

## Text and Image Watermarking Using Random Significant Bit

Y. Pahadiya<sup>1\*</sup>, R. Khatri<sup>2</sup>

<sup>1\*</sup> Dept. of Cyber Security, VITM, Indore, India

<sup>2</sup> Dept. of Cyber Security, VITM, Indore, India

\*Corresponding Author: [amw.yasha@gmail.com](mailto:amw.yasha@gmail.com), Tel.: +91-8600180075

Available online at: [www.ijcseonline.org](http://www.ijcseonline.org)

Received: 21/Jan/2018, Revised: 29/Jan/2018, Accepted: 12/Feb/2018, Published: 28/Feb/2018

**Abstract:** Security of Multimedia is very challenging task in today because data move over Internet. Anyone can easily hack or misuse the data specially images. So hide data such as text document, images, and audio, video in to digital images. In this paper, we proposed random significant bit (RSB) method for text or image watermarking. Random significant bit method and least significant method implemented using java. Compare random significant bit method and Least Significant method on the basis of time. Found that random significant bit method take less time compare to Least Significant method.

**Keywords:** Information security, Image watermarking, Digital watermarking, LSB, RSB.

### I. INTRODUCTION

In generally digital watermarking is a technique for inserting information into an image. It is an evolving field that requires continuous effort to find the best possible method in protecting multimedia content. It is a process of embedding information into digital multimedia content such that the information can later be extracted or detected for variety of purposes including identification and authentication.

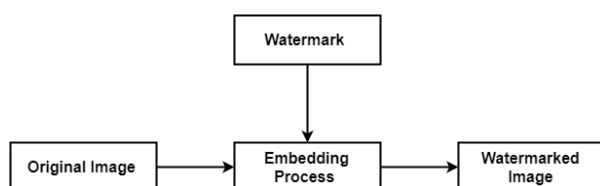


Figure1: Watermarking digital image Work

Watermarks and watermarking techniques can be classified into several categories taking into account by this various criteria [2]. As it can be noted, one of the criteria is *embedding domain* in which the watermarking is implemented. For example, watermarking can be done in the spatial domain. An alternative possibility is the watermarking in the frequency domain.

Watermarking techniques can be classified into the following four categories according to the type of the multimedia document to be watermarked:

- Image Watermarking
- Video Watermarking
- Audio Watermarking
- Text Watermarking.

According to the human perception, digital watermarks can be classified into three different categories, as follows:

- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark
- Dual watermark.

Watermarks and watermarking techniques can be divided into various categories in various ways. The watermarks can be applied in spatial domain. An alternative to spatial domain watermarking is frequency domain watermarking. It has been pointed out that the frequency domain methods are more robust than the spatial domain techniques. Different types of watermarks are shown in the figure:

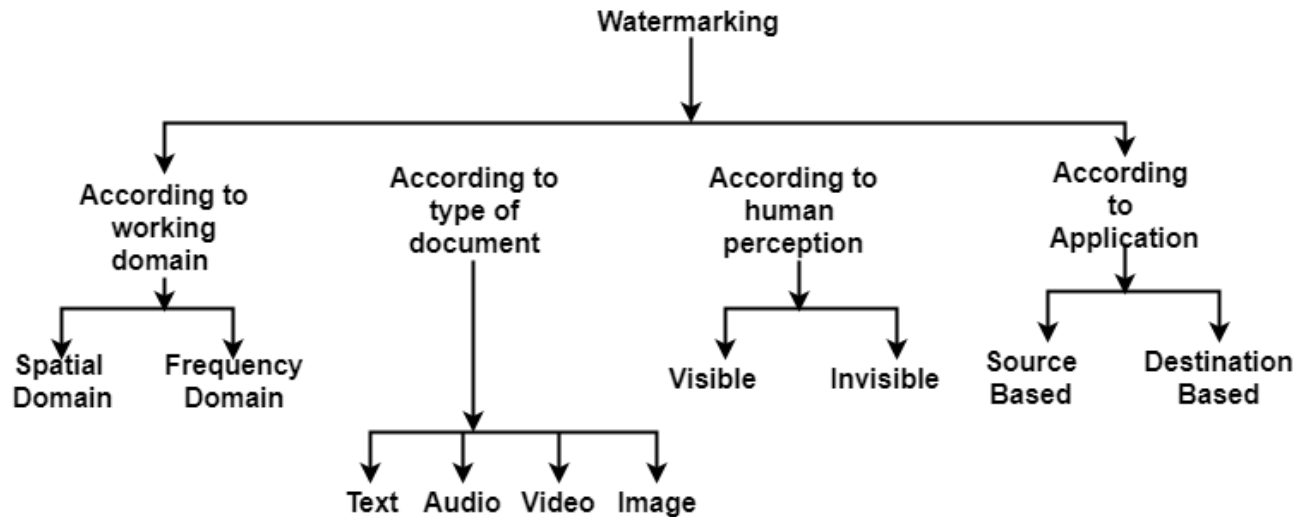


Figure2: Types of Watermarking

Rest of the paper is organized in the following manner, Section I contains all the introductory requirements to understand the research area. It also provides the detailed explanation about image watermarking, Section II presents literature survey on watermarking techniques available with this domains, In Section III we studied wide variety of existing mechanism, algorithms and architectures, In section IV we present our proposed work and algorithm, Section V result analysis shows the calculated result by our proposed algorithm and also compared with existing algorithms, last section VI we conclude the work done by us.

## II. RELATED WORK

The existing watermarking techniques can be classified as either to be object space based or frequency space based approaches. While the object space approaches embed the information by modifying the original data directly, the frequency domain approaches transform the original data into frequency domain first and embed watermarks there. Till very recent, researches on watermarking have been mainly focused on the digital media such as text, image, sound and video [2]. The first attempt to introduce the watermarking technology into the computer graphics world was probably made by R. Ohbuchi. et al.[3,4].

Benedens[5] presented another object space based method through altering the normal vectors calculated from the

surface geometry of a 3D model. He demonstrated the robustness of the method against the simplification attacks.

On the other hand, Kanai et al.[6] proposed a frequency space based approach by using wavelet transform and multi resolution representation of polygon models. Watermarks are embedded in the wavelet coefficient vectors and are

imperceptible and invariant to the affine transform. However, the application of the method is limited to those triangle meshes whose mesh topology fits into a 4-to-i subdivision connectivity scheme.

The method developed by E. Praum et al.[7] also based on multi-resolution representation, but can be applied to arbitrary triangle meshes. This is realized by constructing a set of scalar basis function over mesh vertices. Watermarks are embedded in the model by perturbing the vertices along the direction of surface normal, weighted by the basis functions. They also suggest making watermarks survival from simplification by re-sampling an attacked mesh using the original mesh connectivity.

## III. EXISTING SYSTEM

In the existing method, pixel values of cover image and watermark image are converted into binary. The cover image is of size  $m \times n$  and the watermark image is of size  $(m \times n)/8$ . The 8<sup>th</sup> bit of each pixel of cover image is replaced by the each bit of watermark image. In this way watermark is embedded and watermarked image is obtained.

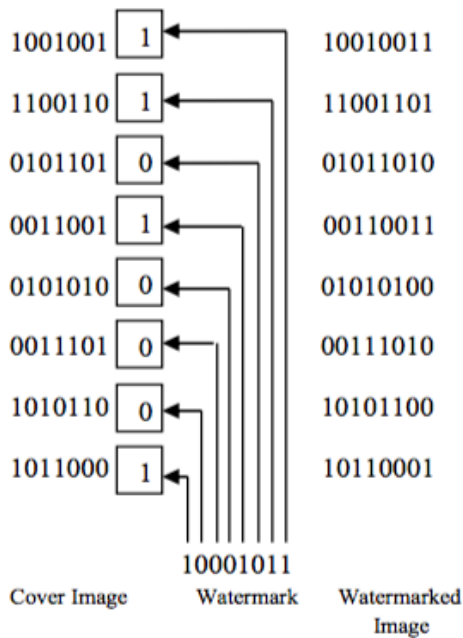


Figure3: Least Significant Bit Method for Watermarking

**IV. PROPOSED SYSTEM**

A complete digital watermarking system consists of 2 basic modules: watermark embedding module and watermark detection and extraction module. Watermark embedding module is answerable for adding the watermark signal to the initial knowledge.

The block diagram of the watermarking system is shown in below figures.

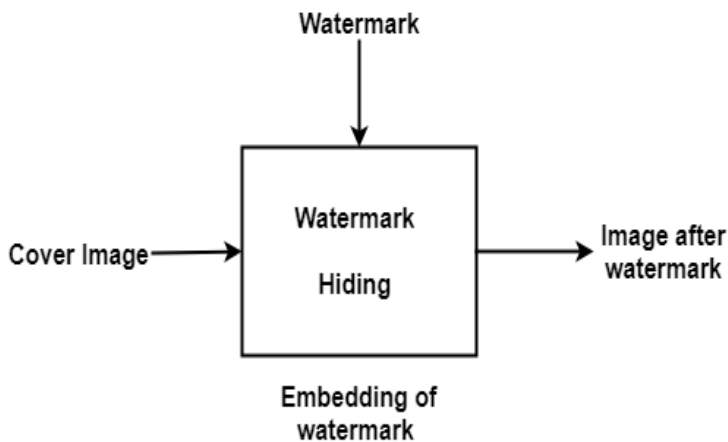


Figure 4: Detection Module of Watermark

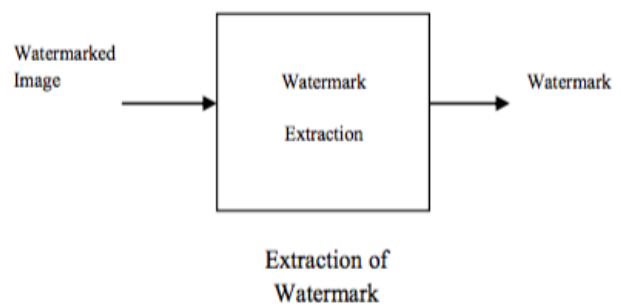


Figure 5: Extraction Module of Watermark

**V. RESULT ANALYSIS**

Water marking is developed in this research with help Java (JDK1.8) and Net Beans IDE8.02 on window operating system. All forms of water marking design in Swing. Graph plotted for computation time and memory management using JFreeChart Library. In Result Analysis compare proposed system with existing system in term of computation time and memory.

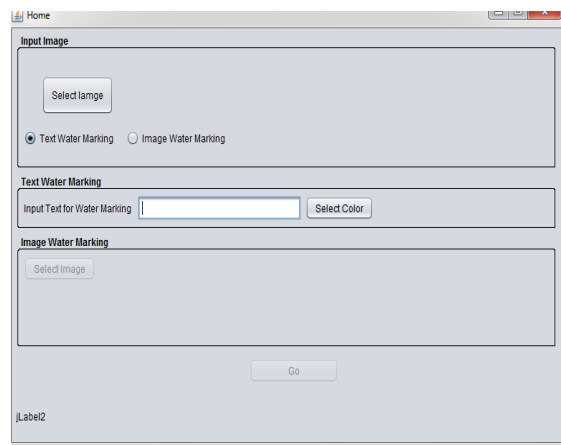


Figure 6: screen shot of random significant bit of watermarking

Table1: Time Comparison between Least significant bit and random significant bit

	<b>LSB</b>	<b>RSB</b>
Image-1	4.3	2.4
Image-2	6.5	4.4
Image-3	3.5	1.8
Image-4	4.5	2.8

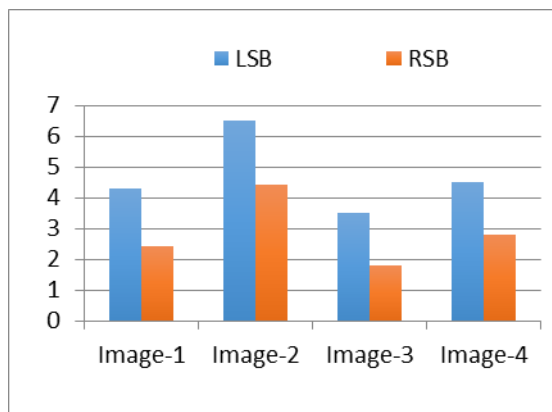


Figure 7: Time Comparison between Least significant bit and random significant bit

## VI. CONCLUSION

A technique within which a watermark is generated employing an m-sequence generator. The watermark was embedded to the random vital bit (LSBs) of the initial image to supply the watermarked image. The watermark was extracted from a suspected image by taking the random vital bits at the correct locations. Detection was performed by a cross-correlation of the initial and extracted watermark. They showed that the ensuing image contained AN invisible watermark with easy extraction procedures. However the watermark wasn't sturdy to additive noise. The proposed algorithm work well as compare to existing algorithms.

## REFERENCES

- [1] C.Y. Chang and S.J. Su, "The Application of a Full Counter propagation Neural Network to Image Watermarking", Conference on Networking, Sensing and Control IEEE, March 2005.
- [2] Wai C. Chu, "DCT-Based Image Watermarking Using Subsampling", IEEE Trans. on multimedia, vol. 5, no. 1, pp.34-38, March 2003.
- [3] Gurpreet Kaur and Kamaljeet kaur, "Image Watermarking Using LSB(Least Significant Bit)", in Proc. of International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 4, April 2013, pp. 858-861.
- [4] Maher EL'ARBI, Chokri BEN AMAR and Henri NICOLAS, "Video Watermarking Based On Neural Networks", IEEE Proc. of ICME, pp. 1577-1580, 2006.
- [5] F.M. Boland , J.J.K. O'Ruanaidh , C. Dautzenberg, "Watermarking digital images for copyright protection", Fifth International Conference on Image Processing and its Applications, pp. 250 – 256, August 1996.
- [6] Martin F. H. Schuurmans., "Keynote Speech III Digital Watermarking", 15th International Conference on VLSI Design. Proceedings, August 2002.
- [7] Yogesh Jadav, "Comparison of LSB and Sub band DCT Technique for Image Watermarking," in Proc. of Conference on Advances in

Communication and Control Systems (CAC2S 2013), pp. 398-401, 2013.

- [8] M. D. Swanson, M. Kobayashi and A. H. Tewfik, "Multimedia data-embedding and watermarking techniques", Proc. of IEEE, vol. 86, no. 6, pp. 1064-1087, 1998.
- [9] Zhang Zhi-Ming, Li Rang-Yan, Wang Lei, "Adaptive Watermark Scheme with RBF Neural Networks," International Conference on Neural Networks and Signal Processing, pp. 1517-1520, Dec 2003.
- [10] J.W Bae, S.H. Lee and J.S. Yoo "an efficient wavelet based motion estimation algorithm", IEEE Trans. INF & SYST, vol. E88-D, no. 1, January 2005.
- [11] Puneet Kr Sharma and Rajni, "Information security through Image Watermarking using Least Significant Bit Algorithm," Computer Science & Information Technology, vol. 2, no. 2, pp. 61-67, May 2012.
- [12] Malihe Soleimani, Faezeh Sanaei Nezhad, Hadi Mahdipour and Morteza Khademi, "A Robust Digital Blind Image Watermarking Based on Spread Spectrum in DCT Domain," Science Academy Transactions on Computer and Communication Network, vol. 2, no. 2, pp. 122-126, June 2012.
- [13] Thanuja T C, P Nagaraju, Vinay J, Kavaya N Bhushan and Naren S Vasanaad, "Hardware Implementation of a Robust Modulo Watermarking Algorithm," ME Journal of Technology and Management, vol. 2, no. 1, pp. 51-56, 2011.
- [14] S. Craver, N. Memon, "Resolving Rightful Ownership with Invisible Watermarking Techniques: Limitations, Attacks and Implications", IEEE Journal on Selected Areas in Communications, vol 16, no. 4, pp. 573-586, 1998.

## Authors Profile

**Yasha Pahadiya** pursued Bachelor of Engineering from University Rajiv Gandhi Prodyogiki Vishwavidyalay Bhopal in 2014. she is currently pursuing Master of Technolology Department of Cyber Security from Vikrant Institute of Technology & Management Indore, since 2014. Her main research work focuses on security Algorithms, internet computing, watermarking.



**Mr. Ravi Khatri** currently working as Associate Professor at Vikrant Institute of Technology & Management Indore and member of IACSIT and ISTE and having 20 research paper and main research area IOT and collaborative Computing He has 8 years of teaching experience.

