ISSN 2047-3338

# Reversible Watermarking: A Complete Review

Navnath Narawade[1] and Dr. Rajendra Kanphade[2]

[1]Electronics Engg. Department, Sant Gadgebaba Amravati University, Amravati, Maharashtra, India
[2]Department of E&TC Engg., Dhole Patil College of Engg., Wagholi, Pune, Maharashtra, India

*Abstract*– **For some critical applications such as the law enforcement, medical and military image system, it is crucial to restore the original image without any distortions. The watermarking techniques satisfying those requirements are referred to as 'reversible watermarking'. Reversible watermarking is designed so that it can be removed to completely restore the original image. Considering the age of reversible watermarking which is just a decade to count, it has fetched enormous attention of researchers to boost of. Due to many researches in this field, it has become very difficult to judge an algorithm for a specific application. So a definite need arises to compare these algorithms on some criteria. In this paper, we present a comprehensive study of all basic algorithms which are reversible.**

***Index Terms*– Reversible Watermarking, Compression, Difference Expansion, Histogram Bin Shifting, Contrast Mapping, DWT, DCT PSNR, Embedding Capacity and Processing Time**

## 1. INTRODUCTION

THE concept of reversible watermark firstly appeared in the patent owned by Eastman Kodak [1]. Honsinger et al. [1] utilised a robust spatial additive watermark combined with modulo additions to achieve reversible data embedding. Goljan et al. [2] proposed a two cycles flipping permutation to assign a watermarking bit in each pixel group. Celik et al. [3] presented a high capacity, reversible data-embedding algorithm with low distortion by compressing quantisation residues. Tian [4] presented a reversible data embedding approach based on expanding the pixel value difference between neighbouring pixels, which will not overflow or underflow after expansion. Thodi and Rodrguez exploited the inherent correlation among the neighbouring pixels in an image region using a predictor. Xuan et al. [5] embedded data into high-frequency coefficients of integer wavelet transforms with the companding technique, and utilised histogram modification as a preprocessing step to prevent overflow or underflow caused by the modification of wavelet coefficients.

The earliest reference to reversible data embedding we could find is the Barton patent [8], filed in 1994. In his invention, the bits to be overlayed will be compressed and added to the bitstring, which will be embedded into the data block. Honsinger et al. [9], reconstruct the payload from an embedded image, then subtract the payload from the embedded image to losslessly recover the original image. Macq [10] proposes an extension to the patchwork algorithm to achieve reversible data embedding. Fridrich et al. [1], develop a high capacity reversible data-embedding technique based on embedding message on bits in the status of group of pixels. They also describe two reversible data-embedding techniques for lossy image format JPEG. De Vleeschouwer et al. [11], propose a reversible data-embedding algorithm by circular interpretation of bijective transformations. Kalker et al. [12], provide some theoretical capacity limits of lossless data compression based reversible data embedding [6] and give a practical code construction. Celik et al. [13], [14], present a high capacity, low distortion reversible data-embedding algorithm by compressing quantization residues. They employ the lossless image compression algorithm CALIC, with quantized values as side-information, to efficiently compress quantization residues to obtain high embedding capacity.

Reversible watermarking has found a huge surge of experimentation in its domain in past decade as the need of recovering the original work image after extracting the watermark arises in various applications such as the law enforcement, medical and military image system, it is crucial to restore the original image without any distortions [7]. In traditional watermarking techniques, our main concern is to embed and recover the watermark with minimum loss. The quality of original work image we get after extraction is highly degraded and not restorable. But in applications like law enforcement, medical and military, in which superior quality of image is needed, we cannot use these algorithms. In medical images, some prerequisite information about the patient is watermarked in it while transmitting and at reception we need to have both, the original image and that information to be recovered lossless. This type of result is achievable by making use of any reversible watermarking algorithm out of a pool of algorithms [10].

The last 10 years has seen considerable interest in Reversible Watermarking. Our attempt here is to study all basic algorithms and applications of reversible watermarking.

For reversible watermarking we compare all techniques based upon the embedding capacity, PSNR and processing time. In this paper, we consider the following points: a) Interest and commercial applications, b) Methods, c) The scientific progress made in the last 10 years, d) The most exciting areas for research, and e) The next 10 years of reversible watermarking.

In our opinion, the interest in reversible watermarking is appropriate. However, we expect that military applications will be overshadowed by applications such as medical application and law enforcement application. These latter applications may turn out to be the most compelling. Considerable progress has been made toward enabling these applications. Further progress is needed in methods for handling geometric and temporal distortions. We expect other exciting developments to arise from research in reversible watermarking. A reversible watermark will drive the next generation era.

## II. SOME IMPORTANT DEFINITIONS

Basically there are four types of watermarking:

*1) Text Watermarking:* Text can be added into image is called text watermarking [16].

*2) Image Watermarking:* Image can be added into an original image is called image watermarking [17].

*3) Audio Watermarking:* Some audio signals are added into audio clip is called audio watermarking [21].

*4) Video Watermarking:* Some video clips are added into video is called video watermarking [18].

In other way, the digital watermarks can be divided into three different types according to perceptibility of watermark are as follows:

*1) Visible watermark:* A watermark which is quite visible is called a visible watermark [19].

*2) Invisible-Robust watermark:* This watermark which is invisible but robust in nature [19].

*3) Invisible-Fragile watermark:* This watermark is invisible and not robust to noise [19].

Again a digital watermark can be divided into two broad categories according to the necessary data for extraction:

*1) Informed (or private Watermarking):* In which the original un-watermarked cover is required to perform the extraction process [20].

*2) Blind (or public Watermarking):* In which the original un-watermarked cover is not required to perform the extraction process [20].

Based on following properties overall efficiency of a watermarking technique can be judged.

- *Effectiveness:* It is the probability of detection of a watermark immediately after embedding.
- *Fidelity:* Perceptual similarity between the original and the watermarked versions of the cover work.
- *Data Payload:* No. of bits a watermark encodes within a unit of time or within a work.
- *Robustness:* Ability to detect the watermark after common signal processing operations.
- *Security:* The embedded information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector (except a secret key), and the knowledge of at least one carrier with hidden message.

Watermarking and Reversible watermarking requirements based upon attacks viz. Low pass filtering attack, Geometric attack, Forgery attack, VQ attack, Cropping attack are as follows: *1) Security, 2) Imperceptibility, 3) Capacity, and 4) Robustness* [22].

The noises which we can be applied are Cropping, Gaussian, Poisson, Salt and Pepper, Rotational, geometric and Multiplicative noise [22].

The performance of a reversible data-embedding algorithm can be measured by the following [4]:

1) *Payload capacity limit:* It is the maximum amount of information that can be embedded.

2) *Visual quality:* It is the visual quality after the embedding of image.

3) *Complexity:* It is the complexity of mathematical equations and hence the algorithm.

## III. TECHNIQUES OF REVERSIBLE WATERMARKING

There are five basic techniques of reversible watermarking; we are studying here i) Difference Expansion, ii) Histogram bin Shifting, iii) Data hiding using Integer Wavelet Transform, iv) Contrast Mapping, and v) Integer Discrete Cosine Transform.

### *A) Difference Expansion*

This scheme usually generates 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.

The algorithm's steps are:

1. Take two adjacent pixel values of x and *y*

2. Find difference and average values of pixels

3. Then we expand into its binary form and add watermark bit right after most significant bit to get

4. Reconstruct the image using and *d'*, we get the watermarked image

The similar process is required to be followed for the lossless recovery of the Original Image and the watermark [4].

### *B) 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. We introduce the Ni et al.'s scheme to work out the concept of this type.

The algorithm steps are:

1. Scan the cover image and construct its histogram

2. The gray value for which the histogram is highest is denoted the peak point a, and the gray value for which the histogram is lowest is denoted by the minimum point b

3. If Hi(b)=0, then b is called a zero point. For simplicity, we assume a<b

4. Scan the image and record the positions of those pixel values to b and place them into the location map L

5. Shift the histogram Hi(x), x ϵ (a, b) to the right to vacate the histogram bin at a+1

6. Extract a data bit s from secret data S. Scan the image once more

7. If the scanned pixel value is a and the data bit to be embedded is 1, then set the pixel value to a+1

8. If the data bit to be embedded is 0, no change has to be done on the scanned pixel [3]

The similar process is required to be followed for the lossless recovery of the Original Image and the watermark.

### *C) Distortion less data Hiding Algorithm Based On Integer Wavelet Transform*

This is a distortion less image data hiding algorithm based on integer wavelet transform that can invert the stego-image into the original image without any distortion after the hidden data are extracted. This algorithm hides data into one (or more) middle bit-plane(s) of the integer wavelet transform coefficients in the middle and high frequency sub bands. It can embed much more data and also satisfy the imperceptibility requirement. The embedding process for the algorithm is as described below:

1. Read the Original Image

2. Perform Integer Wavelet Transform of the Original Image

3. Construct binary Images from the 5th bit of CH, CV and CD

4. Compress the data in the 5th bit plane of CH, CV and CD by arithmetic encoding

5. Read the watermark and reshape it for insertion

6. Find the length of all the bit planes and the watermark to form the header

7. Insert the header, compressed data and watermark into the Image

8. Perform Inverse Integer Wavelet Transform to get the Watermarked Image [4]

The similar process is required to be followed for the lossless recovery of the Original Image and the watermark [5], [7].

### *D) Contrast Mapping*

In this letter, we discuss a spatial domain reversible watermarking scheme that achieves high-capacity data embedding without any additional data compression stage. The scheme is based on the reversible contrast mapping (RCM), a simple integer transform defined on pairs of pixels. RCM is perfectly invertible, even if the least significant bits (LSBs) of the transformed pixels are lost. The data space occupied by the LSBs is suitable for data hiding. The basic RCM watermarking scheme was introduced in [5]. Here, a modified version that allows robustness against cropping is proposed. The control of distortions introduced by the watermarking is investigated as well. The mathematical complexity of the RCM watermarking is further analyzed, and a very low cost implementation is proposed. Finally, the RCM scheme is compared with Tian's difference expansion scheme [3] with respect to the bit-rate hiding capacity and to the mathematical complexity. It is shown that the RCM scheme provides almost similar embedding bit-rates when compared to the difference expansion approach, but it has a considerably lower mathematical complexity [15].

- *Marking:* The marking proceeds as follows:

1) Partition the entire image into pairs of pixels (for instance, on rows, on columns, or on any space filling curve)

2) For each pair

a) If and if it is not composed of odd pixel values, transform the pair using the (1), set the LSB of to "1," and consider the LSB of as available for data embedding

b) If and if it is composed of odd pixel values, set the LSB of to "0," and consider the LSB of as available for data embedding

c) If , set the LSB of to "0," and save the true value

3) Mark the image by simple overwriting the bits of the watermark

A different marking procedure is proposed in [5]. A map of transformed pairs and the sequence of LSBs for all non transformed pairs are first collected. Then, the entire image LSB plane is overwritten by the payload and by the collected bit sequences. The slightly modified procedure proposed in this letter provides robustness against cropping. The location map of the entire image is replaced by the LSB of the first pixel of each pair showing if the pair was transformed or not. Let us further consider that the saved LSB of a non transformed pair is embedded into the available LSB of the closest transformed pair. Thus, all the information needed to recover any original pixel pair is embedded into the pair itself or very close to it. In the case of cropping, except for the borders where some errors may appear, the original pixels of the cropped image are exactly recovered together with the embedded payload. For pixel pairing on row or column direction, there are no problems of synchronization.

Some control codes should be inserted in the payload to validate watermark integrity.

- *Detection and Original Recovery:* Watermark extraction and exact recovery of the original image is performed as follows:

1) Partition the entire image into pairs of pixels

2) For each pair

a) If the LSB is "1," extract the LSB of and store it into the detected watermark sequence, set the LSBs of, to "0," and recover the original pair by inverse transform (3)

b) If the LSB of is "0" and the pair with the LSBs set to "1" belongs to , extract the LSB of , store it into the detected watermark sequence, and restore the original pair as with the LSBs set to "1"

c) If the LSB of is "0" and the pair with the LSBs set to "1" does not belong to, the original pair is recovered by replacing the LSB of with the corresponding true value extracted from the watermark sequence

### *E) Integer Discrete Cosine Transform*

The classic and still most popular domain for image processing is that of the Discrete-Cosine-Transform, or DCT. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they have minimize they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies).

The discrete cosine transform of x is shown in equation (2) below:

$$X_k = \sum_{n=0}^{N-1} x_n \cos\left[\Omega\,(n+1/2)\,k/N\right] \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ (1)$$

$$k = 0, 1, 2 \ldots\ldots\ldots\ldots N-1$$

One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. To begin, we define the middle-band frequencies (Fm) of an 8x8 DCT block as shown below.

$F_L$ is used to denote the lowest frequency components of the block, while $F_H$ is used to denote the higher frequency components. $F_M$ is chosen as the embedding region as to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image.

Another possible technique is to embed a PN sequence W into the middle frequencies of the DCT block. We can modulate a given DCT block x,y using the equation shown below.

$$\begin{aligned} Iw_{x,y}(u,v) &= I_{x,y}(u,v) + k*W_{x,y}(u,v) \qquad u,v\text{€}Fm \\ &= I_{x,y}(u,v) \qquad u,v\text{€}Fm \end{aligned} \quad \ldots\ldots\ldots\ldots\ldots\ (2)$$

For detection, the image is broken up into those same 8x8 blocks, and a DCT performed. The same PN sequence is then compared to the middle frequency values of the transformed block. If the correlation between the sequences exceeds some threshold T, a "1" is detected for that block; otherwise a "0" is detected. Again k denotes the strength of the watermarking, where increasing k increases the robustness of the watermark at the expense of quality [23].

## IV. COMMERTIAL APPLICATIONS

*Authentication:* A digital signature can be embedded as a watermark in a Work. An advantage of this arrangement is for legacy systems. There has been concern because embedding a signature alters the work [10].

*Military Application:* Many images used to target certain location (longitude and latitude of target is embedded) should be reversible. In this case watermark is just to authenticate the target.

*Medical Applications:* Many medical images that need to send to a doctor should be embedded with history of patient. This history of patient may be in text format. Here original image should be completely reversible to take a decision by a doctor.

## V. CONCLUSION AND FUTURE SCOPE

In this paper we have surveyed the current literatures on reversible watermarking which is a recent hot topic of research. We have also classified reversible watermarking algorithms. Due to the space limitations we couldn't cover enough technical details but we have tried to be as clearer as possible.

We have discussed all the above techniques based on PSNR and Embedding Capacity, both, because if we increase the embedding capacity the PSNR gets reduced and vice versa. So we have to maintain an optimum balance between them to get a satisfactory result. A good technique should have PSNR as well as high Embedding Capacity.

Handling of geometric distortion remains a difficult task. More robust system will also significantly lead the area. Secure reversible watermarking with any attack may be a dream and a challenging field in near future.

## REFERENCES

[1]. Honsinger, C.W., Jones, P., Rabbani, M., and Stoffel, J.C.: 'Lossless recovery of an original image containing embedded data'. US patent no. 6278791, 2001

[2]. Goljan, M., Fridrich, J., and Du, R.: 'Distortion-free data embedding for images'. 4th Information Hiding Workshop, LNCS, vol. 2137, (Springer-Verlag, New York, 2001, pp. 27–41.

[3]. Celik, M.U., Sharma, G., Tekalp, A.M., and Saber, E.: 'Reversible data hiding'. Proc. ICIP, 2002, vol. 2, pp. 157–160

[4]. Tian, J.: 'Reversible data embedding using a difference expansion', IEEE Trans. Circuits Syst. Video Technol., 2003, 13, (8), pp. 890–896.

[5]. Xuan, G.R., Yang, C.Y., Zhen, Y.Z., and Shi, Y.Q.: 'Reversible data hiding using integer wavelet transform and companding technique'.Proc. IWDW, 2004

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

[7]. J. Tian, "Wavelet-based reversible watermarking for authentication," in *Security and Watermarking of Multimedia Contents IV—Proc. SPIE*, E. J. Delp III and P. W. Wong, Eds., Jan. 2002, vol. 4675, pp. 679–690.

[8]. J. M. Barton, "Method and Apparatus for Embedding Authentication Information Within Digital Data," U.S. Patent 5 646 997, 1997.

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

[10]. B. Macq, "Lossless multiresolution transform for image authenticating watermarking," in *Proc. EUSIPCO*, Sept. 2000, pp. 533–536.

[11]. C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless

watermarking for media asset management," *IEEE Tran. Multimedia*, vol. 5, pp. 97–105, March 2003.

[12]. T. Kalker and F. M. J. Willems, "Capacity bounds and constructions for reversible data hiding," in *Proc. 14th Int. Conf. Digital Signal Processing*, vol. 1, July 2002, pp. 71–76.

[13]. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding," in *Proc. Int. Conf. Image Processing*, vol. II, Sept. 2002, pp.157–160.

[14]. "Lossless generalized-LSB data embedding," *IEEE Trans. Image Processing*, submitted for publication.

[15]. D. Coltuc and J. M. Chassery, "Very fast watermarking by reversible contrast mapping," *IEEE Signal Process. Lett.*, vol. 14, no. 4, pp. 255–258, Apr. 2007.

[16]. S.W. Weng, Y. Zhao and J.-S. "Pan Reversible watermarking resistant to cropping attack", IET Inf. Secur., 2007, 1, (2), pp. 91–95

[17]. C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation on histogram for reversible watermarking," in *IEEE Int. Multimedia Signal Process. Workshop*, France, Oct. 2001, pp. 345–350.

[18]. G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, and W. Su, "Distortionless data hiding based on integer wavelet transform," in *Proc. IEEE Int. Workshop Multimedia Signal Process.*, St. Thomas, U.S. Virgin Islands, Dec. 2002, vol. 38, no. 25, pp. 1646–1648.

[19]. Craver, S.; Memon, N.; Boon-Lock Yeo; Yeung, M.M.; "On the invertibility of invisible watermarking techniques," Proceedings of International Conference on Image Processing, Oct 1997, Volume: 1Pages: 540 -543.

[20]. Juan R. Hern´andez, Fernando P´erez-Gonz´alez, Jos´e ManuelRodrıguez, and GustavoNietoA, "Performance Analysis of a 2-D-Multipulse Amplitude Modulation Scheme for Data Hiding and Watermarking of Still Images", IEEE transaction, MAY 1998.

[21]. Aweke NegashLemma,JavierAprea,WernerOomen,and Leon van de Kerkhof, "A Temporal Domain Audio Watermarking Technique", IEEE transaction,APRIL 2003.

[22]. Xiangyang Wang, Jun Wu, and Panpan Niu, "A New Digital Image Watermarking Algorithm Resilient to Desynchronization Attacks", IEEE transaction,DEC 2007.

[23]. Mandeep Kaur, Gurinderbir Kaur Sidhu, "Effect of quantization on robustness of DCT digital watermarking techniques", International Conference on Information and Multimedia Technology, 2009.