



# INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume3, Issue3)

Available online at [www.ijariit.com](http://www.ijariit.com)

## Designing and Performance Evaluation of a 3-Level Watermarking Based On Encryption and Compression

**Kirtika Gupta**

M.Tech Scholar, CSE Deptt.

GGSIPIU, Delhi

[gupta.kirtika16@gmail.com](mailto:gupta.kirtika16@gmail.com)

**C. S. Rai**

Prof., CSE Deptt.

GGSIPIU, Delhi

[csrai@ipu.ac.in](mailto:csrai@ipu.ac.in)

**Abstract:** As the mobile handheld gadgets geared up with fingerprint sensors, it turns out to be important to protect the private records of a user (i.e., fingerprint image) in the remote applications. Virtual image watermarking is the process of hiding statistics in any shape (text, image, audio, and video) in the original image without degrading its visual quality. Watermarking is carried out for copyright protection of the authentic records. In this work, we have introduced a new concept with current gray-scale image watermarking strategies. The novelty of the method is that first, we have compressed the cover image with the usage of wavelet compression method before going for the encryption of the same. After that, we have encrypted the cover and watermark image that is based on random key array generation, the usage of consumer key, a few constants and fixed operations. The mixture of all 3 steps collectively made the proposed approach extra robust and more secure in term of watermarking as compression itself is pretty endorsed for facts transfer and information protection. Also, the watermark is extracted with the reverse application of the same steps. Some output parameters are also calculated to reveal the accuracy and robustness of proposed method. Those parameters are Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and a Correlation value between unique watermark image and extracted watermark image. The PSNR, MSE and Correlation values imply that the visual similarity of the signed and attached images is right. Additionally, we've computed the behavior by clubbing the same watermark with different Cover images in terms of MSE, PSNR and Correlation Value and analyze the difference between authentic watermark and extracted watermark. The embedding algorithm is robust against common image processing operations. It is concluded that proposed algorithm is agreeably optimized, robust and show the development of different comparable said strategies.

**Keywords:** Watermarking, Wavelet Compression, Encryption, MSE, PSNR.

### I. INTRODUCTION

As technology increases in the field of medicine, imaging techniques due to teleradiology, telepathy became more popular nowadays. For teleradiology, it requires highly truthiness in image processing system. In this case, watermarking plays an important role in the field of image, audio and video security. Watermarking system covers image in such a way that it can be retrieved for a variety of purposes in future [1]. As for clinical diagnosis, treatment, research, education and other commercial/non-commercial applications, both for private and government organizations, the medical information is very important.

#### A. IMPORTANT PARAMETERS IN WATERMARKING SYSTEMS

There are a lot of parameters and variables in digital watermarking systems, the most important ones are listed here:

1. **Quantum of information embedded:** It is calculated by the definite application and it directly influences the strength of the system. More the information is given, less robust the watermarking will be. In the case of medical images, insertion of more information may destroy the originality of the image.
2. **Watermark intensity:** It is known as the power of the embedded watermark. To enhance the robustness, one may increase this parameter, but at the cost of the deprivation of original image.

3. **Size of watermark:** The larger size of watermark make the system robust. Watermark that is too small tend to have small value in the real application. In medical images system, hospital sign or patient information is embedded, it should not be too large or too small such that the size should not spoil the quality or security of the medical data.
4. **Control information:** As there is nothing to do with the invisibility or robustness of the watermarking system, the control information plays an important role in system security [2].

#### **B. NEED OF MEDICAL IMAGE WATERMARKING**

Medical images have their own requirements when they are used for watermarking. The following requirements are listed below

1. **Imperceptibility:** Imperceptibility shows that watermark in the image must be invisible to the human eye. It is often not permitted to cut the image contents even one bit of information. The need of imperceptibility can be completed by two methods: RONI watermarking and Reversible watermarking.
2. **Robustness:** In telemedicine atmosphere, medical images may pass through many services and receive several processing and annotations, therefore images are normally watermarked with identification codes of physicians who created images in order to authenticate the images.
3. **Capacity:** In watermarking of images, all the data necessary for physicians such as recognition of patient, diagnosis report, and original identification are embedded. This data further enhanced when the image is sent to another physician for the second opinion. Therefore, capacity for hiding the payload must be high.
4. **Authenticity:** Only listed users should have access to the information. The listed users are the patients, HIS (Hospital Information System) personnel, and concerned staff. Special keys are used for this aim to retrieve the original data.
5. **Reversibility:** The allowed user should be able to reverse the hiding process to decipher the information from the image. This gives the un-watermarked real image to the user which can further use it for making a diagnosis.
6. **Intactness of ROI:** In the case of a medical image, the image comprises of the region of interest (ROI) and region of non-interest (RONI). ROI have the important data on which some decision is made. Therefore it is necessary that the watermarking process should not affect the ROI adversely. Distorted ROI will give the wrong diagnosis. This problem is solved by embedding the watermark information in RONI, thereby keeping ROI intact [2].

## **II. METHODOLOGY STEPS**

### **A. Hiding of watermark behind cover image**

1. Inputting of cover image
2. Conversion of colored cover image into gray image
3. Display of gray scale cover image
4. Application of wavelet-based compression on grayscale cover image
5. Inputting of an encryption key to encrypt cover image
6. Encryption of cover image based on random key array generation using user key, some constants, and fixed operations
7. Display of encrypted cover image
8. Display of encrypted watermark
9. Inputting of watermark image
10. Conversion of colored image into binary image
11. Resizing of watermark image according to the size of cover image
12. Display of binary watermark image
13. Encryption of binary watermark image based on random key array generation using user key, some constants, and fixed operations
14. Display of encrypted watermark image
15. Hiding of watermark image behind cover image by addition of encrypted watermark image and encrypted compressed cover image
16. Generation of a random matrix according to the size of watermarked image
17. Addition of generated random matrix to the watermarked image
18. Conversion of newly combined matrix into binary one
19. Display of watermarked image.

### **B. Extraction and decryption of watermark**

20. Recovery of encrypted watermark image from watermarked image by subtracting the generated random matrix from watermarked image
21. Display of recovered encrypted watermark image
22. Inputting of a decryption user key to decrypt watermark image
23. Decryption of watermark image based on random key array generation using user key, some constants, and fixed operations

24. Application of morphological operation on decrypted watermark image
25. Display of extracted watermark image
26. Calculation of output parameters i.e. MSE, PSNR and correlation value between original watermark image and extracted watermark image.

### III. EXPERIMENTAL RESULTS

MATLAB 2013a is used as an implementation platform. Generalized MATLAB toolbox and image processing toolbox are used for implementation. In this work, we have added a brand new idea with present grayscale image watermarking techniques. The novelty of the work is that we've got first compressed the cover image with the use of wavelet approach before going for the encryption of the same. After we've encrypted the cover and watermark image that's based totally on random key array era the use of user key, a few constants, and fixed operations. The mixture of all three steps together makes the proposed approach greater strong and extra comfy in the time period of watermarking as compression itself is tremendously endorsed for records transfer and statistics security. Additionally, the watermark is extracted by the usage of the same steps in reverse order. The snapshots of every step are given below. We have used a watermark 'test.bmp' for our work. This watermark is used with 3 distinctive general cover images i.e. 'Lena.bmp', 'Cameraman.bmp' and 'Baboon.bmp'. The image of every step of proposed technique is taken and shown below best for cover image Lena.bmp. For rest two cover image, we've best-proven cover image, unique watermark and extracted watermark (as shown in Table 1). Also, few output parameters are also calculated to show the accuracy and robustness of proposed method. Those parameters are implied Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Correlation price between authentic watermark image and extracted watermark image. The PSNR, MSE and Correlation values indicate that the visual exceptional of the extracted watermark images is almost identical. The output parameter PSNR is extensively used to measure imperceptibility among the unique watermark and extracted watermark image. PSNR is described by means of the eqn. (1). The mistake among the original watermark and extracted watermark is evaluated via using MSE given by the eqn. (2). The similarity between the authentic watermark and extracted watermark image is evaluated via the usage of NC (Normalized Correlation) given through the eqn. (3).

$$PSNR = 10 \log_{10}(255^2/MSE) \tag{1}$$

Where,

$$MSE = \frac{1}{M \times N} \sum_{m=1}^M \sum_{n=1}^N [(m, n) - w(m, n)]^2 \tag{2}$$

$$NC = \frac{\sum_i \sum_j w(i, j) w'(i, j)}{\sum_i \sum_j |w(i, j)|^2} \tag{3}$$

These three parameters are calculated by comparing original watermark image and extracted watermark image. Figure no. 1 is the snapshot of the cover image. Figure no. 2 is the snapshot of the compressed cover image. Figure no. 3 is the snapshot of the encrypted compressed image. Figure no. 4 is the snapshot of original watermark image. Figure no. 5 is the snapshot of encrypted watermark image. Figure no. 6 is the snapshot of watermarked image i.e. watermark image is hidden behind cover image. Figure no. 7 is the snapshot of extracted encrypted watermark image. Figure no. 8 is the snapshot of decrypted watermark image. The embedding algorithm is robust against common image processing operations. It is concluded that the embedding and extraction of the proposed algorithm are well optimized, robust and show an improvement over other similar reported methods.



Figure 1 snapshot of cover image

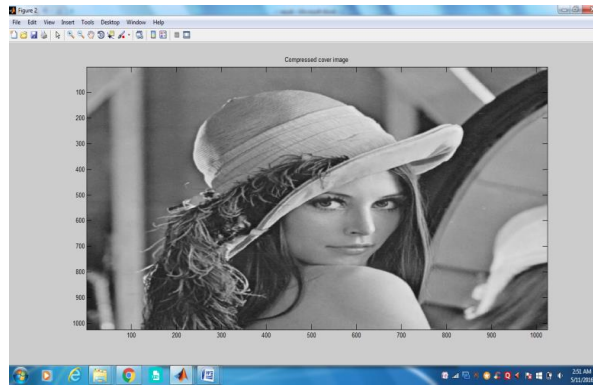


Figure 2 snapshot of compressed cover image

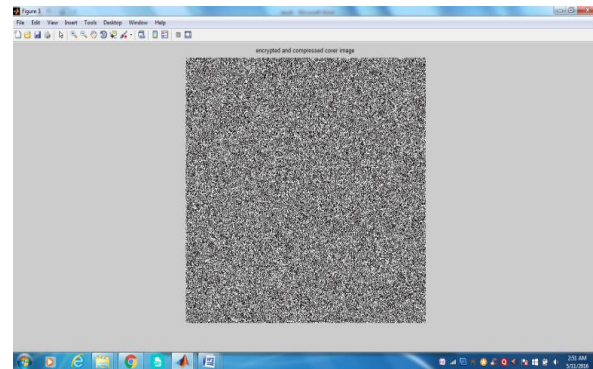


Figure 3 snapshot of encrypted compressed image



Figure 4 snapshot of original watermark image

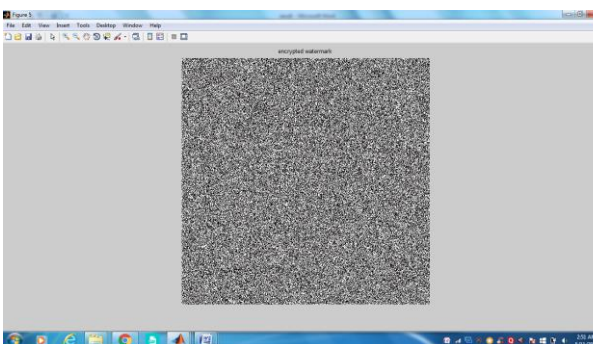








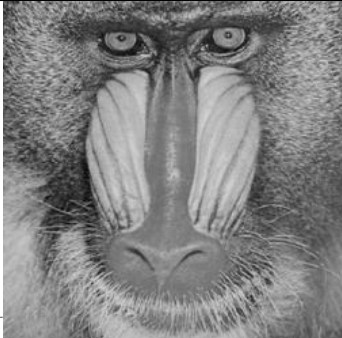


Figure 5 snapshot of encrypted watermark image



Table 1  
Comparative analysis of MSE, PSNR and Correlation Value for Watermark (test.bmp)

S. No.	Original Watermark	Extracted Watermark	Cover Image	MSE	PSNR	Correlation Value
1.			 Lena.bmp	0.024	64.3	0.9440
2.	 test.bmp		 Cameraman.bmp	0.096	58.28	0.803
3.	 test.bmp		 Baboon.bmp	0.048	61.28	0.892

### CONCLUSION AND FUTURE WORK

For the protection of copyright in case of a digital image, many digital watermarking strategies had been proposed. An image watermark is the invisible image signal which may be inserted into digital media. This virtual media could be very imperceptible to a person, but it could be detected by laptop. The insertion of the watermark does not disturb the visual quality of cover image also, it is a proof against some traditional sign processing operations, along with cropping, resizing and lossy JPEG compression. In this paper, we conclude our dialogue on a watermarking system with compressed/encrypted layout. As the virtual content is regularly disbursed, the watermarking procedure is carried out within the compressed/encrypted form. As a result, the layout in which encryption is done is of great effect, considering there may be a courting between the efficiency of compression and safety of the watermarked content material. In this work, we have implemented an advanced grayscale picture watermarking scheme with the use of compression and encryption technique. The proposed approach is pretty strong and efficient in terms of securing the image information. The evidence of above assertion is the fee of MSE, PSNR and Correlation value. Those values are plenty stepped forward in comparison from that of different existing watermarking strategies. Also, we conclude that equal watermark behave otherwise with extraordinary cover images as MSE, PSNR and Correlation value among unique watermark and extracted watermark is a great deal one of a kind. Further, this approach can be extended by incorporating RGB image and updating the technique for the equal. This will take the RGB image watermarking up to an extraordinary height.

### REFERENCES

- [1] Rasha Thabit, BeeEeKhoo, "A new robust lossless data hiding scheme and its application to color medical images"  
[www.elsevier.com/locate/dsp](http://www.elsevier.com/locate/dsp).
- [2] Praveen Kumar E, Remya Elizabeth Philip, Sunil Kumar P, Sumithra M G, "DWT-SVD Based Reversible Watermarking

- Algorithm for Embedding the Secret Data in Medical Images” IEEE – 31661
- [3] Praful Saxena, Shanon Garg and Arpita Srivastava, “DWT-SVD Semi-Blind Image Watermarking Using High-Frequency Band” 2nd International Conference on Computer Science and Information Technology (ICCSIT'2012) Singapore April 28-29, 2012
- [4] Sudeb Das, Malay Kumar Kundu, “Effective management of medical information through ROI-lossless fragile image watermarking technique” *computer methods and programs in biomedicine* 111 (2013) 662–675
- [5] SHANG Yv-fan and KANG Yi-ning, “Medical Images Watermarking Algorithm Based on Improved DCT” *Journal of Multimedia*, vol. 8, no. 6, December 2013