International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 2; Issue 6; November 2017; Page No. 745-748

Reversible watermarking based on entropy masking and DWT

Dr. Pushpinder Kaur
Associate Professor, BZSFS Khalsa Girls College Morinda, Ropar, Punjab, India

Abstract
We propose a new reversible watermarking scheme. One first contribution is a DWT [Discrete Wavelet Transform] modulation which adaptively takes care of the local specificities of the image content. In this paper, we propose a new reversible watermarking scheme. One first contribution is a DWT modulation which adaptively takes care of the local specificities of the image content. By applying it to the image prediction-errors and by considering their immediate neighborhood, the scheme we propose inserts data in textured areas where other methods fail to do so. Furthermore, our scheme makes use of a classification process for identifying parts of the image that can be watermarked with the most suited reversible modulation. This classification is based on a reference image derived from the image itself, a prediction of it, which has the property of being invariant to the watermark insertion. Entropy masking is another human visual system's characteristic, which rarely has been addressed in visual models. In this paper we also propose a universal entropy masking model for watermarking embedding algorithm to keep the balance between watermarks' imperceptibility and its robustness. Also we conclude from the experiments that a suitable domain of entropy calculation will result in optimal watermarking performance. For the implementation of this proposed work we use Image Processing Toolbox under the Matlab software.

Keywords: DWT, watermarking, entropy masking, robustness

Introduction

DIGITAL watermarking is a process in which some information is embedded within a digital media so that the inserted data becomes part of the media. This technique serves a number of purposes such as broadcast monitoring, data authentication, data indexing. Watermarks have two categories of roles: In the first category, the watermark is considered as a transmission code and the decoder must recover the whole transmitted information correctly. In the second category, the watermark serves as a verification code. In the latter system, the watermark detector must simply determine the presence of a specific pattern. Since the footprint of the verification watermarking, that is, the number of pixels per watermark code bit is typically higher, this case has higher robustness as compared to the subliminal channel case. In watermarking schemes, the watermark message is embedded in the host signal in different ways, for example, additively or multiplicatively. These methods allow the user to restore exactly the original image from its watermarked version by removing the watermark. Thus it becomes possible to update the watermark content, as for example security attributes (e.g., one digital signature or some authenticity codes), at any time without adding new image distortions. Since the introduction of the concept of reversible watermarking in the Barton patent, several methods have been proposed. Among these solutions, most recent schemes use Expansion Embedding modulation, DWT modulation or, more recently, their combination.

Among these solutions, most recent schemes use Expansion Embedding modulation, DWT modulation or, more recently, their combination. One of the main concerns with these modulations is to avoid underflows and overflows. Indeed, with the addition of a watermark signal to the image, caution must be taken to avoid gray level value underflows (negative) and overflows (greater than for a bit depth image) in the watermarked image while minimizing at the same time image distortion.

Reversible watermarking (RW) methods are used to embed watermarks, e.g., secret information, into digital media while preserving high intactness and good fidelity of host media. It plays an important role in protecting copyright and content of digital media for sensitive applications, e.g., medical and military images. Although researchers proposed some RW methods for various media, e.g., images, audios, videos, and 3-D meshes; they assume the transmission channel is lossless. The robust RW (RRW) is thus a challenging task. For RRW, the essential objective is to accomplish watermark embedding and extraction in both lossless and loss environment. As a result, RRW is required to not only recover host images and Watermarks without distortion for the lossless channel, but also resist unintentional attacks and extract as many watermarks as possible for the noised channel. Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. This technique is better than Digital Signatures and other methods because it does not increase overhead.

The main contributions of this paper to the watermarking community are:

- A reversible watermarking algorithm for copyright protection of plain text documents is proposed.
- There is no restriction about the type and length of text.
- Pure alphabetical watermarks are used which are more

convenient to be used for plain text

- No changes are made in the text rather attributes of the text are used in the proposed approach.
- This approach towards medium size files like emails, short articles and news is robust and practical to identify the original copyright owner of the contents.

Watermarking Process

Digital Watermarking software looks for noise in digital media and replaces it with useful information. A digital media file is nothing more than a large list of 0's and 1's. The watermarking software determines which of these 0's and 1's correspond to redundant or irrelevant details.

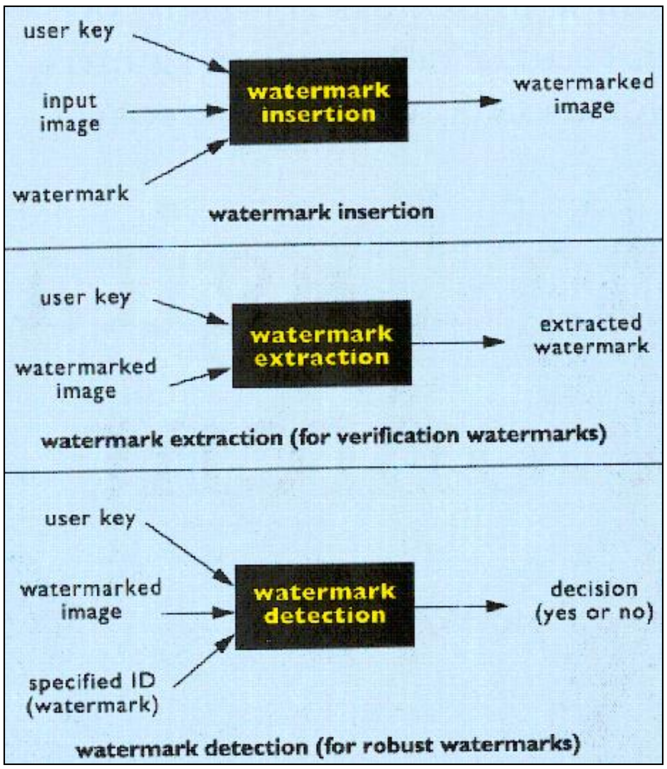

Fig 1

Requirements of water marking

To be effective in the protection of the ownership of intellectual property, the invisibly watermarked document should satisfy several criteria:

1. the watermark must be difficult or impossible to remove, at least without visibly degrading the original image,
2. the watermark must survive image modifications that are common to typical image-processing applications (e.g., scaling, color re-quantization, dithering, cropping, and image compression),
3. an invisible watermark should be imperceptible so as not to affect the experience of viewing the image, and
4. For some invisible watermarking applications, watermarks should be readily detectable by the proper authorities, even if imperceptible to the average observer. Such decidability without requiring the original, un-watermarked image would be necessary for efficient recovery of property and subsequent prosecution.

Embedding Stage

One of the most important features that make the recognition of images possible by humans is color. Color is a property that depends on the reflection of light to the eye and the processing of that information in the brain. The color is used every day to tell the difference between objects, places, and the time of day. Usually colors are defined in three dimensional color spaces usually colors are defined in three dimensional color spaces. These could be RGB (Red, Green, and Blue), HSV (Hue, Saturation, and Value) or HSB (Hue, Saturation, and Brightness). The last two are dependent on the human perception of hue, saturation, and brightness. Color represents the distribution of colors within the entire image. This distribution includes the amounts of each color, but not the locations of colors.

Watermarking Algorithm

In this approach, a block DCT-based algorithm is developed to embed the binary watermark into the color host image. Since small high frequency components may be discarded in some image processing operation such as JPEG compression, the very low frequency components of the color host image will be utilized for the watermark embedding.

The Embedding Algorithm

In the technique presented here, the color image is decomposed into three components R, G and B. Watermark information will be embedded in the G plane using equation 1 to produce G'. Assume that *f (i, j)* represents the pixel of the component of the RGB representation of the color host image, *w (i, j)* represents the binary pixel of the watermark.

$$F_k(u,v) = DCT\{f_k(i,j)\},$$

If w(i,j)=1 then

$$F_k(x,y) = \begin{Bmatrix} \Delta Q_e\left(\frac{F_k(x,y)}{\Delta}\right) & x,y \in H_k & 1 \le k \le N_{HB} \\ F_k(x,y) & x,y \notin H_k & 1 \le k \le N_{HB} \end{Bmatrix}$$

If w(i,j)=0 then

$$F_k(x,y) = \begin{Bmatrix} \Delta Q_o\left(\frac{F_k(x,y)}{\Delta}\right) & x,y \in H_k & 1 \le k \le N_{HB} \\ F_k(x,y) & x,y \notin H_k & 1 \le k \le N_{HB} \end{Bmatrix}$$

Where Qe is the quantization to the nearest even number and Qo is the quantization to the nearest odd number Δ is a scaling quantity and it is also the quantization step used to quantize either to the even or odd number. The predefined coefficients in each 8x8 sub block are represented by NHB

Extracting Stage

In a digital watermarking scheme, it is not convenient to carry the original image all the time in order to detect the owner's signature from the watermarked image. Moreover, for those applications that require different watermarks for different copies, it is preferred to utilize some kind of watermark-independent algorithm for extraction process i.e. dewaters marking. Its robustness against many attacks including rotation, low pass filtering, salt n paper noise addition and compression. For better activeness, watermark should be acoeperceptually invisible within host media, statistically invisible to unauthorized removal, readily extracted by owner of image, robust to accidental and intended signal distortion like filtering, compression, re-sampling, retouching, crapping etc. For a digital watermark to be effective for ownership, it must be robust, recoverable from a document, should provide the original information embedded reliably and also removed by authorized users.

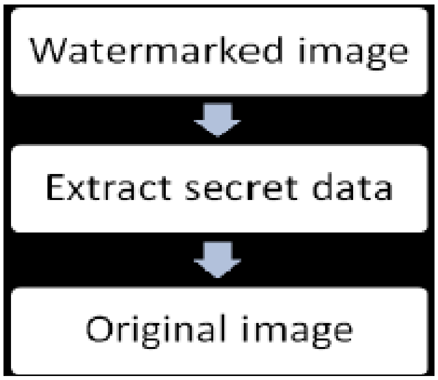

Fig 2

The Extraction Algorithm

The embedded information w (i,j) can be extracted by performing 8x8 DCT transform for the watermarked host image and indicate the same coefficients of the host image that carries the 16 bits of the embedded watermarks using the same secret key in the initial scrambling operation.

$$If\ \ Q\left(\frac{F_k(x,y)}{\Delta}\right) \text{ is odd then } w(i,j)=0$$

$$If\ \ Q\left(\frac{F_k(x,y)}{\Delta}\right) \text{ is even then } w(i,j)=1$$

Where Q is rounded to the nearest integer, the scaling quantity is the same as the one used in the embedding process.

Robustness

The watermark should be robust such that it must be difficult to remove. The watermark should be robust to different attacks. The robustness describes whether watermark can be reliably detected after performing some media operations.

Entropy

Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image.

R = -sum (x.*log(x)

Where x signifies the histogram counts for a grey-scale image. Entropy of an image is one of the parameters of an image and it doesn't change when the image is not changed. Entropy is used as a quality metrics to measure the degree of perceptibility of watermark in the cover image by comparing the original and watermarked images. Thus the effect of embedding algorithm on cover image in terms of perceptual similarity between the original image and watermarked image using is measured through Entropy. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image.

Let P contains the histogram counts. The entropy is represented as

$E = -\Sigma p\ log2(P)$

Discrete wavelet transform

Discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency *and* location information (location in time). DWT involves decomposition of image into frequency channel of constant bandwidth. This causes the similarity of available decomposition at every level. DWT is implemented as multistage transformation.

Conclusion

In this paper, our primary focus is on new reversible watermarking scheme. Which originality stands in identifying parts of the image that are water marked. In this paper we also discuss universal entropy masking model for watermarking embedding algorithm to keep the balance between watermarks' imperceptibility and its robustness. Also we conclude from the experiments that a suitable domain of entropy calculation will result in optimal watermarking performance. Here we discuss on discrete wavelet transform and robustness.

References

1. Coatrieux G, Wei Pan. Reversible Watermarking Based on Invariant Image Classification and Dynamic Histogram Shifting, IEEE Transactions on information Forensics & Security, 2013; 8(1).
2. Kamlesh C Badhe, Prof. Jagruti R Panchal. Implementation of Audio Watermarking Using Wavelet Families, International Journal of Innovative Science, Engineering & Technology, 2014; 1(4).
3. Seema, Sheetal Sharma. DWT-SVD Based Efficient Image Watermarking Algorithm to Achieve High Robustness and Perceptual Quality, International Journal of Advanced Research in Computer Science and Software Engineering, 2012; 2(4).
4. Luo L, Chen Z, Chen M, Zeng X, Xiong Z. Reversible image watermarking using interpolation technique, IEEE Trans. Inf. Forensics Security, 2010; 5(1):187-193.
5. Coltuc D. Improved embedding for prediction-based reversible watermarking, IEEE Trans. Inf. Forensics Security, 2011; 6(3):873-882.
6. Lin CC, Tai WL, Chang CC. Multilevel reversible data hiding based on histogram modification of difference images, Pattern Recognition., 2008; 41:3582-3591.
7. Yang CH, Tsai MH. Improving histogram-based reversible data hiding by interleaving predictions, IET Image Process., 2010; 4(4):223-234.
8. Tsai P, Hu YC, Yeh HL. Reversible image hiding scheme using predictive coding and histogram shifting, Signal

Process, 2009; 89:1129-1143.
9. Coltuc D, Chassery JM. Distortion-free robust watermarking: A case study, in Proc. Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose, CA, 2007, 65051N-8.
10. Pan W, Coatrieux G, Cuppens N, Cuppens F, Roux C. An additive and lossless watermarking method based on invariant image approximation and Haar wavelet transform, in Proc. IEEE EMBC Conf., Buenos Aires, Argentina, 2010, 4740-4743.
11. Sachnev V, Kim HJ, Nam J, Suresh S, Shi YQ. Reversible watermarking algorithm using sorting and prediction, IEEE Trans. Circuit Syst. Video Technol., 2009; 19(7):989-999.
12. Hwang HJ, Kim HJ, Sachnev V, Joo SH. Reversible watermarking method using optimal histogram pair shifting based on prediction and sorting, KSII, Trans. Internet Inform. Syst., 2010; 4(4):655-670.
13. Chao HM, Hsu CM, Miaou SG. A data-hidding technique with authentication, integration, and confidentiality for electronic patient records, IEEE Trans. Inf. Technol. Biomed., 2002; 6(1):46-53.
14. Rakesh Ahuja SS, Bedi Himanshu Agarwal. A Survey of Digital Watermarking Scheme, MIT International Journal of Computer Science & Information Technology, 2012; 2(1):52-59.
15. Ramana P, Reddy. Dr. Munaga VNK prasad, Dr. D. Sreenivasa Rao, - Robust Digital Watermarking of Images using Wavelets. International Journal of Computer and Electrical Engineering, 2009, 1(2).