no. 3, pp. 91–100, Oct. 2004.

[8] C. C. Chang, W. L. Tai, and M. H. Lin, "A reversible data hiding scheme with modified side match vector quantization," in *Proceedings of the International Conference on Advanced Information Networking and Applications*, vol. 1, pp. 947–952, Taiwan, Mar. 2005.

Table 1: Comparisons between the three types of reversible schemes

	Data compression	Difference expansion	Histogram bin shifting
Schemes	Celik et al. [4]	Alattar' [1]	Yang et al. [34]
Best embedding capacity	13 %	27 %	4 %
Complexity	Depend on compression	low (multiple and addition)	low (accumulate and addition)
Robustness	No	No	Moderately

[9] J. B. Feng, H. C. Wu, C. S. Tsai, and Y. P. Chu, "A new multi-secret images sharing scheme using largrange's interpolation," *Journal of Systems and Software*, vol. 76, no. 3, pp. 327–339, June 2005.

[10] J. Fridrich, J. Goljan, and R. Du, "Invertible authentication," in *SPIE Proceedings of Security and Watermarking of Multimedia Content*, pp. 197–208, San Jose, Jan. 2002.

[11] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in *SPIE Proceedings of Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents*, vol. 4675, pp. 572–583, San Jose, Jan. 2002.

[12] J. Fridrich, M. Goljan, Q. Chen, and V. Pathak, "Lossless data embedding with file size preservation," in *SPIE Proceedings of EI*, San Jose, Jan. 2004.

[13] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding-new paradigm in digital watermarking," *EURASIP Journal of Signal Processing*, vol. 2002, no. 2, pp. 185–196, Feb. 2002.

[14] M. Goljan, J. Fridrich, and R. Du, "Distortion-free data embedding," in *Proceedings of 4th Information Hiding Workshop*, vol. 2137, pp. 27–41, Pittsburgh, PA, Apr. 2001.

[15] C. W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data," *US Patent*, vol. 6,278,791, 2001.

[16] T. Kalker and F. M. Willems, "Capacity bounds and code constructions for reversible data-hiding," in *Proceedings of Electronic Imaging 2003, Security and Watermarking of Multimedia Contents V*, pp. 604–611, California, USA, Jan. 2003.

[17] A. Leest, M. Veen, and F. Bruekers, "Reversible image watermarking," in *Proceedings of the ICIP International Conference on Image Processing*, vol. 3, pp. II-731-4, Barcelona, Spain, Sep. 2003.

[18] Z. Ni, Y. Q. Shi, N. Ansari, and S. Wei, "Reversible data hiding," in *ISCAS Proceedings of the 2003 International Symposium on Circuits and Systems*, vol. 2, pp. II–912–II–915, Thailand, May 2003.

[19] D. M. Thodi and J. J. Rodriguez, "Reversible watermarking by prediction-error expansion," in *Proceedings of the 6th IEEE Southwest Symposium on Image Analysis and Interpretation*, vol. 3, pp. 21–25, Lake Tahoe, USA, Mar. 2004.

[20] D. M. Thodi and J. J. Rodriguez, "Prediction-error based reversible watermarking," in *Proceedings of the ICIP International Conference on Image Processing*, vol. 3, pp. 1549–1552, Genova, Oct. 2004.

[21] J. Tian, "High capacity reversible data embedding and content authentication," in *IEEE Proceedings of International Conference on Acoustics, Speech, and Signal Processing*, vol. 3, pp. III–517–20, Hong Kong, Apr. 2003.

[22] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits Systems and Video Technology*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[23] J. Tian, "Wavelet-based reversible watermarking for authentication," in *Proceedings of SPIE Sec. and Watermarking of Multimedia Cont. IV*, vol. 4675, Jan. 2002.

[24] J. Tian and R. O. Wells, "Reversible data-embedding with a hierarchical structure," in *Proceedings of the ICIP International Conference on Image Processing*, vol. 5, pp. 3419–3422, Genova, Oct. 2004.

[25] C. L. Tsai, K. C. Fan, C. D. Chung, and T. C. Chung, "Reversible and lossless data hiding with application in digital library," in *Proceedings of the 38th Annual International Carnahan Conference on Security Technology*, pp. 226–232, Albuquerque, USA, Oct. 2004.

[26] C. S. Tsai and C. C. Chang, "A repeating color watermarking scheme based on human visual model," *Eurasip Journal on Applied Signal Processing*, vol. 13, pp. 1965–1972, 2004.

[27] C. D. Vleeschouwer, J. E. Delaigle, and B. Macq, "Circular interpretation of histogram for reversible watermarking," in *Proceedings of the IEEE 4th Workshop on Multimedia Signal Processing*, pp. 345–350, France, Oct. 2001.

[28] C. D. Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," *IEEE Transactions on Multimedia*, vol. 5, no. 1, pp. 97–105, Mar. 2003.

[29] X. Wu, "Lossless compression of continuous-tone images via context selection, quantization, and modeling," *IEEE Transactions on Image Processing*, vol. 6, no. 5, pp. 656–664, May. 1997.

[30] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni, "Reversible data hiding based on wavelet spread spectrum," in *Proceedings of the IEEE 6th Workshop on Multimedia Signal Processing*, pp. 211–214, Italy, Sept. 2004.

[31] G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, and W. Su, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," *IEE Electronics Letters*, vol. 38, no. 25, pp. 1646–1648, Dec. 2002.

[32] X. Wu and N. Memon, "Context-based, adaptive, lossless image codec," *IEEE Transactions on Communications*, vol. 45, no. 4, pp. 437–444, Apr. 1997.

[33] B. Yang, M. Schmucker, C. Busch, X. Niu, and S. Sun, "Approaching optimal value expansion for reversible watermarking," in *Proceedings of the 7th Workshops on Multimedia and Security*, pp. 95–102, USA, Sept. 2004.

[34] B. Yang, M. Schmucker, X. Niu, C. Busch, and S. Sun, "Reversible image watermarking by histogram modification for integer dct coefficients," in *Proceedingd of the IEEE 6th Workshop on Multimedia Signal Processing*, pp. 143–146, Siena, Italy, Sept. 2004.

[35] J. M. Zain, L. P. Baldwin, and M. Clarke, "Reversible watermarking for authentication of dicom images," in *Proceedings of the 26th Annual International Conference of the Engineering in Medicine and Biology Society*, pp. 3237–3240, USA, 2004.

[36] L. B. Zhang and K. Wang, "Embedded multiple subbands scaling image coding using reversible integer wavelet transforms," in *Proceedings of the International Symposium on Intelligent Multimedia, Video and Speech Processing*, pp. 599–602, Hong Kong, Oct. 2004.

Jen-Bang Feng received the M.S. degree in Department of Applied Mathematics from National Chung Hsing University, Taichung, Taiwan, in 2003. He is currently pursuing his Ph.D. degree in Institute of Computer Science from Nation Chung Hsing University, Taichung, Taiwan. His current research interests includes data hiding, watermarking, and secret sharing.

Iuon-Chang Lin received the B.S. in Computer and Information Sciences from Tung Hai University, Taichung, Taiwan, Republic of China, in 1998; the M.S. in Information Management from Chaoyang University of Technology, Taiwan, in 2000. He received his Ph.D. in Computer Science and Information Engineering in March 2004 from National Chung Cheng University, Chiayi, Taiwan. He is currently an assistant professor of the Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan, ROC. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

Chwei-Shyong Tsai was born in Changhua, Taiwan, Republic of China, on September 3rd, 1962. He received his B.Sc. degree in Applied Mathematics in 1984 from National Chung Hsing University, Taichung, Taiwan. He received his M.Sc. degree in Computer Science and Electronic Engineering in 1986 from National Central University, Chungli, Taiwan. Consequently, he received his Ph.D. degree in Computer Science and Information Engineering in 2002 from National Chung Cheng University, Chiayi, Taiwan. On August 2002, he received his tenure as associate professor of the Department of Information Management at National Taichung Institute of Technology, Taichung, Taiwan. Since August 2004, he is an associate professor of the Department of Management Information Systems at National Chung Hsing University, Taichung, Taiwan. His research interests include image watermarking, image authentication, information hiding, bio-information and E-learning.

Yen-Ping Chu is a Professor in the Computer Science and Information Engineering and the library director at Tung Hai University, Taichung, Taiwan. His research interests include high-speed networks, operating system, neural network, and computer assistant learning.