Evaluation of Lossless Watermarking Techniques

Dr.Smitha Rao M.S
Reva Institute of Technology and Management
Bangalore, India

***Abstract*—One of the mechanisms to deter unauthorized copy and distribution of digital media is Digital Watermarking. Digital watermarking involves embedding of identifying information into the digital content which can be later recovered for verification and authentication. In conventional watermarking schemes certain amount of distortion to the recovered image is acceptable. This does not apply to all applications, particularly in military applications, space and medical imagery etc., loss of a single bit of information from the original image is not acceptable. Reversible watermarking is a novel category of watermarking schemes that can not only strengthen the ownership of the original media but also can completely recover the original media from the watermarked media. In reversible watermarking, the embedding process has an additional burden of embedding extra information in the payload that includes the recovery data that is used by the decoder to reconstruct the original image bit by bit. Thus the payload consists of the authentication information and recovery data. Reversible watermarking is especially suitable for the applications that require high quality images like for certain applications of digital media such as for legal evidence, digital commerce, security surveillance etc. any modification/tampering done to media has to be detected. Various lossless watermarking schemes are discussed in this paper.**

Keywords*—Reversible Coding, PSNR, Histogram modification, Difference Expansion, DWT, Fragile Watermarking, Blind Watermarking

I. INTRODUCTION

Growth of computer technology and internet has led to tremendous opportunities for digital media content creation and distribution. Real time audio and video delivery, electronic advertising, digital repositories etc are some of the digital media applications. One of the major impediments to this growth is the lack of effective intellectual property protection of digital media to discourage unauthorized copying and distribution. Digital documents are easy to manipulate, to copy and to broadcast. The existing copyright laws are inadequate to deal with digital media. This led to the emergence of new technologies to deter unauthorized copying and distribution of digital content. One of such technologies is Digital watermarking, which today is synonymous to digital content protection. Digital watermarking is the process of embedding information into the source content that can be detected and extracted. Watermark is integrated into the content of host signal itself and requires no additional file header or conversion of data format. Unlike cryptographic technologies, digital watermarking does not restrict access to the source content but protects ownership of the content.

There have been many proposed novel techniques to hide watermark in digital images. These techniques can be classified into different categories according to several criteria like visibility, source content to be watermarked, embedding domain etc. Each of these classifications provides a wide range of algorithms that can be employed to achieve optimal performance for embedding and detection. In conventional watermarking scheme a certain amount of distortion to the recovered image is acceptable. This does not apply to all applications, particularly in military applications, space and medical imagery etc., loss of a single bit of information from the original image is not acceptable. Fragile or semi-fragile watermarking techniques can be employed to detect tampering and thus provide media authentication function. In some of such applications irreversible modification may not be admissible especially for legal evidence and surveillance applications. Watermarking techniques modify original data as a modulation of the watermark information and unavoidably cause permanent distortion to the original data. One of the interesting forms of watermarking algorithms is reversible watermarking algorithms. Reversible watermarking is a novel category of watermarking schemes that can not only strengthen the ownership of the original media but also can completely recover the original media from the watermarked media. The retrieved watermark can be used to determine the ownership by comparing the retrieved watermark with the assigned one. In reversible watermarking, the embedding process has an additional burden of embedding extra information in the payload that includes the recovery data that is used by the decoder to reconstruct the original image bit by bit. Thus the payload consists of the authentication information and recovery data. Reversible watermarking is especially suitable for the applications that require high quality images like for certain applications of digital media such as for legal evidence, digital commerce, security surveillance etc. any modification/tampering done to media has to be detected. Similar to conventional watermarking schemes, reversible watermarking schemes have to be robust against the intentional or the unintentional attacks, and should be imperceptible. Reversible watermarking is also referred as lossless watermarking. In this paper both the terminologies are used interchangeably. This paper focuses on the various techniques and algorithms used for reversible watermarking along with the characteristics of reversible watermarking algorithms.

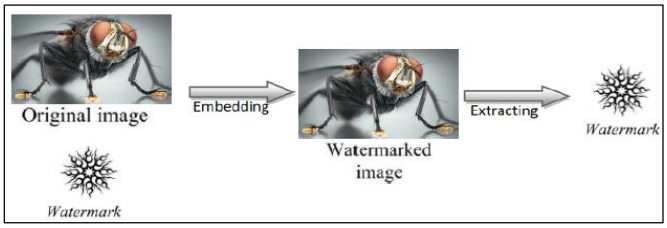

Figure1: Conventional Watermark Process

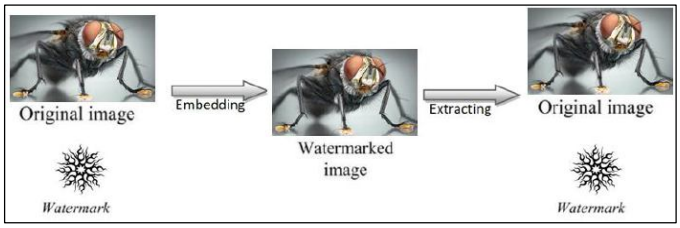

Figure 2: Reversible Watermark Process

Organization of the paper is as follows: Requirements for Lossless watermarking are elaborated in Section II, Lossless watermarking techniques are presented in Section III. Comparison of these techniques presented in Section IV. Finally, conclusions are summarized in Section V.

II. Requirements for Lossless watermarking

Conventional watermarking and reversible watermarking is shown in Fig 1 and Fig 2 respectively. The original image recovered during the extraction process of reversible watermarking is identical to the original image prior to watermarking. This feature of digital watermarking is useful in many applications. The applications could involve any form of digital media like audio, still images, video, text etc. Lossless watermarking scheme could be combined with other features of watermarking like robustness/fragile, visible/invisible, blind/non blind etc. Certain basic criterion for reversible watermarking are

A. Imperceptibility :

Also referred as Perceptual transparency, imperceptibility, refers to the characteristic where the embedded watermark should not effect the quality of cover media and hence the watermark should go un-noticed.

B. Robustness:

Robustness is a measure of the ability of the embedding algorithm to introduce the watermark in such a way that it is retained in the source content despite several stages of processing.

C. Oblivious versus non-oblivious (blind or non-blind):

In applications such as copyright protection and data monitoring, the watermark extraction algorithm can use the original un-watermarked data to find the watermark, this is called non-oblivious watermarking (non-blind watermarking). In other applications such as copy protection and indexing the watermark extraction algorithm cannot access the un-watermarked data. This significantly raises the difficulty of extraction; such methods are called oblivious watermarking algorithms.

D. Security:

Security of a watermarking technique can be judged the same way as with an encryption technique. The watermarking algorithm is truly secure, if knowing the exact algorithm to embed and extract data does not help an unauthorized party in actually recovering the original content from the watermarked data.

E. File Size:

Digital watermarking should not increase the size of the file considerably, which would raise suspicion on the embedded content.

F. Payload of watermark:

The amount of bits that the watermark signal carries depends on the application, for example, for copy protection purpose; a payload of one bit is more than sufficient. Watermarking granularity is a term used to refer to the number of bits that are actually needed to represent the entire watermark in the source content. In case of reversible watermarking, to recover the original source, the payload should also include the recovery information needed to reconstruct the original source hence the embedding capacity for this form of watermarking is higher.

Therefore, the reversible watermarking also has to satisfy all requirements of the conventional watermarking such as robustness, imperceptibility, and readily embedding and retrieving. Apart from these standard requirements reversible watermarking algorithms need to satisfy additional properties like blind watermarking and higher embedding capacity. In blind watermarking the original image can be recovered from the watermarked image without the presence of the original source.

III. Lossless watermarking techniques

In traditional watermarking schemes, watermarking is performed by embedding a digital signal into a digital host signal resulting in watermarked signal. This processes of embedding the watermark introduces certain amount of distortion into the host media and results loss of imperceptibility resulting in reduction of Peak Signal-to-Noise Ratio(PSNR). For applications pertaining to military, space, medical, legal etc. even certain amount of distortion is not acceptable as it results in loss of signal fidelity. Hence these applications require reversible watermarking, which can recover the original host signal perfectly after the watermark extraction. Reversible watermarking basically comes in two

flavors. The first type tests for underflow and overflow conditions prior to embedding the watermark and the second type of reversible watermarking schemes involves pre processing of the source digital media content prior to embedding the watermark. Various techniques of reversible watermarking are:

A. Lossless Watermarking using Difference Expansion

Tian [1] presented a reversible data embedding approach based on expanding the pixel value difference between neighboring pixels, which will not overflow or underflow after expansion. The difference is represented in binary form and right shifted by one bit to embed a single bit in the difference. The difference is said to be embeddable or changeable by substituting the LSB bit of the expanded difference with the watermark bit. The expanded difference should meet the overflow (pixels values > 255) and underflow (pixel values < 0) conditions. The original image is completely recovered from the watermarked images using reversible watermark embedding.

The DE embedding technique involves pairing the pixels of the host image and transforming them into a low-pass image containing the integer averages and a high-pass image containing the pixel differences. If 'x' and 'y' be the intensity values of a pixel-pair, then 'a' and 'h' are defined as

$$a = \lfloor (x+y)/2 \rfloor$$

$$h = x - y$$

This transformation is invertible, so that the gray levels 'x' and 'y' can be computed from 'l' and 'h' as

$$x = a + \lfloor (h+1)/2 \rfloor$$

$$y = a - \lfloor a/2 \rfloor$$

An information bit 'b' is embedded by appending it to the LSB of the difference, thus creating a new LSB. The watermarked difference is

$$h(new) = 2h + b$$

Disjoint sets are formed based on the following property:

- A pixel pair difference (h) can be either changed, expanded or unaltered
- Changed pairs provide no extra storage and expanded pairs give one free bit of storage
- An altered h must still result in an image in range [0,255], this can be determined mathematically:

$$|h| < \min(2(255-a), 2a+1)$$

  - Alterable h values are those wherein h values are expanded
  - If h value cannot be expanded, they are changed
- h values are left unaltered if they cannot stay in [0,255]

Altering the value(h) for embedding Watermark bit (b) through changing is obtained by

- testing the following condition for overflow and underflow for the grey scale image

$$|2\lfloor h/2 \rfloor + b| \le \min(2(255-a), 2a+1)$$

- New difference value h(new) for a changed pixel pair is obtained by:

$$h(new) = 2\lfloor h/2 \rfloor + b$$

- Remove the LSB and replace with Watermark bit(b)
- Store the remove LSB as part of the payload in order to restore the original image losslessly. This does not provide extra storage space as the original LSB also needs to be stored as part of the payload.

Altering the value h for embedding Watermark bit (b) through expanding is obtained by

- testing the following condition for overflow and underflow for the grey scale image

$$|2h + b| \le \min(2(255-a), 2a+1)$$

- New difference value h(new) for a expanded pixel pair is obtained by:

$$h(new) = 2h + b$$

- Left shift all the values by one
- Insert the water mark into the newly freed LSB. This provides one bit of extra storage space

In the next step a location map is created of all expandable difference values after embedding. This is done to find out whether a particular pixel pair has been expanded, changed or left unaltered at the time of watermark recovery. The location map represents a 1 for all those pixel pair which are expandable and 0 for those which are not expandable.

Watermark= Compressed Location Map+LSBvector+ Payload

During the extraction process the watermark bits are located from the Location map and using the LSB Vector the original values are restored back losslessly. This is done by forming disjoint sets based on the following property:

- A pixel pair difference (h) can be either changeable or unchangeable
- Condition to test whether high pass value is changeable or not is based on the following condition

$$|2\lfloor h/2 \rfloor + b| \le \min(2(255-a), 2a+1)$$

b: represents the watermark bit

Find all changeable pairs. All expandable pairs are also changeable. Collect all LSB from the changeable/expandable pairs.

Watermark=Compressed Location Map+LSB ector + Payload

Use the header information to identify the various components of the total payload. (Original Payload, compressed location map and the LSB vector set.)Recover the watermark,

decompress the location map losslessly. Using this map locations of expanded and changed pairs can be found. Calculate the original differences h(orig) for expandable pair using:

$$h(orig) = \lfloor h/2 \rfloor$$

Calculate the original differences h(orig) for changeable pair using:

$h(org) = 2\lfloor h/2 \rfloor + c$ c: stands for LSB vector bit.

Thus the original image is restored losslessly.

B. Histogram Modification

In[5], Ni et al. proposed a reversible data hiding method based on histogram modification wherein the entire signal is pre processed prior to the embedding process. In the scheme, part of the cover image histogram is shifted rightward or leftward to produce redundancy for data embedding. This shifting information is carried as part of the payload and used while restoring the original image back. In their scheme, the zero and peak points of an image histogram are shifted to vacate an empty bin for data embedding and achieved reversibility. Their scheme achieves low computational cost and high visual quality; however, the embedding capacity is low and mainly depends on the distribution of image histogram. In [6] Zhao et al. proposed a reversible data hiding based on multilevel histogram modification. In this scheme, the inverse "S" order is adopted to scan the image pixels for difference generation. The embedding capacity is determined by two factors, the embedding level and the number of histogram bins around 0.

C. Wavelet Transform

Sunil Lee et al [3] use the integer-to-integer wavelet transform for reversible watermarking. This method splits the input image into the blocks, and each block are transformed into the wavelet coefficients. Only the high frequency sub bands namely LH, HL, HH are used for watermark embedding. Watermark is embedded into this wavelet coefficient using either the LSB substitution or bit shifting. The wavelet coefficients are tested for its overflow and underflow conditions before the watermark is embedded in it. The authors also derive the conditions for both the overflow and the underflow using the reversibility nature of the Le Galle 5/3 integer wavelet transform (IWT). Since the method uses blind watermark extraction, which does not require the original images, a location map of the watermark embedding position is added to the watermarked images.

In [4] a watermarking scheme is proposed in which the image is decomposed in to wavelet coefficients and a visual recognizable logo and content based watermark information is embedded in the wavelet coefficients. The wavelet coefficients corresponding to the points located in a neighborhood that have maximum entropy are used for embedding the visual logo and the relations between the neighboring coefficients in the selected wavelet sub bands are embedded into middle frequency pairs of the first scale coefficients. This method embeds the maximum amount of watermark while the watermark is imperceptible. This technique provides two levels of protection while maintaining the image quality. The embedding of relation coefficients provide the capability to identify malicious changes made on the image. Similar to wavelet transforms, Integer Cosine Transform could also be used to achieve reversibility [9].

IV. COMPARISIONS

Difference expansion though is a very simple algorithm to implement, it is not robust against various forms of attacks and could be used as a form of fragile watermark. Unlike Difference Expansion that checks for the suitability of a pixel prior to embedding, Histogram modification prepares the host signal for embedding by employing pre-processing tasks. Some variations to these schemes exist. Alattar [7] developed Tian's method by using four neighboring pixels to carry more of secret data to improve the embedded capacity and image quality. Hong et al. [8] introduced a novel difference expansion scheme based on modification of prediction errors. This scheme firstly predicts pixel values and then obtains error values. Secret bits are embedded reversibly by modifying the values of prediction errors, which provides higher embedding capacity with better image quality. Histogram modification methods though have less embedding capacity but are high on robustness factor. Wavelet transforms is a new time-frequency analyzing method to localize spatial and frequency domain.DWT based techniques are the most popular schemes used by researchers to embed the watermark into a source media in transform domain. Watermarks can be embedded within source media by modifying the transform domain DWT coefficients. These methods provide better robustness and quality as compared with methods of spatial domain.

V. CONCLUSIONS

Reversible watermarking algorithms are attracting huge interest in recent times. Its key advantage is not only the secret data but also the host image can be accurately recovered during the extraction process. Because of this lossless feature it plays an important role in some specific scenarios such as military, medical diagnosis, law enforcement and so on, where the cover images must be accurately reconstructed after data extraction. The reversible Watermarking algorithms can be basically categorized into two main flavors; one based on the embedding domain ; ie. spatial domain or frequency domain; and the other based on the robustness factor, ie; fragile or robust. Various techniques discussed in this paper can be implemented based on the application domain.

REFERENCES

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

[2] 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.

[3] Sunil Lee, Chang D. Yoo and Ton Kalker, "Reversible Image Watermarking Based on Integer to Integer wavelet Transform," IEEE Transactions on Information Forensics and Security, Vol. 2 No. 3, [September 2007].

[4] Krishnan, N.; Selvakumar, R.K.; Rajapandian, S.; Arul Mozhi, K.; Nelson Kennedy Babu, C.; , "A Wavelet Transform Based Digital Image Watermarking and Authentication," India Conference, 2006 Annual IEEE , vol., no., pp.1-6,[Sept. 2006].

[5] Ni Z, Shi Y, Ansari N, Su W. Reversible data hiding. In: IEEE proceedings of ISCAS'03, vol. 2. 2003. p. II-912–915

[6] Zhao, Z., H. Luo, Z.M. Lu and J.S. Pan, 2011. Reversible data hiding based on multilevel histogram modification and sequential recovery. AEU-Int. J. Electron. Commun., 65: 814-826.

[7] A.M. Alattar, "Reversible Watermarking Using the Difference Expansion of a Generalized Interger Transform", IEEE Transactions on Image Processing, Vol. 13, No. 8, pp. 1147-1156, 2004

[8] Hong, W., J. Chen and T.S. Chen, 2009. Blockwise reversible data hiding by contrast mapping. Inform. Technol. J., 8: 1287-1291.

[9] L. T. Ko, J. E. Chen, H. C. Hsin, Y. S. Shieh, and T. Y. Sung, "A unified algorithm for subband-based discrete cosine transform," Mathematical Problems in Engineering, vol. 2012, Article ID