ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

A Digital Watermarking Algorithm Using Random Matrices

K.Mounika
Department of CSE,
Sri Venkateswara College of
Engineering and Technology,
Tiruvallur, India.

Dr. K.Sankar
Department of CSE,
Sri Venkateswara College of
Engineering and Technology,
Tiruvallur, India.

Dr. R.Jayasankar
Department of Mathematics,
Thiruvalluvar University College
of Arts & Science, Arakkonam,
India

Abstract - ***A very big challenge in the recent scenario is to protect our digital assets from various scourges. The current focus is to protect unauthorized copying of digital assets which give rise to piracy. Existing digital watermarking techniques protect our digital assets by embedding a digital watermark into a host digital image. This embedding does induce slight distortion in the host image but the distortion is usually too small to be noticed. Even though there are various techniques of digital watermarking, our constant effort is to increase the robustness of the digital watermark. Ultimately, to increase the security of the copyright of protection the proposed work is in the direction of random matrix and ancient magic square. Of course, this algorithm has considerably increased the robustness in digital watermark while enhancing the security of production.***

Keywords:*Digital watermarking, Random Matrix, Embedding, Extraction.*

1. INTRODUCTION

Channelizing digital assets using internet has involved a technique that is able to protect the copyright of published Medias into a certainty. The easy distribution of these documents through the web may defile protection laws against unauthorized copies and make fidelity questionable. Digital watermarking has been projected as asolution against these practices. Digital watermark is an authenticating technique of digital data with secret information that can be extracted to the receptor. The image in which this data is inserted is called 'cover image' or 'host image'**.** The watermarking process has to be resistant against possible attacks, keeping the content of the watermark readable in order to be recognized when extracted. Features like robustness and fidelity are essentials of a watermarking system however the size of the embedded information has to be considered since data becomes less robust as its size increases. Therefore a trade-off of these features must be considered.

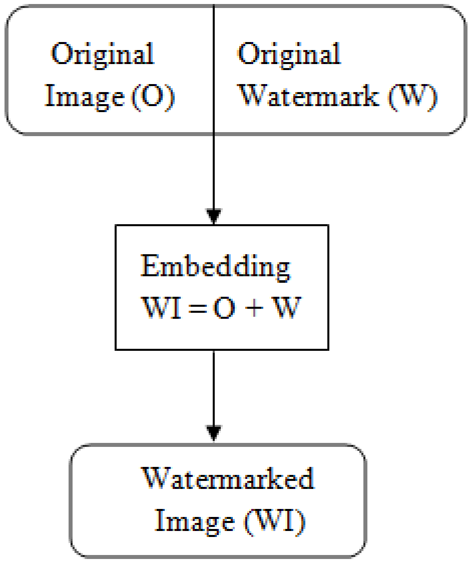
Typical mechanisms considering the security aspects are watermarking and cryptography, respectively. The first one aims to insert a secret message, the watermark, into the saved data so that its existence is kept secret. To be effective, a watermark should not introduce intelligible object in the host data and it should be detectable also if unintentional or intentional modifications of the watermarked signal occurred. The State of the art is that watermarking methods embed the watermark bits into the most significant portions of the digital data, so that they cannot be removed without marring the original content.

2. PRINCIPLE OF DIGITAL WATERMARKING

The digital watermarking system essentially consists of a watermark embedder and a watermark detector. The watermark embedder inserts a watermark onto the cover signal and the watermark detector detects the presence of watermark signal.

A digital watermarking process have three phases, first embedding, second attack and third detection. In Embedding, an algorithm accepts the host image and the watermark image or data to be embedded and produces a watermarked image. The watermarked image is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack.

There are different kinds of attacks like copy, removal, mosaic etc. Watermark detection is an algorithm which is used to find the attacked data to attempt to extract the watermark from it. If the watermarked image is not modified during transmission, then the watermark is still present and it can be extracted. If the watermarked image is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, but it is carried with the watermarked image itself. [2] Figure 1 and Figure 2 shows the flowchart of watermarking process.



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

Fig.1 Flowchart of embedding of watermark

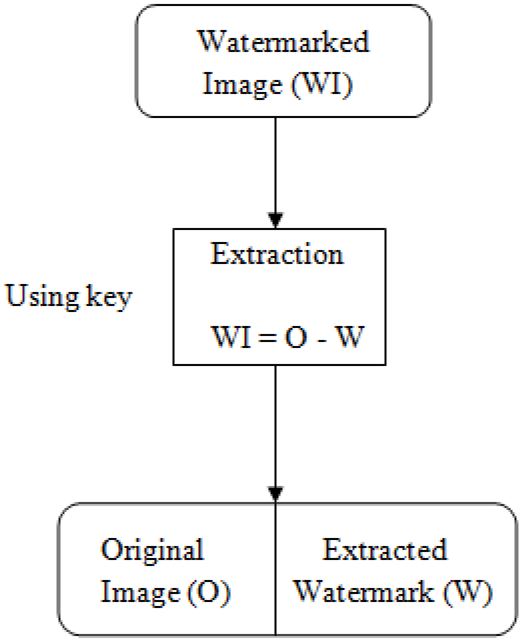


Fig.2 Flowchart of extraction of watermark

The watermarked image is processed through a detector in which generally a reverse process to that used during the embedding phase is applied to retrieve the watermark. The different watermarking algorithms differ in the way in which itembeds the watermark on to the cover object. A secret key is used during the embedding and theextraction process in order to prevent illegal access to the watermark. This paper deals with the new watermarking technique which helps to protect digital image based on RMI (Randomized Matrices).

3. Overview of randomized matrix.

This is an auto generated Image based on Random Matrix Image generated in SCILAB using random function [3]. In SCILAB Random Matrix can be generated using random function having randomized number from given range. In simulation we can also generate real number. For example we want to generate a random matrix of 8 x 8 from 0 to 10 numbers. Matrix may cover any number from 0 to 10 like shown in figure 3 (b).

3.1 WATERMARKING EMBEDDING ALGORITHM

Step1: Read the original image.

Step2: Generate RMI (in range of 0 to 10) which is to be embedded. (Secret Key Matrix)

Step3: Add this Generated Image and Original Image in matrix addition form.

Step4: Now generate image from matrix form.

Step5: The output image is a watermarked image.

3.2 WATERMARK EXTRACTION ALGORITHM

Step1: Read the watermarked image.

Step2: Read matrix (a secret key) which is sent with image.

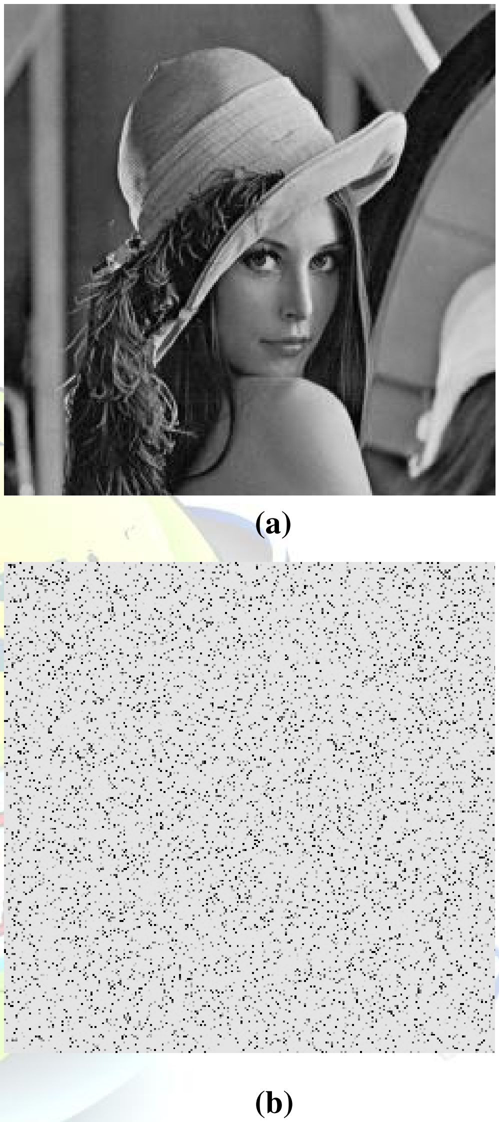
Step3: Subtract Matrix from watermarked Image in matrix subtraction form.

Step4: Now generate two different images from theses matrices form.

Step5: The output images are Original image andwatermarked image.

4. IMPLIMENTATION & RESULTS

SCILAB simulations are performed by using 256×256 pixel gray level "Lena" image and 256 × 256 pixel watermark(RMI)[4]. Figure 3. (a) and (b) Shows greyscale image of 256X256 pixel and RMI Watermark respectively. Figure 4 (a) and (b) show 8X8 pixel matrix of Figure 3 (a) and (b) images respectively. Figure 5 (a) and (b) shows output image and 8x8 matrix of watermarked Lena image


(a)

(b)

Fig. 3 (a) Original Lena Image (b) RMI watermark

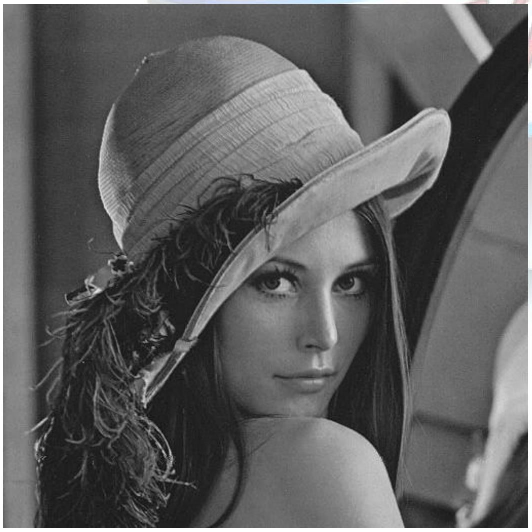
$$\begin{bmatrix} 195 & 195 & 196 & 197 & 197 & 198 & 199 & 199 \\ 196 & 196 & 196 & 197 & 197 & 197 & 198 & 198 \\ 197 & 197 & 197 & 197 & 196 & 196 & 196 & 196 \\ 199 & 198 & 198 & 197 & 196 & 195 & 194 & 194 \\ 199 & 198 & 197 & 196 & 195 & 194 & 193 & 193 \\ 198 & 198 & 197 & 196 & 195 & 194 & 193 & 193 \\ 197 & 196 & 196 & 195 & 195 & 194 & 194 & 194 \\ 196 & 196 & 195 & 195 & 195 & 194 & 194 & 194 \end{bmatrix}$$

(a)

2	2	9	8	2	6	3	6
7	2	0	0	0	0	8	3
9	1	3	0	4	0	1	1
2	6	3	0	7	2	4	2
9	3	0	6	3	6	7	2
5	5	3	7	7	0	5	2
5	1	0	7	5	8	0	5
2	0	5	5	9	7	6	6

(b)

Fig.4 (a) 8x8 matrix of Lena (b) 8x8 matrix



(a)

$$\begin{bmatrix} 8069 & 3938 & 4523 & 6516 & 7316 & 5731 & 6692 & 5324 \\ 8066 & 3936 & 4524 & 6505 & 7297 & 5722 & 6692 & 5320 \\ 8056 & 3931 & 4523 & 6476 & 7265 & 5692 & 6680 & 5304 \\ 8057 & 3931 & 4531 & 6461 & 7238 & 5674 & 6678 & 5296 \\ 8025 & 3915 & 4517 & 6436 & 7203 & 5651 & 6655 & 5278 \\ 8023 & 3913 & 4508 & 6428 & 7201 & 5645 & 6652 & 5272 \\ 8003 & 3901 & 4498 & 6432 & 7202 & 5652 & 6634 & 5268 \\ 7992 & 3898 & 4486 & 6424 & 7196 & 5646 & 6630 & 5261 \end{bmatrix}$$

(b)

Fig.5 (a) Watermarked Image
(b) 8x8 matrix of Fig.5(a)

Figure 5 (a) shows that watermarked Lena image and (b) shows 8x8 matrix of watermarked the image. Figure. 5(b)is the output of the product of two matrices shown in image Figure 4 (a) and (b). The change in pixel values that shows embedment of Random matrix to Lena image.

5. CONCLUSION

A new kind of approach of digital watermarking process based on embedding the random matrix is presented in this paper. The experimental part has been used random matrix as a watermark to prevent an attacker for easy attack on the watermarked image. The important rationality for this is each image usually has different matrix form with array from 0 to 10.

The obtrusive part of this work is the use of random matrix conversion to authenticated user can detect and extract watermark from watermarked image.

REFERENCES:

1. D. L. Bhaskari, P. S. Avadhani, and M. Viswanath, “A Layered Approach for Watermarking In Images Based On Huffman Coding,” *International Journal on Computer Science and*

Engineering, vol. 02, no. 02, pp. 149–154, 2010.

2. I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital watermarking and Steganography*, Second Edi. Morgan Kaufmann Publishers, Elsevier, 2008.

3. H. Kostopoulos, S. Kandiliotis, I. Kostopoulos, and M. Xenos, "A Digital Image Watermarking Technique Using Modulated Pascal' S Triangles," *International Conference Signal Processing, Pattern Recognition & Applications*, pp. 82–86, 2003.

4. D. LalithaBhaskari, P. S. Avadhani, A. Damodaram,"Watermark Insertion Algorithm Implementation UsingAuxiliary Carry And LSB methods", proc. Int.conference onSystemics, cybernatics and Informatics, Jan 3-5,2006,Hyderabad, India, pp 666-668.

5. J.-L. Liu, D.-C.Lou, M.-C.Chang, and H.-K. Tso, "A robust watermarking scheme using self-reference image," *Computer Standards &Interfaces*,Elsevier, vol. 28, no. 3, pp. 356–367, Jan. 2006

6. S. Radharani and M. L. Valarmathi, "A Study on Watermarking Schemes for Image Authentication," *International Journal of Computer Applications*, vol. 2, no. 4, pp. 24–32, May 2010

7. M. Wu and B. Liu, "Attacks on digital watermarks," *Conference Record of the Thirty-Third Asilomar Conference on Signals, Systems, and Computers (Cat. No.CH37020)*, vol. 2, pp. 1508–1512.

8. X. Wu and Zhi-Hong Guan, "A novel digital watermark algorithm based on chaotic maps," *Physics Letters A, Elsevier*, vol. 365, no. 5–6, pp. 403–406, Jun. 2007.