IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 4 (Nov. - Dec. 2013), PP 01-04
www.iosrjournals.org

Survey on Reversible Watermarking

Priyanka S. Aher[1], K. U. Rahane[2]
[1,2](Department of Computer Engineering, AVCOE, Ahmednagar, India)

Abstract: *A number of research papers has been produced about reversible watermarking. Reversible watermarking is one of the important scheme of the watermarking schemes. Some security measures must be there to protect the records from unauthorized user and destruction of information. Basic idea of digital watermarking is to embed the data into the cover media to provide the security to data. The watermarking techniques satisfying these requirements called as Reversible watermarking. Ownership of the original media remains same but the best thing is original media is recovered from the watermarked media. This is the best and main feature of reversible watermarking to extract the original image as it is without any distortion. This feature is applicable in various areas such as medical as well as military images. If there is effect on the cover then it would changes the meaning of this data. The aim of this paper is to represent the purpose of reversible watermarking, some of the techniques related to reversible watermarking.*

Keywords: *Reversible watermarking, Security, copyright protection*

I. INTRODUCTION

Digital watermarking is the important method to protect the copyright of digital images. In Intellectual Property Right (IPR), a trademark or logo of the owner can be selected as a watermark. This watermark is embedded into the original image to protect that image. The original image after embedding the watermark, is known as watermarked image. The watermarked image can be published and owner can prove the ownership of the image by retrieving the watermark from the watermarked image.

In hospitals and health care systems there is huge amount of data storage. It also transmits that data to other systems for diagnosis. It includes medical images, patient records and some administrative documents. Among all these data, medical images and patient records are the important data that needs to be protected against unauthorized access and malicious attacks. To provide the security to this information integrity, confidentiality and authenticity are the three important requirements. Confidentiality can be maintained by embedding the patient information into the medical images. After performing the embedding operation the watermarked image and original image should be similar to perform the diagnosis with the hidden information. To maintain the integrity of medical images is another important issue. Authentication should be provided to the medical images. And for all this there is the requirement of watermarking. Digital watermarking is a process that embeds the information into the host media to provide the security purpose. Security involves copy control authentication, copyright protection.[1]

Digital watermarking is used so that correct information is received and proper treatment is provided to the patient. It is important to extract the image and information as the original image without any distortion in image. In medical images, after transmission, it is necessary to have both, original image and information to be lossless. Our main aim is to embed and extract the watermark with minimum loss. Reversible watermarking recovers the original image after extracting the watermark. The reversible watermarking provides the authentication and also recovers the original image. [2] A general watermarking scheme has to meet the following requirements. [3]

1. Robustness:
The watermarked image should not be destructed from the standard image processing and malicious attacks. For example before transmitting, image can be compressed or rotated. Robustness of the watermark data means that the watermark data should not be destroyed if someone performs the some operations on data. It may be malicious attacks or non-malicious operations for example rotation, scaling. There may be some intentional or non- intentional attacks that tries to remove the embedded watermark. It is the important requirement of the watermarking.

2. Imperceptibility: A watermark that is embedded into the image may be visible or non-visible. The visible watermark is perceptible. To decrease the risk of cracking, most of the watermarks are invisible. At the same time the quality of watermarked image is also important. If the watermark embedding process affect the quality of the watermarked image, then it will lose its value. Therefore the quality of the original image and the

3. Embedding and Extracting : The watermark embedding process must be easy. Similarly, it must be secure to embed and retrieve the watermark by the owner.

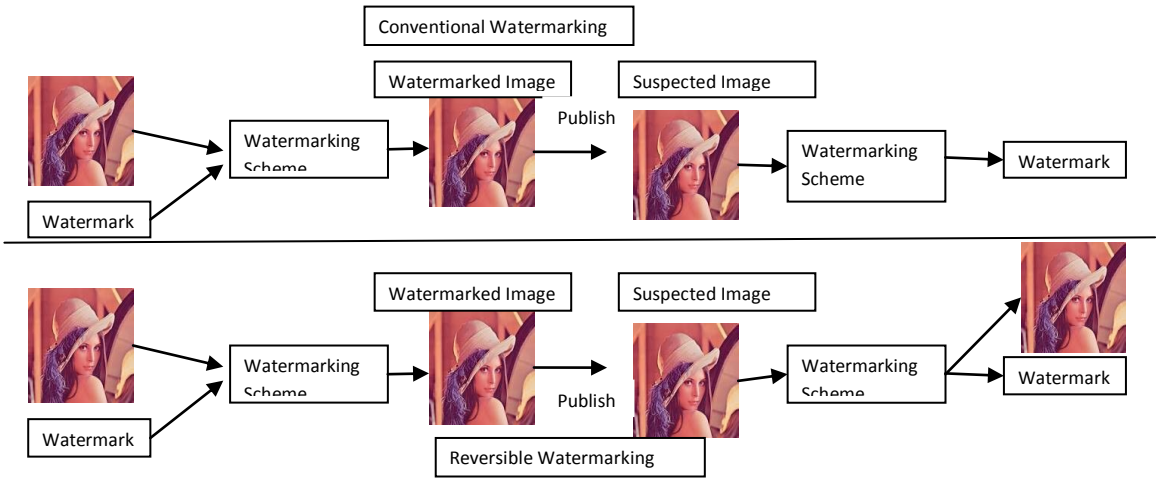

Figure 1: Flowchart for conventional and reversible watermarking

In recent years a special kind of digital watermarking is discussed widely that is called as reversible watermarking. It not only assures the ownership of the original media but also completely recovers the original media from the watermarked media. It is the key feature of reversible watermarking to extract the original image as it is.

The watermark extracted can be used to determine the ownership by comparing the extracted watermark and the assigned one. Like conventional watermarking scheme, Reversible watermarking has to be robust against the intentional or non-intentional attacks. And it should be imperceptible to avoid the attacks and value lost. The requirements satisfied by the conventional watermarking such as robustness, imperceptibility has to satisfy by the reversible watermarking methods. With the above requirements reversible watermarking has to satisfy the following two characteristics:

1. Blind : To retrieve the embedded watermark, it requires the original image in some conventional watermarking schemes. In reversible watermarking, it is not necessary to have the original image. It can directly extract the embedded watermark. Such a technique is known as blind watermarking that means it does not require the original image to extract the watermark.

2. Higher embedding capacity : Capacity property of digital watermarks refers to amount of information that can be embedded within the media. The embedding capacity of the reversible watermarking is much more than the conventional watermarking scheme. The embedding capacity should not be low as it affects the accuracy of extracted watermark and the recovered image.

The general procedure of the conventional and reversible watermarking scheme can be illustrated by the figure 1.The procedure of the conventional and reversible watermarking are similar except one step. The change is that in reversible watermarking one function is extra that recovers the original image from the suspected image. That's why the reversible watermarking is suitable for the applications where high quality images are required. For example military and medical applications. There are two research fields that are connected with the digital watermarking that are data hiding (steganography)[4] and image authentication [5]. The purpose of data hiding is to hide the secret information in the cover image. The purpose of image authentication is to verify whether the received image is tampered or not. To achieve this goals, it is required that data hiding scheme should have a large capacity to carry more secret information. And the information hidden must be imperceptible so that information will be secure. The image authentication scheme also embeds the information in protected image. It has to keep imperceptibility between the original image and processed image. The goal of reversible watermarking is to assure the ownership and to recover the original image. Imperceptibility, blind and readily embedding and retrieving, robustness are the different criteria's of reversible watermarking. A number of schemes for digital images are already proposed. In this paper some of the schemes of reversible watermarking are focused. Schemes for digital images are focused. There are several reversible watermarking schemes which have been proposed [6,7,8,9,10,11,12].

II. REVERSIBLE WATERMARKING SCHEME BY APPLYING DATA COMPRESSION

To extract the original image from the watermarked image, the recovery information is embedded into the original image. With the recovery information, we also have to embed the watermark data into the original

image. That's why the capacity required to embed the information is more. So, to embed more data, a solution is to compress the embedding data. By applying the data compression it reduces the size of embedding data. There are various techniques related to this. [13,14,15,16] The embedding procedure is as below:

1. The L-level scalar quantization is applied to each pixel and the reminders are generated.

$$QL(x) = L * \frac{x}{L} \quad \text{("Equation 1")}$$

For example, the 4*4 block of original image is:

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

,The watermark W $\{10\ 0010\ 1011\}_2$, 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

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

2. To compress the reminders CALIC lossless compression algorithm is used. Using adapted CALIC lossless compression algorithm [29, 32] to compress the remainders. With the above example, it is assumed that 16 remainders are compressed to the 12 digit data. It is denoted as {x0,x1,…..,x11}. It can be decompressed to the original 16 remainders.
3. We have converted the data using L-ary scalar quantization concatenate that data. For the above same example, watermark W is converted from {10 0010 1011}2 to {4 2 1 0}5, and it becomes {x0, x1, x2, . . . , x10,x11, 4, 2, 1, 0}
4. The compressed data and watermark are added to the quantified image and the watermark image is generated.
   Finally, the watermarked image is produced.

$$H'= \begin{pmatrix} 20+x0 & 35+x1 & 5+x2 & 20+x3 \\ 35+x4 & 10+x5 & 30+x6 & 10+x7 \\ 20+x8 & 10+x9 & 15+x10 & 20+x11 \\ 10+4 & 20+2 & 10+1 & 25+0 \end{pmatrix}$$

The robustness of this type of reversible watermarking is weak. Due to this it cannot resist the distortions. And any loss of the compressed data crashes the whole embedded data. That's why such type of watermarking schemes lack robustness.

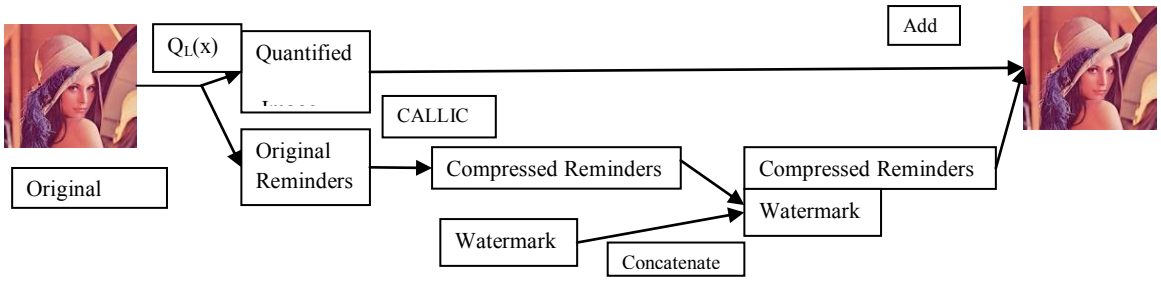

Figure 2: Watermark Embedding Process

III. HISTOGRAM ROTATION-BASED IMAGE WATERMARKING

The basic principle of this scheme is based on the histogram rotation of randomly selected two zones and randomness of Discrete Fractional Random Transform(DFRT)[18,19]. The proposed method assumes that histogram property of the randomly selected two zones is most likely to DFRTed version of host image. DFRT can be derived from the discrete fractional random Fourier transform(DFRFT). Random matrix generates the randomness. The overall process is similar. From diagonal symmetric random matrix DFRT can be generated.[17] As like the patchwork scheme, two pseudo-random zones of the host image are transformed in

opposite directions. The watermarking scheme proposed here is blind watermarking as it does not require the original image to extract the watermark. All the embedding and extracting procedures are carried out in the DFRT domain.

1. DFRT is used to transform the host image X. The fractional order of random kernel matrix. This two values are used as a secret keys.
2. Choose the two random zones A and B from the DFRT of the host image and two non-overlapping M × M random blocks. The center of mass of zones A and B that is Ma and Mb are computed.
3. Va and Vb represent the vectors pointing from the center of the circle to Ma and Mb. Rotate the slightly to them and watermark embedding is achieved. Va and Vb are rotated clock-wise and anti-clockwise to embed the message bit 0 (bit 1).
4. Perform the process until all the bits of the watermark are embedded. Apply the inverse DFRT to the watermarked coefficients of the DFRTed image. The final watermarking image is obtained by this.

IV. CONCLUSION

In this paper, We have defined and introduced the reversible watermarking schemes. watermarking scheme classified into two types. They are the schemes which apply data compression and histogram shifting. Reversible watermarking schemes are still in development and have great potential possibilities. Form this paper, We provided an introduction of reversible watermarking.

REFERENCES

[1] Hsiang-Cheh Huang and Wai-Chi Fang (2011) *IEEE/NIH Life Science Systems and Applications Workshop*.

[2] Lain Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, Zhang Xiong (2010) *Information Forensics and Security, IEEE Trans-actions*, vol.5, no.1, pp.187-193.

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

[4] J. B. Feng, H. C. Wu, Tsai, Chu, A new multi-secret images sharing scheme using LaGrange's interpolation, Journal of Systems and Software, volume - 76, pp. 327–339, June 2005.

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

[6] A. M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Transactions on Image Processing, vol. 13, page- 1147–1156, Aug. 2004.

[7] M. U. Celik, G. Sharma, A. M. Tekalp, Saber, Lossless generalized-lsb data embedding, Transaction of IEEE on Image Processing, volume-14, page 253–266, Feb. 2005.

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

[9] T. Kalker, Willems, Capacity bounds and code constructions for reversible data-hiding, Proceedings of Electronic Imaging 2003, Security and Watermarking of Multimedia Contents V, page- 604–611,USA, Jan- 2003.

[10] D. M. Thodi, Rodriguez, Reversible watermarking by prediction-error expansion, Proceedings of the 6th IEEE Southwest Symposium on Image Analysis and Interpretation, volume-3, page-21–25,USA,March. 2004.

[11] C. Tsai, K. C. Fan, C.Chung, T. Chung, Reversible and lossless data hiding with application in digital library, Proceedings of the 38th Annual International Carnahan Conference on Security Technology, page-226–232, Albuquerque, USA, October- 2004.

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

[13] M. U. Celik, G. Sharma, Tekalp, Saber, Lossless generalized-lsb data embedding, Transactions of IEEE on Image Processing, volume - 14, page- 253–266, Feb. 2005.

[14] C. D. Vleeschouwer, J. E. Delaigle, Macq, Circular interpretation of histogram for reversible watermarking, Proceedings of the IEEE 4th Workshop on Multimedia Signal Processing, page- 345–350, France, October-2001.

[15] M. U. Celik, Sharma, Tekalp, Saber, Localized lossless authentication watermark, International Society for Optical Engineering, volume - 5020, pp. 689–698, USA, January- 2003.

[16] M. U. Celik, G. Sharma, A. M. Tekalp, Saber, Reversible data hiding, Proceedings of the International Conference on Image Processing, page157–160, USA, September 2002.

[17] Z. Liu, H. Zhao, Liu, "Optics Communications" 255 **(2005)**.

[18] A.Umaamaheshvari, Thanushkodi, IJCSNS 11 **(2011)**.

[19] Youngseok Lee, Kim, Histogram Rotation-Based Image Watermarking with Reversibility International Journal of Security and Its Applications Volume-6, April, 2012