

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

7,000

Open access books available

186,000

International authors and editors

200M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



A Novel Digital Image Watermarking Scheme for Data Security Using Bit Replacement and Majority Algorithm Technique

Koushik Pal¹, G. Ghosh¹ and M. Bhattacharya²

¹*Institute of Radio Physics and Electronics, University of Calcutta, Kolkata*

²*Indian Institute of Information Technology and Management, Gwalior
India*

1. Introduction

Recent history has witnessed the rapid development in information technologies that has given an extended and easy access to digital information. Along with several developments it leads to the problem of illegal copying and redistribution of digital media. As a result the integrity and confidentiality of the digital information has come under immense threat. The concept of an emerging technology, digital watermarking came in order to solve the problems related to the intellectual property of media. (P.W.Wong, 1998). Digital Watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages or even classified information to digital media. (Rafael C Gonzalez and Richard E. Woods, 2002), (Cox I. J., Miller M., Bloom J., 2002).

Watermarks can either be visible or invisible. Here in this chapter we utilize the invisible technique. This is used in public information settings such as digital images libraries, museums, and art galleries and also in defense communication where data security is of prime importance. Watermark embedding utilizes two kinds of methods; one is in the spatial domain and the other in the transform domain. In the spatial domain the watermark is directly embedded into the image pixels whereas in the frequency domain the image is decomposed into blocks and then mapped into the transform domain (M. Kutter, F. A. P. Petitcolas, 1999).

This is basically a process of hiding information in an image known as cover image. Copyright protection is achieved by robust watermarking while image authentication is usually achieved by fragile watermarking techniques. In the fragile watermarking scheme if any alteration of the message is found then it is broken and it can be easily detected as tampered by the provider of the watermark. In general, fragile schemes modify the least-significant-bits LSB planes of the original image in an irreversible way. Often a secret key is also used to encrypt the information (P.W. Wong, 1998). Invertible watermarking is a new process which enables the exact recovery of the original image upon extraction of the embedded information (M.L. Miller, I.J. Cox, J.M.G. Linnartz and T. Kalker, 1999). This work implements both authentication and confidentiality in a reversible manner without affecting the image in any way. Security of images imposes three mandatory characteristics: confidentiality, reliability and availability (J. Fridrich, 2002).

Confidentiality means that only the entitled persons have access to the images.

Reliability has two aspects, **integrity**: the image has not been modified by a non-authorized person; **authentication proofs** that the image belongs indeed to the correct person and is issued from the authorized source.

Lastly availability is the ability of an image to be used by the entitled persons in the normal conditions of access and exercise.

This chapter 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 chapter an indigenous approach is described for recovering the data from the damaged copies of the data under attack by applying a majority algorithm to find the closest twin of the embedded information. A new type of non-oblivious detection method is also proposed. The improvement in performance is supported through experimental results which show much enhancement in the visual and statistical invisibility of hidden data.

1.1 LSB watermarking and its limitation

The most straight-forward method of watermark embedding would be to embed the watermark into the least-significant-bits (LSB) of the cover object (Ling Na Hu Ling Ge Jiang, 2002). Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a smaller object may be embedded multiple times (D. Osborne, D. Abbott, M. Sorell, and D. Rogers, 2004). Even if most of these are lost due to attacks, a single surviving watermark would be considered as a success. LSB substitution however despite of its simplicity brings a host of drawbacks. Although it may survive from all these transformations such as cropping, any addition of noise or lossy compression, a better attack would be to simply set the LSB bits of each pixel to defeat the watermark with negligible impact on the cover object. Furthermore, once the algorithm is discovered, the embedded watermark could be easily modified by an intermediate party. An improvement on basic LSB substitution would be to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given “seed” or key (P.W. Wong, 1998). The algorithm however would still be vulnerable to replace the LSB’s with a constant. Even in locations that were not used for the watermarking bits, the impact of the substitution on the cover image would be negligible.

LSB modification proves to be a simple and fairly powerful tool for steganography (Johnson, N. F., Duric, Z., and Jajodia, S., 2001), however it lacks the basic robustness that watermarking applications require.

1.2 Attack and 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. Different types of alteration which is known as attack 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. Methods or a

combination of methods considered unintentional are used intentionally as an attack on a watermarked document in order to render the watermark undetectable. Compression is a common attack as data transferred via network is often compressed using JPEG (most commonly). 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 some of the pixels of an image resulting 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. In this paper we have taken two very popular attacks known as Salt and pepper noise and image compression.

In present chapter the section 2 contains proposed watermarking method for data authentication. Section 3 describes image quality matrices, section 4 presents the experimental results, section 5 explains flow diagram and section 6 discusses the conclusion of the work.

2. Proposed watermarking technique for data authentication

Our proposed methodology for data hiding does not follow the conventional LSB technique because of its inherent limitations. We have developed a new digital watermarking scheme that uses several bits of the cover image starting from lower order to higher order to hide the information logo. Here we generally hide several sets of the same data forming the information logo into the cover image. So if some of the information is lost due to attack, we can still collect the remaining information from the cover image and can reconstruct the hidden information very closer to the original one.

The detailed step wise algorithm along with the pseudo code written in MATLAB for both the embedding scheme and the recovery scheme is given here. The flow diagram of both the embedding and recovery process is also given in section 5 for better understanding.

2.1 Embedding the digital watermark

Step 1. *Two images are taken as input:*

First of all, the cover image is taken as input. Then the message or information logo is taken as input. The cover image is taken to be a gray scale image. The logo or information is a binary image basically a sequence of 0's and 1's.

Step 2. *The size of the images is extracted:*

Next to make the program compatible to run for any size of the cover image and information logo keeping in mind the data carrying capacity of the cover image the dimensions of the respective images are extracted and stored in to two variables..

Step 3. *Normalize and reshape the logo:*

After normalizing the information logo it is being reshaped in one dimension.

Step 4. *Transforming the cover image into wavelet domain using DWT:*

The cover image is transformed to wavelet domain using discrete wavelet transform. Here we use 'haar' transform to do the DWT. Here the 1st level DWT was used to obtain more

capacity for hiding the information. The cover image is decomposed into 4 subdomains as HH, HL, LH and LL according to different frequencies of the cover image.

Step 5. Calculate the length of transformed cover image and 1 D logo

Step 6. Calculate the size of each sub domain decomposed cover image and reshape them in to 1D

Step 7. Determine the maximum coefficient value of each of the 4 sub domain

Step 8. Finding the position to hide the information logo into the transformed logo:

The position for hiding the binary logo in each sub domain must be in between zero and the maximum coefficient value of that sub domain.

Step 9. Hiding a number of sets of same information logo in HL and LH domain:

More than one set of same information is being hidden in HL and LH band or domain for easier and good quality recovery. The hiding process in each of these domains follows a specific formula. The formula is that the black dots in each sets of 1D information logo is hidden in a position of information logo position from where a constant value is subtracted.

Step 10. Reshaping the decomposed image back to its normal dimension

Step 11. Write the watermarked image to a file and display it.

2.2 Recovery of the embedded watermark

We have assumed that the cover image that is hiding the watermark is available at the receiving end. So again in the process of recovery we first take the original image that has been used to hide the information. Along with that we also send the receiver of the message, 3 keys which essentially act as private keys. These keys are required to decrypt and to the extract the encrypted, embedded messages.

Step 1. take input the watermarked and original image

Step 2. Find 1st level decomposition of both the two inputs using DWT

Step 3. Find the size of each sub domain of both the two decomposed input image

Step 4. reshape each of the decomposition of both watermarked and original cover image into 1 D

Step 5. take two input keys equal to the dimension of logo to find the size of 4 decompositions of logo

Step 6. Determining maximum coefficient values of original cover image

Step 7. Finding positions that were used to hide logo for each decomposition

Step 8. Extracting positional sets for different sets of logo from each decomposition

Step 9. Recovery of different sets of logo from each of the sub bands using majority algorithm and construction of final logo from the different recovered sets

Step 10. after reshaping display each of the recovered sets of logo and the final constructed logo

3. Image quality metrics

To measure the amount of visual quality degradation between original and watermarked images different types of image quality metrics are used. In present work we have used *peak signal-to-noise ratio* (PSNR) and structural similarity index measure (SSIM).

3.1 Peak Signal-to-Noise Ratio (PSNR)

It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed in terms of dB

for wide range signals The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression. The cover image in this case is the original data, and the information logo is the error introduced by watermarking. When comparing deformed image with the original one an *approximation* to human perception of reconstruction quality is made, therefore in some cases one reconstruction may appear to be closer to the original than another, even though it has a lower PSNR. So a higher PSNR would normally indicate that the reconstruction is of higher quality.

It is most easily defined via the mean square error (**MSE**) which is for two $m \times n$ monochrome images I and K where one of the images is considered a noisy approximation of the other and is defined as:

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2$$

The PSNR is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \\ &= 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \end{aligned}$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

3.2 Structural Similarity Index Measure (SSIM)

It is a method for measuring the similarity between two images. The SSIM index is a full reference metric, in other words, the measuring of image quality based on an initial distortion-free image as reference. SSIM is designed to improve on traditional methods like PSNR and MSE which have proved to be inconsistent with human eye perception. The resultant SSIM index is a decimal value between -1 and 1, and value 1 is only reachable in the case of two identical sets of data. The SSIM metric is calculated on various windows of an image. The measure between two windows x and y of common size $N \times N$ is:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

Where μ_x the average of x ;

μ_y the average of y ;

σ_x^2 the variance of x ;

σ_y^2 the variance of y ;

σ_{xy} the covariance of x and y ;

$c_1 = (k_1 L)^2$, $c_2 = (k_2 L)^2$ two variables to stabilize the division with weak denominator;

L the dynamic range of the pixel-values (typically this is $2^{\#bits \text{ per pixel}} - 1$);

$k_1=0.01$ and $k_2=0.03$ by default.

4. Results and discussions

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

In section 4.1. three sets of cover image along with three information logo are taken as input and watermarked image as result of embedding technique. The computed value of quality matrices are also given to find the image quality.

In section 4.2. watermarked images and recovered information logos are given.

In section 4.3. outcomes of same recovery technique has shown but under two attacks known as salt and pepper noise and image compression. For salt and pepper noise the percentage is varied up to 40% and compression up to 5%. The required noisy watermarked images and recovered logo from those images are presented.

In this section eight different sets of recovered logo and the final constructed logo using majority algorithm are also given for two different examples.

4.1 Embedding of watermark into cover image

From table 1 we can see that the results obtained from the quality metric are very satisfactory and hence we can conclude from the obtained data that the watermarked image is not very much different from the original cover image that is being used. Also we can observe that the difference between the watermarked image and the original is appearing all most same to human visual system to detect.

Higher PSNR value indicates good quality of picture. After embedding the information logo in the cover image like *Lina*, *Tower*, *Fruits* etc. we have found a quite higher PSNR value.

Similarly SSIM is another measuring metric used for finding the similarity between the two images. Here we found that after embedding the information logo the similarity between cover image and watermarked image is almost close to 1 as 0.98 which describes a good *structural similarity* between these two images

4.2 Recovery of watermark from watermarked image without any attack

From table 2 we can see that the hidden watermark image i.e. the logo or information is successfully recovered from the watermarked image. Primarily we have considered the communication is ideal and hence no external interference has been included. In practice in the real world scenario we have to consider the noise and which are being incorporated in present experiment into the sent watermarked image. There are chances of unauthorized users in reality where the watermarked image can also be easily altered by unauthorized access from unwanted users.

4.3 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.

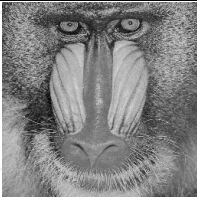
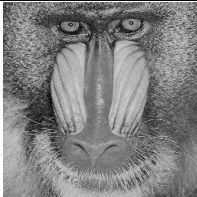
Cover image (dimension 256X256)	Message image (dimension 16X16)	Watermarked image (dimension 256X256)	PSNR in dB	SSIM
			42.343	0.9889
Lena	S logo	Watermarked Lena		
			41.806	0.9781
Tower	K logo	Watermarked Tower		
			41.506	0.9853
Fruit	Max Payne logo	Watermarked Fruit		
			42.893	0.9798
Hat	M Logo	Watermarked Hat		
			42.1347	0.9621
Baboon	C Logo	Watermarked Baboon		

Table 1. Cover image, message image and watermarked image with PSNR and SSIM value

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. In present chapter we have considered two types of attack as (i) *salt and pepper noise* and (ii) *image compression*.

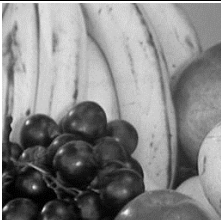
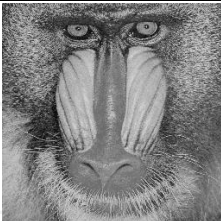
Watermarked Image (dimension 256X256)	Recovered message image (dimension 16X16)
	
Lena	S logo
	
Tower	K logo
	
Fruit	Max Payne logo
	
Hat	M Logo
	
Baboon	C Logo

Table 2. Watermarked image and recovered logo from it without any attack.

4.3.1 Majority algorithm technique

After recovering 8 different sets from attacked watermarked image we have to find the best sets of pixel which is much closer to the original hidden or embedded information logo. The rest portions’ black dots are replaced by white dots. For this every sets of recovered logo is checked with each other to find the similarity. From the following results it can easily understandable the strength of this algorithm. The recovered 8 sets are practically not

recognizable but the final derived logo is quite recognizable and the quality matrices also reflect the strength of this new algorithm.

Two sets of result are given here to understand the algorithm. K logo and S logo both have been constructed from 8 different recovered sets after 40% salt and pepper noise attack.

				
Recovered K logo from 1 st set	Recovered K logo from 2 nd set	Recovered K logo from 3 rd set	Recovered K logo from 4 th set	
				Derived K logo from these 8 set using Majority Algorithm
Recovered K logo from 5 th set	Recovered K logo from 6 th set	Recovered K logo from 7 th set	Recovered K logo from 8 th set	

Table 3. Constructed K logo from recovered 8 sets using Majority Algorithm Technique

				
Recovered S logo from 1 st set	Recovered S logo from 2 nd set	Recovered S logo from 3 rd set	Recovered S logo from 4 th set	
				Derived S logo from these 8 set using Majority Algorithm
Recovered S logo from 5 th set	Recovered S logo from 6 th set	Recovered S logo from 7 th set	Recovered S logo from 8 th set	

Table 4. Constructed S logo from recovered 8 sets using Majority Algorithm Technique

4.3.2 Salt and pepper noise

Salt and pepper noise is a form of noise typically seen on images. It represents itself as randomly occurring white and black pixels. An effective noise reduction method for this type of noise involves the usage of a median filter, morphological filter or a contra harmonic mean filter. Salt and pepper noise creeps into images in situations where quick transients, such as faulty switching, take place.

In this section we have demonstrated proposed technique after using the salt and pepper noise to corrupt the images up to 40 %. This algorithm can recover embedded information from the tempered watermarked image after this attack using majority algorithm.

Watermarked image (dimension 256X256)	Attacked image (Salt and Pepper noise)	Reconstructed message image or logo from 8 different recovered sets (dimension 16X16)			
					
					
					
Lena	10%	S logo			
					
					
					
Lena	20 %	S logo			
					
					
					
Lena	30 %	S logo			
					
					
					
Lena	40 %	S logo			

Table 5. Watermarked image, attacked image and recovered logo using majority algorithm technique

From the above set of results it is clear that the proposed algorithm can withstand even 40% salt and pepper attack with ease and the information logo that is derived from the watermarked image closely resembles the information logo that was embedded into the image.

Hence we can say that the proposed algorithm efficiently handles salt and pepper noise.

Similarly in the next table the strength of the proposed algorithm is demonstrated against the salt and pepper attack with some different sets of data.

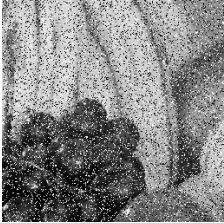
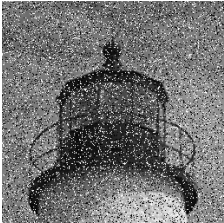
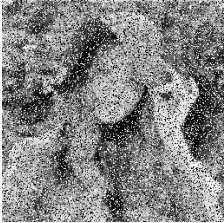
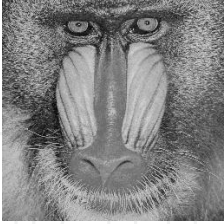
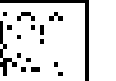
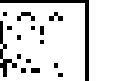
Watermarked image (dimension 256X256)	Attacked image (Salt and Pepper noise)	Reconstructed message image or logo from 8 different recovered sets (dimension 16X16)
		  
Fruit	30 %	Max Payne
		  
Tower	30 %	K logo
		  
Hat	40 %	M Logo
		  
Baboon	40 %	C Logo

Table 6. Four different sets of Watermarked image, salt and pepper noise attacked image and recovered logo using majority algorithm technique

4.3.3 Image compression

The objective of image compression is to reduce irrelevance and redundancy of the image data in order to be able to store or transmit data in an efficient form. Image compression may be lossy or lossless. Lossless compression is preferred for medical imaging.

The proposed algorithm also demonstrates its strength against the compression attack as well.

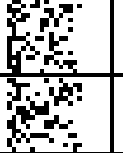
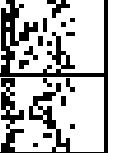
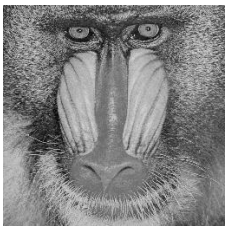
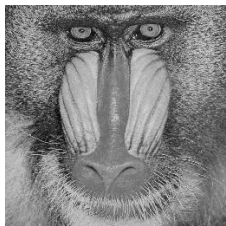
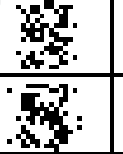
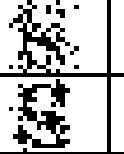
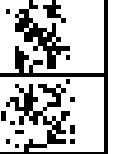
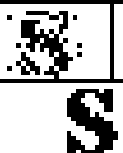
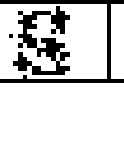
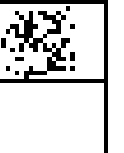
Watermarked image (dimension 256X256)	Attacked image	Reconstructed message image or logo from 8 different recovered sets (dimension 16X16)			
					
					
					
Tower	2 % Compression	K logo			
					
					
					
Baboon	5 % Compression	S logo			

Table 7. Watermarked image, attacked image and recovered logo using majority algorithm

SSIM is used for finding the similarity between the two images. The similarity between original logo and the recovered logo from the watermarked image is measured using SSIM. Following results describe that the proposed algorithm is quite efficient for Salt and pepper Noise up to 40 % and JPEG Compression up to 5% as the SSIM is close to 1.

Used Logo (dimension 16X16)	Types of Attack	Amount of distortion	SSIM
S Logo	Salt and pepper Noise	20%	0.9554
		30%	0.9032
		40%	0.7954
S Logo	Compression	1%	0.9687
		2%	0.8654
		5%	0.7496

4.3.4 Applying the proposed technique on medical images

Medical images are very special as they are very informative. They need more care when we use them. Every medical image contains much more information which may be needed in future. So we have to keep the information of these images intact. The proposed algorithm can also be used on medical images like X ray, MRI, CT Scan for data hiding and authentication.

Here we use some medical images as cover image, some trade mark logo as information, and salt and pepper noise and image compression as attack. Here we can see the proposed algorithm can recover embedded information logo from both types of attacked image up to

40% for salt and pepper noise and up to 3% for compression attack. Even after attack the hidden information logo can be efficiently recovered and is easily recognizable. The good SSIM values of the following table ensure the close similarity between the original and recovered logo.

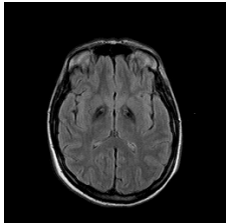
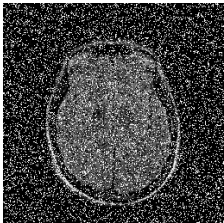
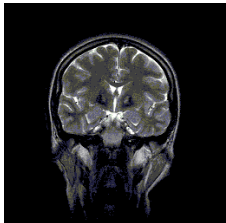
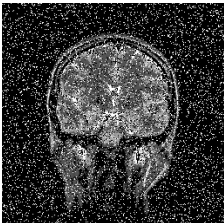
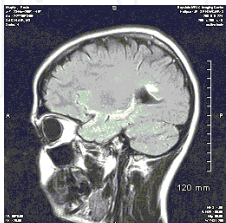
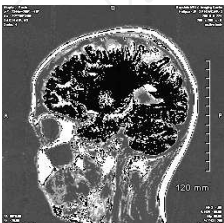
Watermarked image (dimension 256X256)	Attacked image	Reconstructed message image or logo from 8 different recovered sets (dimension 16X16)			
					
					
				SSIM	
				0.7863	
MRI of Brain (Top View)	40% Salt and Pepper	R logo			
					
					
				SSIM	
				0.7801	
MRI of Brain (Rear View)	40% Salt and Pepper	JS logo			
					
					
				SSIM	
				0.8291	
Brain CT Scan (Side View)	3% compression	Man logo			

Table 8. Recovery of information logo from different attacked watermarked medical images

5. Design flow of the proposed scheme

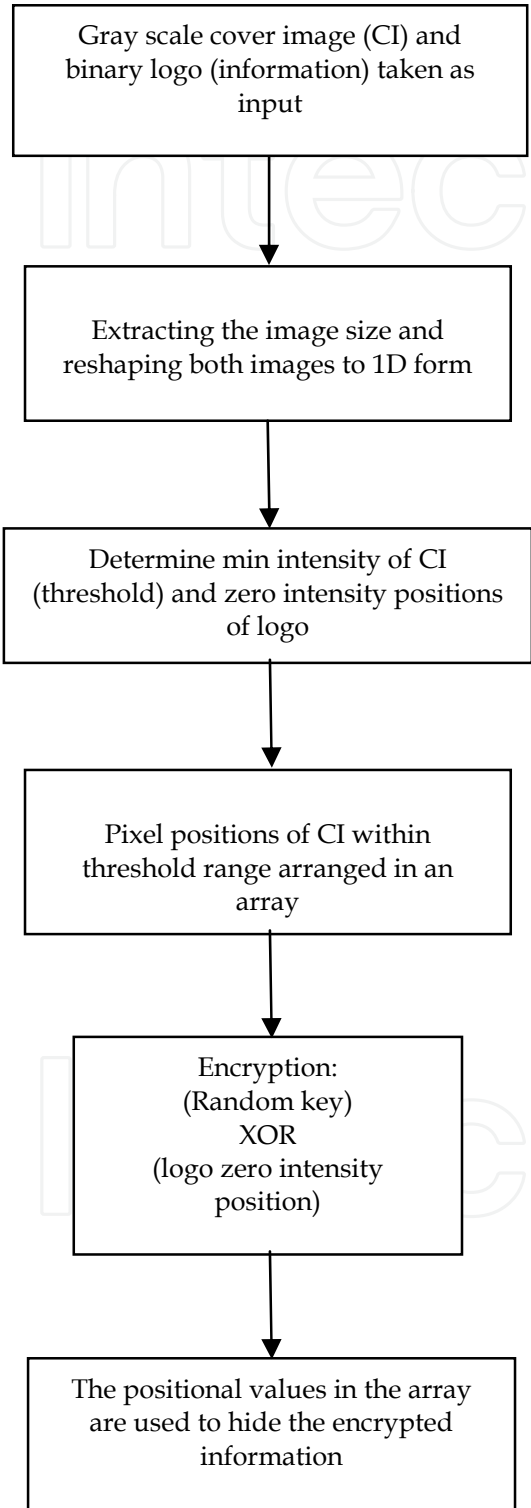


Fig. 1. Embedding or hiding technique

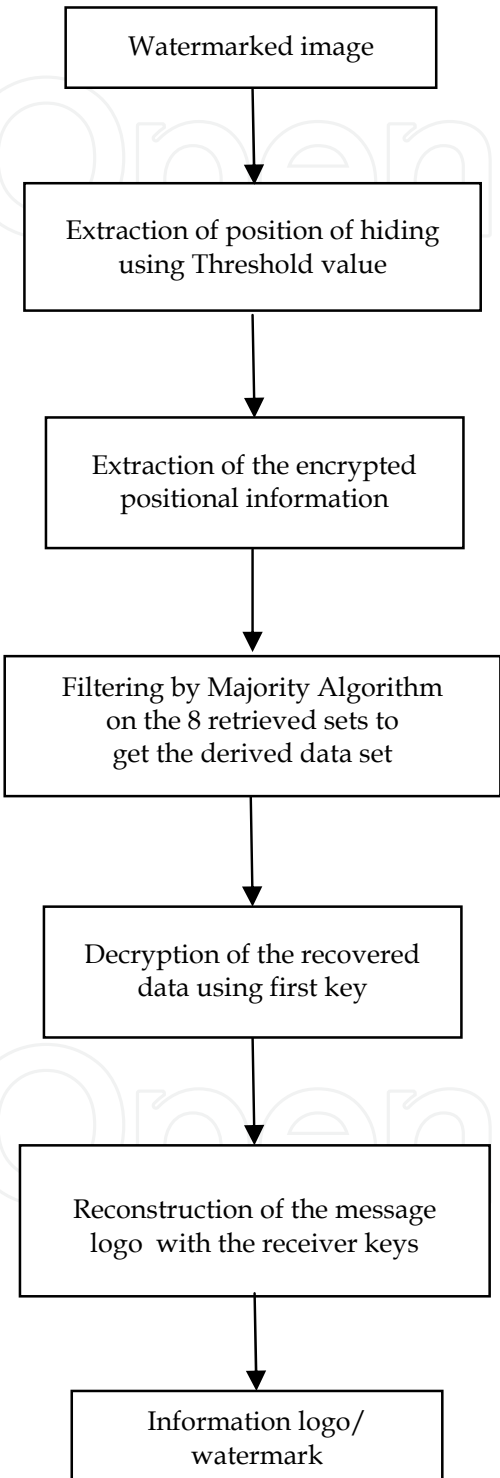


Fig. 2. Decoding or Recover Technique

6. Conclusion

Digital Watermarking has emerged as an important area of research. It mainly deals with the addition of hidden messages or copyright notices into digital media. There are many algorithms available for watermarking and it can be done for different media. They can also be attacked in different ways. Digital Watermarking has many applications in the digital world today. The digital watermarking can be thought as digital communication scheme where an auxiliary message is embedded in digital multimedia signals and is available wherever the later signals move. Therefore the detection reliability is significantly enhanced by embedding rather than by transmitting the same watermark through different sub channels (bands). Thus, this diversity technique can give very good results in detecting the watermark, considering the fact that many watermark attacks are more prone to fading.

The proposed algorithm aims at obtaining a solution to the several problems of digital communication and also for data hiding. It has been seen that the proposed algorithm is robust against compression and 'salt and pepper' noise attack and also utilizes a private key which is required for the recovery of the hidden information and hence lending security to the algorithm. The results obtained show satisfying statistics of the performance of the proposed algorithm. The obtained PSNR and SSIM value supports the quality of the encryption method. It is also seen that the embedded information is successfully recovered from the watermarked image by using majority algorithm technique. The majority algorithm technique is very much efficient and a newer approach which is very unique and easy to understand.

Hence we can conclude by stating the fact that the proposed algorithm provides a method for secure communication and data hiding.

7. Acknowledgement

It is my pleasure to express my heartiest thank to all the faculty members of Institute of Radio physics and Electronics, University of Calcutta, Kolkata for their heartiest cooperation.

I am also thankful to all the faculty members of Electronics and communication Engineering Department of Guru Nanak Institute of Technology, sodepore, Kolkata for their ungrudging support.

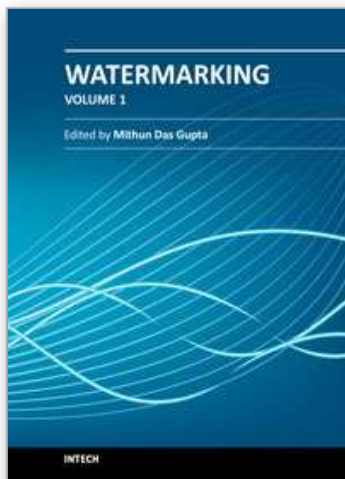
I am also very grateful to my family members for their continuous encouragement.

8. References

- Cox I. J., Miller M., Bloom J., 2002, "Digital Watermarking," Morgan Kaufmann Publishers.
- D. Osborne, D. Abbott, M. Sorell, and D. Rogers. Multiple embedding using robust watermarks for wireless medical images. In IEEE Symposium on Electronics and Telecommunications, page section 13(34), Timisoara, Romania, Oct. 2004.
- E.T. Lin and E.J. Delp, "A Review of Fragile Image Watermarks," in Proceedings of the Multimedia and Security Workshop at ACM Multimedia'99, ACM, Ed., Orlando, Florida, USA, Oct. 1999, pp. 35-39.

- F. Hartung and M. Kutter, "Multimedia watermarking techniques, "Proceedings of the IEEE, vol. 87, no. 7, pp. 1079–1107, July 1999.
- J. Fridrich et al, Lossless Data Embedding for All Image Formats, Proc. SPIE Photonics West, Security and Watermarking of Multimedia Contents, pp. 572–583, 2002.
- Johnson, N. F., Duric, Z., and Jajodia, S., 2001, "Information Hiding: Steganography and Watermarking - Attacks and Countermeasures," Kluwer Academic Press.
- Ling Na Hu Ling Ge Jiang, Blind Detection of LSB Watermarking at Low Embedding Rate in Grayscale Images. M. Celik, G. Sharma, E. Saber and A. Tekalp. Hierarchical watermarking for secure image authentication with localization. IEEE Trans. Image Process, 11(6):585–595, June 2002.
- M. Kutter and F. A. P. Petitcolas. A fair benchmark for image watermarking systems. In Proc. SPIE Security and Watermarking of Multimedia Contents, volume 3657, pages 226–239, San Jose, CA, USA, Jan. 1999.
- M.L. Miller, I.J. Cox, J.M.G. Linnartz and T. Kalker, "A Review of Watermarking Principles and Practices," in Digital Signal Processing for Multimedia Systems, K.K. Parhi and T. Nishitani Eds. New York: Marcel Dekker Inc., 1999, pp. 461–485.
- P.W. Wong, "A public key watermark for image verification and authentication", in Proceedings of the IEEE International Conference on Image Processing, Chicago, IL, October 1998, pp. 455–459.
- P. Wong, "A watermark for image integrity and ownership verification, " Final Program and Proceedings of the IS&T PICS 99, pp. 374–379, Savannah, Georgia, April 1999. Conference on Image Processing, 1, 455–459.
- Rafael C Gonzalez and Richard E. Woods, Digital Image Processing, Prentice Hall, 2002, ISBN-81-7808-629-8
- Shi Y. Q., 2005, "Reversible Data Hiding," IWDW 2004, Korea, Lecture Notes in Computer Science 3304, pp. 1–12.

IntechOpen



Watermarking - Volume 1

Edited by Dr. Mithun Das Gupta

ISBN 978-953-51-0618-0

Hard cover, 204 pages

Publisher InTech

Published online 16, May, 2012

Published in print edition May, 2012

This collection of books brings some of the latest developments in the field of watermarking. Researchers from varied background and expertise propose a remarkable collection of chapters to render this work an important piece of scientific research. The chapters deal with a gamut of fields where watermarking can be used to encode copyright information. The work also presents a wide array of algorithms ranging from intelligent bit replacement to more traditional methods like ICA. The current work is split into two books. Book one is more traditional in its approach dealing mostly with image watermarking applications. Book two deals with audio watermarking and describes an array of chapters on performance analysis of algorithms.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Koushik Pal, G. Ghosh and M. Bhattacharya (2012). A Novel Digital Image Watermarking Scheme for Data Security Using Bit Replacement and Majority Algorithm Technique, Watermarking - Volume 1, Dr. Mithun Das Gupta (Ed.), ISBN: 978-953-51-0618-0, InTech, Available from:

<http://www.intechopen.com/books/watermarking-volume-1/a-novel-digital-image-watermarking-scheme-for-data-security-using-bit-replacement-and-majority-algor>

INTeCH
open science | open minds

InTech Europe

University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China

Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2012 The Author(s). Licensee IntechOpen. This is an open access article distributed under the terms of the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

IntechOpen

IntechOpen