

The Secure Watermarking of Digital Color Images by Using a Combination of Chaotic Mapping

P. Gopi Krishna^{#1}, D.Yasodha Rani^{*2}, G. Niharika^{*3}, B. Vardhani^{*4}, CH. Mohana Ramya^{*5}

#Assistant Professor, Department of Electronics and Communication Engineering, Vignan's Institute of Engineering for women, Visakhapatnam, Andhra Pradesh, India.

Abstract -(We live in) / (This is) a digital era where fast flowing development in computer networks and data editing programs is seen. In content to transferring data or investigating data identity, the data can run into few difficulties like manipulation of data, illegal copying of data, and distribution of digital documents. A Watermarking technique can be used to protect the digital data from such data manipulations. It is a process of hiding digital information in carrier signal which is typically used to identify the ownership of copyright of such signal and includes Logistic Chaos mapping. Here the carrier signal can be any digital information like an image or text. The reason behind the usage chaotic mapping is to increase security and the key length of protection which is a new approach appended to LSB technique with problem formulations like PSNR and BER.

Key Words: Watermarking, Chaotic mapping, PSNR, BER

1. INTRODUCTION

The major application of watermarking technique is in military purposes especially while a signal or a message is to be sent. The message can be image or video or audio. Finally the message is invisibly watermarked and the receiver has to find the hidden information to extract it and separate it from original message so that it can conclude receiving correct message from a correct person. The other use of watermarking technique is to provide copyrights to digital data.

The process of digital watermarking technique is to embed a watermark or logo into the original host image by applying watermarking algorithms onto to the host images. The watermark embedding is a simple usage of watermarking insertion algorithm into a host image to form watermarked image. Whereas watermark extraction process is retrieving the inserted watermark from the watermarked image so that original image and watermark are separated. But, extraction is possible only when the watermarking process is reversible. If the watermark embedded is irreversible, then extraction of the embedded watermark is impossible [1].

1.1 Digital Image Watermarking

In digital image watermarking system, in order to generate watermark image the information carrying image (logo image) is embedded into an original image (host image). After generating the watermarked image, that image is processed and then decoded at the receiver size in order to obtain the host image (original image) [4].

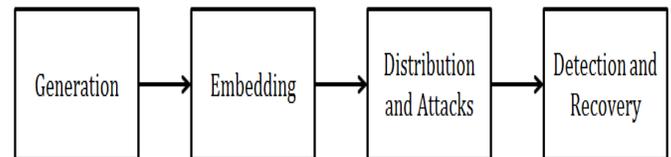


Figure 1.1(a): Basic Model of Watermarking

1.2 Applications of Digital Image Watermarking

- Copyright Protection
- Digital right management
- Tamper Proofing
- Broadcast monitoring
- Fingerprinting
- Access control
- Medical applications
- Image and content authentication
- Media forensics

1.3 Watermarking Techniques

Depending upon the domain in which the watermark is embedded, they are classified into spatial and frequency domain techniques.

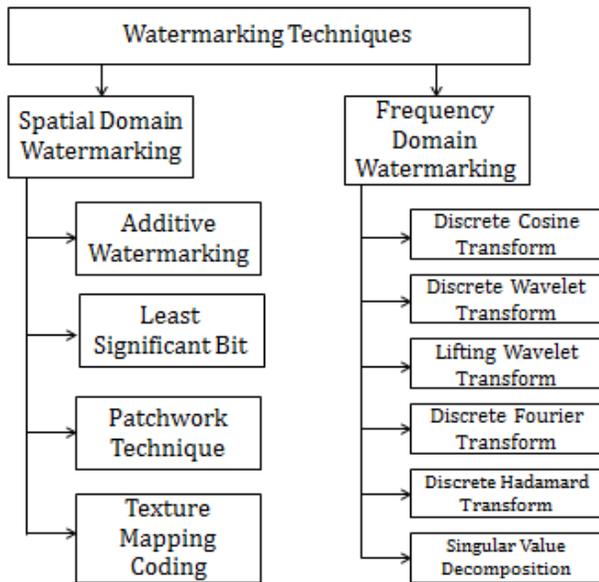


Figure 1.3(a): Different Watermarking Techniques

Spatial Domain: Here, the information can be added by varying the values of the pixel of the carrier signal. The values of color or the intensities of some selected pixels are directly modified by this technique. This technique is not robust against various attacks. The various spatial domain techniques are Additive Watermarking, Least Significant Bit, Patchwork and Text mapping coding etc. This technique is less tedious when compared to frequency domain techniques or wavelet [3].

Frequency Domain: This domain inserts a message by changing the transform coefficients of the cover message rather than the pixel values. Ideally, it has the impact in the spatial domain of allotting the concealed data through various order bits in a way that is robust. There are present a number of transforms (Discrete Cosine, Discrete Fourier, Discrete Wavelet Transforms) which can be applied to digital images.

1.4 Least Significant Bit

The most straight forward method to implement is LSB technique. In this process watermark bit is added to each pixel of the LSB. During extraction or detection method, the last bit of every pixel is read. In this technique, regardless of the possibility that the watermarked image is cropped the recipient can even get the required information since the information is inserted number of times. This method cannot be utilized for practical purposes as it is very sensitive to noise. It is not very robust [2].

1.5 Chaotic Mapping

Chaotic maps are used for image encryption which involves feature like non deterministic, random, periodicity etc. In the proposed method, the logistic mapping is used. The advantages of this mapping can be quick speed to produce a chaotic sequence [4] [5]. The purpose of using this mapping at different values in the permutations process is increasing security and key's length.

$$X_{n+1} = \lambda * x_n * (1 - x_n)$$

Where x takes values in the interval (0, 1)

'λ' is the control parameter and its value is between zero and four.

2. SOFTWARE REQUIREMENT

MATLAB installation is required. MATLAB can be used quite extensively. Some of its applications include signal and image processing, communication, control design, financial modeling and analysis, computational biology, and test and measurement. MATLAB also provides add-on toolboxes which are basically a collection of special purpose functions, which extends special environment to solve problems included in a particular class of applications.

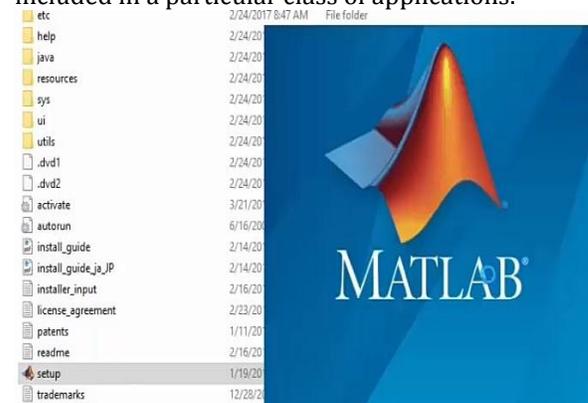


Figure 2(a): Installation of MATLAB

3. IMPLEMENTATION

3.1 Proposed Algorithm

The Insertion algorithm steps are as follows:

1. Host image is received from the input.
2. Three different logos are received from input.
3. The cover image is divided into RGB bands.
4. From existing bands, R, G and B bands are selected.
5. A logistic chaotic mapping is applied on the logos.
6. The bits of logo1, logo2, and logo3 are inserted in least significant bit (LSB) of R, G, and B channel bits, respectively.

7. After inserting the last bit of logos, the opposite action of permutation logo is applied on the channel R, G and B.
8. Watermarked image is produced.

The extraction algorithm steps are as follow:

1. The watermark image is received from input.
2. The watermark image is divided into RGB bands.
3. From existing bands, R, G and B bands are selected.
4. Two selected bands are permutations by two logistic chaos mapping with different amount of data.
5. The bits of logo1, logo2, and logo3 are inserted in least significant bits (LSB) of R, G, and B channel bits, respectively.
6. After extracting, the last bit of both logos is produced.

3.2 Flowchart and Result

It describes the step by step procedure of Watermarking by Insertion and Extraction steps.

The flow chart of insertion steps in the proposed method:

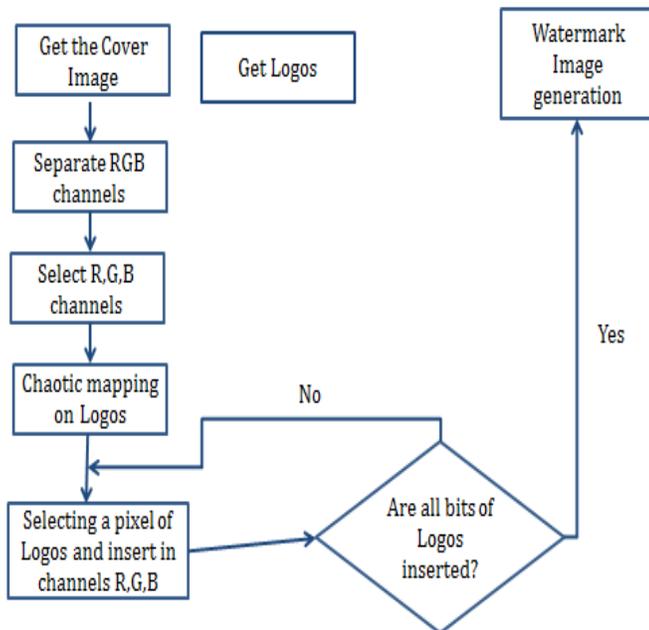


Figure 3.2(a): Insertion of Logos

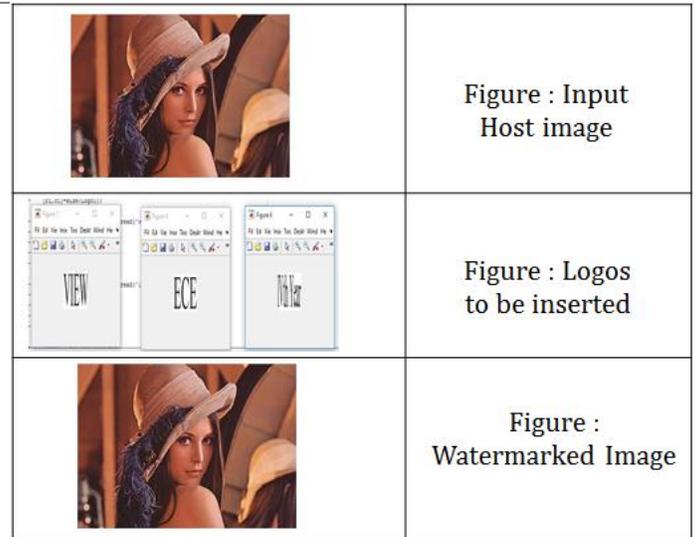


Figure 3.2(b): Output of Insertion

The flow chart of extraction steps in the proposed method:

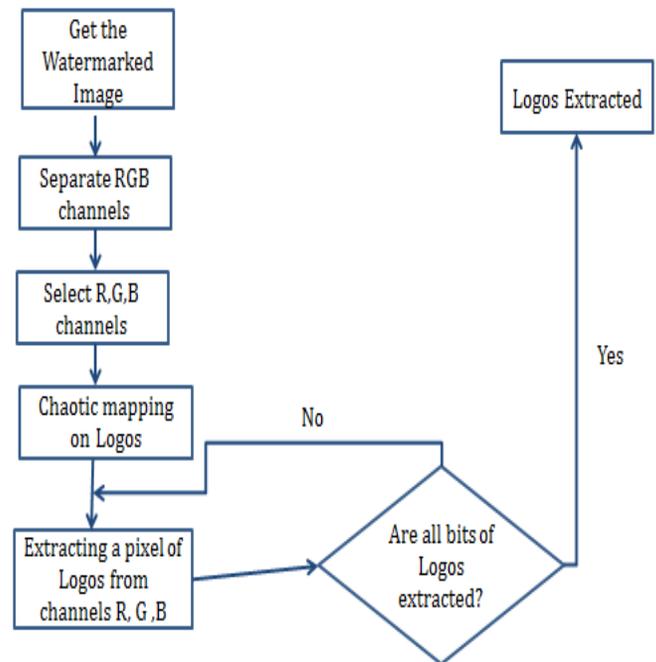


Figure 3.2(c): Extraction of Logos

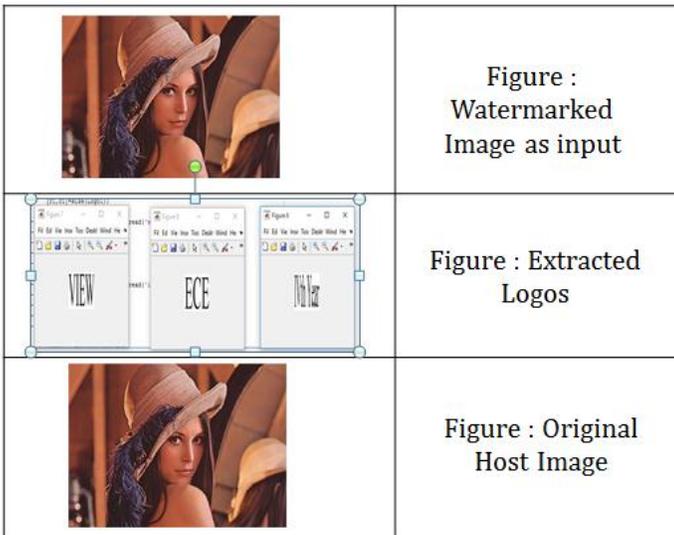


Figure 3.2(d): Output of Extraction

3.3 Evaluation

PSNR: The term PSNR referred as peak signal to noise ratio, this factor used to detect unobservable terms and it is also used to find the similarity between the watermarked images and Unwatermarked image.

$$PSNR = \frac{\sum(PSNR_i)}{3}$$

$$PSNR_i = 10 \log \left(\frac{M \times N \times \max([H(x,y,i)]^2)}{\sum_{x=1}^M \sum_{y=1}^N [H(x,y,i) - H'(x,y,i)]^2} \right)$$

PSNR_i show that PSNR of each color channel. H(x,y,i) and H'(x,y,i) indicates the amount pixel of the (x,y,i) and i index in the host and watermark images is equal to M×N.

	lina	peppers	F16
Cover Images			
PSNR	61.7406	60.8385	64.5554
	greens	Lake	House
Cover Images			
PSNR	57.7534	67.7403	61.9289

Figure 3.3(a): PSNR values

Bit Error Rate (BER): BER is used to compare the similarities between the original logos and extracted logos. This term mainly used to calculate the resistance factor.

$$BER = \frac{\sum_{x=1}^M \sum_{y=1}^N \sum_{z=1}^K |W(x,y) - W'(x,y)|}{M \times N \times K} \times 100$$

Where W(x,y) and W'(x,y) are the logos inserted image and logo extracted image.

If BER value approximately zero indicates a low error in the extraction process.

PSNR metric is higher and BER value is lower shows the system design with more success.

	lina	peppers	F16
Cover Images			
BER	0.000	0.000	0.000
	greens	Lake	House
Cover Images			
BER	0.000	0.000	0.000

Figure 3.3(b): BER values

4. CONCLUSION

With the increasing development of computer systems, security is considered more than ever. In some ways of improving security, chaos-based methods have been used for improving the level of security. Due to the high sensitivity of the chaotic mapping in alteration or changes, there are suitable for use in the security methods. The proposed test and comparing the proposed approach with other methods shows the high sensitivity and successful application of this method in the images. The proposed mapping in this paper also has high sensitivity and acceptable key length. The carried out tests on this mapping are evidence for this matter.

5. FUTURE SCOPE

High capacity is required for watermarking applications used for secure media distribution, thumbnail embedding and medical imaging. Therefore, the usability of proposed watermarking system for high capacity data embedding applications can be further investigated.

6. REFERENCES

- [1] Lei, B., Tan, E.-L., Chen, S., Ni, D., Wang, T., & Lei, H. (2014). Reversible watermarking scheme for medical image based on differential evolution. *Expert Systems with Applications*, 41(7), 3178- 3188 .
- [2] Bansal, N., Deolia, V. K., Bansal, A., & Pathak, P. (2014). Digital Image Watermarking Using Least Significant Bit Technique in Different Bit Positions. Paper presented at the Computational Intelligence and Communication Networks (CICN), 2014.
- [3] Moniruzzaman, M., Hawlader, M. A. K., & Hossain, M. F. (2014, May). An image fragile watermarking scheme based on chaotic system for image tamper detection. In *Informatics, Electronics & Vision (ICIEV), 2014 International Conference on* (pp. 1- 6). IEEE.
- [4] Munir, R. (2015, May). A chaos-based fragile watermarking method in spatial domain for image authentication. In *Intelligent Technology and Its Applications (ISITIA), 2015 International Seminar on* (pp. 227-232). IEEE.
- [5] Wu, X, & Guan, Z-H. (2007). A novel digital watermark algorithm based on chaotic maps. *Physics Letters A*, 365(5), 403-406
- [6] Xiao, D., & Shih, F. Y. (2012). An improved hierarchical fragile watermarking scheme using chaotic sequence sorting and subblock postprocessing. *Optics Communications*, 285(10), 2596-2606.
- [7] May, R. M. (1976). Simple mathematical models with very complicated dynamics. *Nature*, 261(15560), 459-467.
- [8] Caragata, D., El Assad, S., & Luduena, M. (2015). An improved fragile watermarking algorithm for JPEG images. *AEU-International Journal of Electronics and Communications*, 69(12), 1783- 1794.
- [9] Teng, L., Wang, X., & Wang, X. (2013). Cryptanalysis and improvement of a chaotic system based fragile watermarking scheme. *AEU International Journal of Electronics and Communications*, 67(6), 540-547.
- [10] Chang, C.-C., Chen, K.-N., Lee, C.-F., & Liu, L.-J. (2011). A secure fragile watermarking scheme based on chaos-and-hamming code. *Journal of Systems and Software*, 84(9), 1462-1470.