

# Watermarking Text and Image with Encryption

Karan Singh Rajawat<sup>1</sup>, Deepak Chaudhary<sup>2</sup> Dr. Amit Kumar<sup>3</sup>

<sup>1</sup>M.Tech Student IET College, Alwar, Raj, India, <sup>2</sup>Assistant Prof. <sup>3</sup>Associate Prof IET College Alwar, raj, India  
Email: karan.rajawat@gmail.com deeapk.se17@gmail.com amitpanwar889@gmail.com

**Abstract**— Watermarking is a very active research field with a lot of applications. Although it is a relatively new field, it has produced important algorithms for hiding messages into digital signals. This work presents a new method that combines image as well as text into the image with encryption technique for safe transmission purpose. This method is based on the combination of key with watermarking. During the insertion encryption key is applied to the image during the insertion of image as well as text. Then, this secret key is also useful when we extract the water mark from the embedded image. We have applied and showed the results of our method to different images.

**Index Terms**—water mark, bit, key, etc.

## 1 INTRODUCTION

Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. 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. The hiding process has to be such that the modifications of the media are imperceptible. For images, this means that the modifications of the pixel values have to be invisible. Furthermore, the watermark must be either robust or fragile, depending on the application. By "robust", we mean the capability of the watermark to resist manipulations of the media, such as lossy compression (where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, among others. In some cases, the watermark may need to be fragile. "Fragile" means that the watermark should not resist tampering, or would resist only up to a certain, predetermined extent.

The example below illustrates how digital watermarking can hide information in a totally invisible way. The original image is on the left; the watermarked image is on the right and contains the name of the author.

Digital watermarks can be largely divided into fragile watermarking and robust watermarking. Fragile watermarking is mainly used for protecting data that cannot be copied, but some problems remain to be solved such as methods for data build-in and authentication, and the types of data to be inserted for data authentication. The protection of a fragile watermark can be guaranteed by maintaining security either by the insertion method or Data-Hiding Method using Digital Watermark in the Public Multimedia Network inserted data. Robust watermarking emphasizes the robustness of the watermark information built into the digital image. Thus, the extraction of ownership information should be possible even from intentional or unintentional image transformation and lossy compression [5, 6]. As such, robust watermarking is mainly used for the ownership protection of multimedia contents.



Figure 1: Original Image

Figure 2: Watermarked Image

## METHODOLOGY

MATLAB stands for MATrix LABoratory and the software is built up around vectors and matrices. This makes the software particularly useful for linear algebra but MATLAB is also a great tool for solving algebraic and differential equations and for numerical integration. MATLAB has powerful graphic tools and can produce nice pictures in both 2D and 3D. It is also a programming language, and is one of the easiest programming languages for writing mathematical programs. MATLAB also has some tool boxes useful for signal processing, image processing, optimization, etc.

In the MATLAB workspace, most images are represented as two-dimensional arrays (matrices), in which each element of the matrix corresponds to a single pixel in the displayed image. For example, an image composed of 200 rows and 300 columns of different colored dots stored as a 200-by-300 matrix. Some images, such as RGB, require a three-dimensional array, where the first plane in the third dimension represents the red pixel intensities, the second plane represents the green pixel intensities, and the third plane represents the blue pixel intensities.

This convention makes working with graphics file format images similar to working with any other type of matrix data. For example, you can select a single pixel from an image matrix using normal matrix subscripting:

$$I(2,15)$$

This command returns the value of the pixel at row 2, column 15 of the image I.

## IMAGE SIZE

Image files tend to be large. We shall investigate the amount of information used in different image type of varying sizes. For example, suppose we consider a 512X512 binary image. The number of bit used in this image is

$$512 \times 512 \times 1 = 262,144 = 32768 \text{ bytes}$$

## OBJECTIVES

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, and video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.

Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications. A new watermarking scheme will developed to embedded text as well as image into the original image. The proposed scheme based on bit system with encryption algorithms. And reverse process for extraction the text and image from the watermarked image is discussed, after extract the text string and image compared with original image. For quantifying the error between images, like PSNR, SNR, and CRR. And some time embedded image effected by noise and due to this quality of the image degraded but this method is applicable for distortion and extracted exact string "text" and image, and check the quality of water mark image with original watermark image.

## WATERMARKING APPLICATIONS

The increasing amount of research on watermarking over the past decade has been largely driven by its important applications in digital copyrights management and protection. One of the first applications for watermarking was broadcast monitoring. It is often crucially important that we are able to track when a specific video is being broadcast by a TV station. This is important to advertising agencies that want to ensure that their commercials are getting the air time they paid for. Watermarking can be used for this purpose. Information used to identify individual videos could be embedded in the videos themselves using watermarking, making broadcast monitoring easier. Another very important application is owner identification. Being able to identify the owner of a specific digital work of art, such as a video or image can be quite difficult. Nevertheless, it is a very important task, especially in cases related to copyright infringement. So, instead of including copyright notices with every image or

song, we could use watermarking to embed the copyright in the image or the song itself.

## WATERMARKING PROPERTIES

Every watermarking system has some very important desirable properties. Some of these properties are often conflicting and we are often forced to accept some trade-offs between these properties depending on the application of the watermarking system. The first and perhaps most important property is effectiveness. This is the probability that the message in a watermarked image will be correctly detected. We ideally need this probability to be 1.

Another important property is the image fidelity. Watermarking is a process that alters an original image to add a message to it; therefore it inevitably affects the image's quality. We want to keep this degradation of the image's quality to a minimum, so no obvious difference in the image's fidelity can be noticed. The third property is the payload size. Every watermarked work is used to carry a message. The size of this message is often important as many systems require a relatively big payload to be embedded in a cover work. There are of course applications that only need a single bit to be embedded. The false positive rate is also very important to watermarking systems. This is the number of digital works that are identified to have a watermark embedded when in fact they have no watermark embedded. This should be kept very low for watermarking systems.

Lastly, robustness is crucial for most watermarking systems. There are many cases in which a watermarked work is altered during its lifetime, either by transmission over a lossy channel or several malicious attacks that try to remove the watermark or make it undetectable. A robust watermark should be able to withstand additive Gaussian noise, compression, printing and scanning, rotation, scaling, cropping and many other operations.

## WATER MARK ALGORITHMS FOR TEXT:

1. Read the input image (im).
2. Read the text string (str).
3. Convert the input image into single column.
4. Find out the length of string.
5. Check if the image size is sufficient to accommodate the string.
6. Apply bitand function to 0 the least significant bit of each element of image.
7. Find the randpermutation using randperm.
8. Apply step 9-11 for each charter of the string (for key or without key) for each bit of each character.
9. Calculation of the index of the pixels to be modified.
10. Convert each charter into 8 bit system then Apply bitget function to acquire the j-th bit of the ith character.

11. Apply bitset function to set the pixel indicated by index.
12. Inserting a character cap (end of string).
13. For each bit of the character cap.
14. Calculating the index, Updating bits into template t\_im.
15. Reconstruct the watermarked image.

### WATER MARK ALGORITHMS FOR IMAGE

1. Read the input image (image).
2. Read the logo for water marking (im\_logo).
3. Find out the size of im\_logo.
4. Check if image is large enough to hold im\_logo.
5. Convert the image into a single column vector.
6. Convert im\_logo into a single column vector.
7. Apply bitand function with image.
8. Apply step 9-11 for for each bit of the each pixel.
9. Calculating the linear index of the pixel to be changed.
10. Apply bitget function for each bit of pixel.
11. Apply bitset for each index.
12. Inserting a character cap (end of string).
13. For each bit of the character cap.
14. Calculating the index, Updating bits into template t\_im.
15. Reconstruct the watermarked image.

### DEWATERMARK ALGORITHMS

1. Read watermarked image and key.
2. Convert the watermarked image into single column.
3. Apply randperm function for random variables.
4. Apply loop to find the character cap.
5. Using index find out the bit position using bitget function.
6. Extract the least significant bit.
7. Change combination of bit into character using and store into bitword.
8. Display the extracted image or text.

### COMPRESSION TOOL:

Using above proposed algorithms designed a tool in MATLAB and run on MATLAN command, interface is shown in below figure.



Figure 3: GUI of Water Marking Model

### WATER MARK INSERTION

Click on insert the water mark and first read the input image and write the test as a string (for example karan rajawat) and apply the said water mark algorithms, results are shown in below for encryption key can be inserted but key should be remember at the time of dewater marking other we cannot extract the water marked image from the embedded image.

#### Text as water Mark:

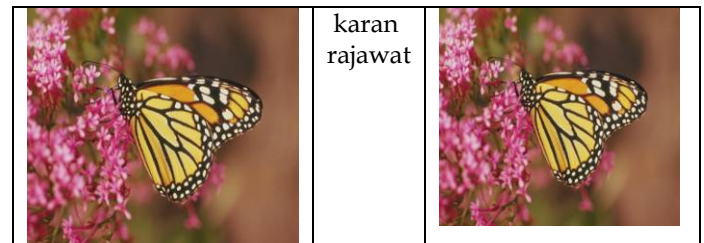


Figure 4: Input image and text

Figure 5: Water marked image

#### Image as a water mark:

Here we read one input image and one water mark image and insert the water mark into the original image, result are show in below with image.

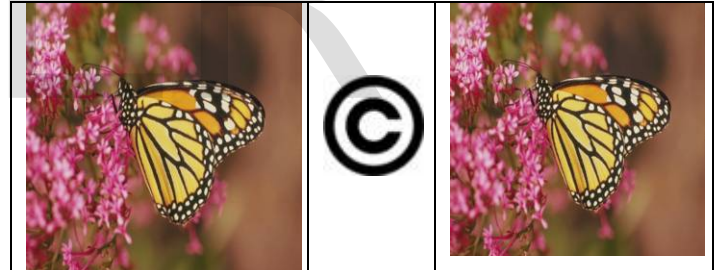


Figure 6: Input image Figure 7: Watermark image Figure 8 : Water marked image

### WATER MARK EXTRACTION

Click on extract button for extract the water mark image from the embedded image, read the embedded image ( encryption key which is inserted during the insertion process) and apply the said de water mark algorithms, here inserted string show which is exact same as input string results are shown in below.

#### Text extraction



Figure 9: Watermarked image and Extracted Text

**Image extraction**

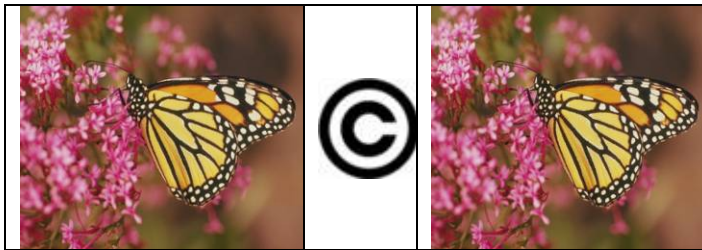


Figure 10: Input image, Watermark image and Water marked image

**QUALITY DISTORTION**

In practice, a watermarked image may be altered either on purpose or accidentally. The watermarking system should be robust enough to detect and extract the watermark [16]. Different types of alterations or attacks can be done to degrade the image quality by adding distortions.

The distortions are limited to those factors which do not produce excessive degradations; otherwise the transformed object would be unusable. These distortions also introduce degradation on the performance of the watermark extraction algorithm [17, 18]. Methods or a combination of methods, considered unintentional are used intentionally as an attack on a watermarked image in order to render the watermark undetectable.

Compression is a common attack, as data transferred via network is often compressed using JPEG. High quality images are often converted to JPEG to reduce their size. Another method is deletion or shuffling of blocks. In images rows or columns of pixels may be deleted or shuffled without a noticeable degradation in image quality. These may render an existing watermark undetectable. Salt and pepper noise is another type of attack that replaces the intensity levels of some of the pixels of an image resulting in loss of information from those pixels. Some of the best known attacks are mentioned here; they may be intentional or unintentional, depending on the application.

This is used to develop a watermarking method which minimizes the quality deterioration of the watermarked image by finding the optimal implementation radius. With a modified coder, our method is able to adapt to the properties of an image which leads to a more robust watermark while maintaining the same influence on overall quality of a watermarked image.

**RECOVERY OF WATERMARK FROM WATERMARKED IMAGE UNDER ATTACKS**





In watermarking terminology, an attack is any processing that may impair detection of the watermark or communication of the information conveyed by the watermark. The processed watermarked data is then called attacked data. There are two kinds of watermark attacks:


Non-intentional attacks, such as compression of a legally obtained, watermarked image or video file, and intentional Attacks, such as an attempt by a multimedia pirate to destroy the embedded information and prevent tracing of Illegal copies of watermarked digital video. The present work describes only one attack:



(1) Salt and pepper noise

In this section we have demonstrated the proposed watermarking technique after using the salt and pepper noise to corrupt the watermarked images up to 0.04 with text and 0.02 for image.

**Text as a water mark**





Watermarked image	Extract water mark text
 Watermarked image	Karan rajawat
 Watermarked image with salt & pepper noise density:0.01	Karan rajawat
 Watermarked image with salt& pepper noise density: 0.02	Karan rajawat
 Watermarked image with salt&pepper noise	karan rajawat

density:0.03	
	karan rajawat
Watermarked image with salt& pepper: noise density:0.04	

	
Watermarked image with salt& pepper noise density: 0.02	

Here salt&pepper noise attack to water marked image(text) and we extract the water mark text from the affected image. Result shows that text is recover without any loss of information. With different noise density text is same for each case.

**Image as a water mark**

Watermarked image	Extract water mark image
	
Watermarked image	
	
atermarked image with salt &pepper noise density:0.01	

Here salt & pepper noise attack to water marked image (image) and we extract the water mark image from the affected image. Result shown that image is recovered without any loss of information. With different noise density quality of image is same for each case.

**INFLUENCE OF WATERMARK PARAMETERS**

In the first part of the research, we evaluate the influence of the watermark on the overall quality of an image and develop a watermarking method that takes into account the influence.

There are different approaches to image quality evaluation and they are based on objective and subjective parameters. The quality of a compressed image is evaluated by analyzing the difference between the original and the compressed one.

One of the most widely used parameters for the evaluation of image quality is the MSE. The list of Image Quality measures implemented in this package include,

1. Structural Content (SC)

$$SC = \frac{\sum_{j=1}^M \sum_{k=1}^N x_{j,k}^2}{\sum_{j=1}^M \sum_{k=1}^N x'_{j,k}^2}$$

2. Mean Square Error (MSE)

$$MSE = \frac{1}{MN} \sum_{j=1}^M \sum_{k=1}^N (x_{j,k} - x'_{j,k})^2$$

3. Peak Signal to Noise Ratio (PSNR in dB)

$$PSNR = 10 \log \frac{(2^n - 1)^2}{MSE} = 10 \log \frac{255^2}{MSE}$$

4. Normalized Cross-Correlation (NCC)

$$NK = \frac{\sum_{j=1}^M \sum_{k=1}^N x_{j,k} \cdot x'_{j,k}}{\sum_{j=1}^M \sum_{k=1}^N x_{j,k}^2}$$

5. Average Difference (AD)

$$AD = \frac{\sum_{j=1}^M \sum_{k=1}^N (x_{j,k} - x'_{j,k})}{MN}$$

6. Maximum Difference (MD)

$$MD = Max (|x_{j,k} - x'_{j,k}|)$$

7. Normalized Absolute Error (NAE)

$$NAE = \frac{\sum_{j=1}^M \sum_{k=1}^N |x_{j,k} - x'_{j,k}|}{\sum_{j=1}^M \sum_{k=1}^N |x_{j,k}|}$$

## RESULT OF QUALITY PARAMETER

First read the watermark original image and image which is extracted from the nosily image (salt & pepper) with different density e.g. 0.01, 0.02 and calculate the below quality parameter, which are shown in below table.

Table1: value of quality parameter

S.No	Parameter	Without noise	Noise density 0.01	Noise density 0.02
1	Mean Square Error	831.5556	831.5556	831.5556
2	Peak Signal to Noise Ratio	18.9319	18.9319	18.9319
3	Normalized Cross-Correlation	1.0482	1.0482	1.0482
4	Average Difference	-11.5556	-11.5556	-11.5556
5	Structural Content	0.8456	0.8456	0.8456
6	Maximum Difference	13	13	13
7	Normalized Absolute Error	0.2227	0.2227	0.2227

## RESULTS AND ANALYSIS

This experimental image used MATLAB in an environment with Windows 7, and used one input image and text (karan rajawat) and logo for as a water mark. PSNR (Peak Signal to Noise Ratio), Mean Square Error, Normalized Cross-Correlation, Average Difference, Structural Content were used on the original water mark image and the extracted image to evaluate the picture quality of the image.

In this section several experimental results are given to show the outcome of the proposed watermarking technique.

In Section water mark insertion image and text inserted into the original image are shown.

In Section water mark Extraction, watermark image and text are extracted from the embedded image.

In Section recovery of watermark from watermarked image under attacks salt and pepper take a cover image along with information logos are taken as input. The watermarked image is shown after embedding. The computed value of the quality metrics are also given to find the image quality.

## CONCLUSION AND FUTURE SCOPE

The current paper presents a new digital watermarking method through bit replacement technology, which stores multiple copies of the same data that is to be hidden in a scrambled form in the cover image. In this paper an indigenous approach is described for recovering the data from the damaged copies of the data under attack by noise salt & pepper with different density (0.01, 0.02, 0.03 and 0.04) and quality of image is same with attack. In future this type of algorithm will be implemented with video and we will also calculate the execution time of the algorithms and check the performance. And quality parameters were also calculated for water marked image.

## Reference

- [1] Ante Poljicak, Lidija Mandic, Darko Agic, "Discrete Fourier transform-based watermarking method with an optimal implementation radius", *Journal of Electronic Imaging* 20(3), 033008 (Jul-Sep 2011).
- [2] L. N. Hu and L. G. Jiang, "Blind Detection of LSB Watermarking at Low Embedding Rate in Grayscale Images," In: M. Celik, G. Sharma, E. Saber and A. Tekalp, Eds., *Hierarchical Watermarking for secure Image Authentication with Localization*, IEEE Transactions on Image Process, Vol. 11, No. 6, 2002, pp. 585-595.
- [3] N. F. Johnson, Z. Duric and S. Jajodia, "Information Hiding: Steganography and Watermarking—Attacks and Countermeasures," Kluwer Academic Press, Norwell, 2001,
- [4] P. Wong, "A Watermark for Image Integrity and Ownership Verification," *Image Processing, Image Quality, Image Capture Systems Conference*, Portland, May 1998, pp. 374-379.
- [5] W. Puech and j.m. rodrigues, "a new crypto-watermarking method for medical images safe transfer".
- [6] Jung-Hee Seo\*, and Hung-Bog Park, "Data-Hiding Method using Digital Watermark in the Public Multimedia Network", *International Journal of Information Processing Systems*, Vol.2, No.2, June 2006.
- [7] Siddhart Manay, Byung-Woo Hong, Anthony J. Yezzi, and Stefano Soatto *Integral invariant signatures*, In *Proceedings of ECCV 2004*, number LNCS 3024, pages 87-99. Springer, 2004.
- [8] Helmut Pottmann, Qixing Huang, Yongliang Yang, and Stefan KAopl. *Integral invariants for robust geometry processing*, Technical report, *Geometry Preprint Series*, Vienna Univ. of Technology, 2005.
- [9] Ucheddu F, Corsini M, Barni M. *Wavelet-based blind watermarking of 3D models*, *Proceedings of the 2004 Multimedia and Security Workshop*, Magdeburg, 143-154, 2004.
- [10] Ohbuchi R, Mukaiyama A, Takahashi S. *A frequency-domain approach to watermarking 3D shapes*, *Proceedings of Eurographics'02*, Saarbrucken, 373-382, 2002.
- [11] Tanmoy Kanti Das and Subhamoy Maitra "Analysis of the "Wavelet Tree Quantization" watermarking strategy and a modified robust scheme" *Multimedia Syst.* Vol. 12 N. 2, PP.151-163, 2006.

[12] D. S. Taubman and M. W. Marcellin, JPEG2000 - Image Compression Fundamentals, Standards and Practice, Kluwer Academic Publishers, pp.6, 2001.

[13] Ozer H., Sankur B., and Memon N., "An SVDBased Audio Watermarking Technique," in Proceedings of the Multimedia and Security Workshop, New York, pp. 51-56, 2005.

[14] Kim H. and Choi Y., "A Novel Echo-hiding Scheme with backward and Forward Kernels," IEEE Transactions on Circuits and Systems for Video Technology; vol. 13, no. 8, pp. 885-889, 2003.

[15] C.-H. Huang and J.-L.Wu, "Attacking visible watermarking schemes," IEEE Trans. Multimedia, vol. 6, no. 1, pp. 16-30, Feb. 2004.

[16] R. Bangaleea and H.C.S. Rughoopth, "Performance improvement of spread Spectrum Spatial Domain Watermarking Scheme Through Diversity and Attack Characterization", in IEEE conference Africon , pp 293-298 ,2002.

[17] Alper Koz, A. Aydin Alatan, "Oblivious Spatio-Temporal Watermarking of Digital Video by Exploiting the Human Visual System" , IEEE transactions on circuits and systems for video technology, Volume:18, Number:3, page: 326-337, March 2008.

[18] Liang Fan, Fang Yanmei, "A DWT-Based Video Watermarking Algorithm Applying DS-CDMA", IEEE

Region 10 Conference TENCON 2006, 14-17 November 2006.

[19] F. Bartolini, A. Tefas, M. Barni, and I. Pitas, "Image authentication techniques for surveillance applications," Proceedings of the IEEE, vol. 89, no. 10, pp. 1403-1418, 2001.

[20] M. Barni, F. Bartolini, A. Manetti, and A. Piva, "A data hiding approach for correcting errors in h.263 video transmitted over a noisy channel," in Proceedings of MMSP01, 2001 IEEE Workshop on Multimedia Signal Processing, October 3-5 2001, pp. 65-70.

[21] S. I. Cox, J. Kilian, F. Leighton, and T. Shanon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.

[22] Chaw-seng Woo, "Digital image watermarking methods for copyright protection and authentication", May 2007.

[23] M. Cancellaro, F. Battisti, M. Carli, G. Boato, "A joint Digital watermarking and encryption method",

[24] Melinos Averkiou "Digital Watermarking".

[25] Koushik Pal, Goutam Ghosh, Mahua Bhattacharya, "Reversible Digital Image Watermarking Scheme Using Bit Replacement and Majority Algorithm Technique, Journal of Intelligent Learning Systems and Applications, 2012, 4, 199-206 doi:10.4236/jilsa.2012.43020  
Published Online August 2012

IJSER