International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

# Secure and robust digital watermarking using co-efficient differencing and chaotic encryption

**A.Pradeep kumar[1], M. Muarli Krishna [2]**
Assistant Professor[1,2]
Department of ECE
Malla Reddy Engineering College

## ABSTRACT

This paper presents a chaotic encryption based blind digital image watermarking technique applicable to both grayscale and color images. Discrete Cosine Transform (DCT) is used before embedding the watermark in the host image. The host image is divided into 8×8 non-overlapping blocks prior to DCT application, and the watermark bit is embedded by modifying difference between DCT coefficients of adjacent blocks. Arnold Transform is used in addition to chaotic encryption to add double layer security to the watermark. Three different variants of the proposed algorithm have been tested and analyzed. The simulation results show that the proposed scheme is robust to most of the image processing operations like JPEG compression, sharpening, cropping, median filtering, etc. To validate the efficiency of the proposed technique, the simulation results are compared with certain state-of-art techniques. The comparison results illustrate that the proposed scheme performs better in terms of robustness, security and imperceptivity. Given the merits of the proposed scheme, it can be used in applications like e-healthcare and telemedicine to robustly hide electronic health records in medical images.

## INTRODUCTION

Introduction Data hiding is of importance in many applications. For hobbyists, secretive data transmission, for privacy of users etc. the basic methods are: Steganography and Cryptography. Steganography is a simple security method. Generally there are three different methods used for hiding information: steganography, cryptography, watermarking. In cryptography, the information to be hidden is encoded using certain techniques; this information is generally understood to be coded as the data appears nonsensical. Steganography is hiding information; this generally cannot be identified because the coded information doesn't appear to be abnormal i.e. its presence is undetectable by sight. Steganography is of different types: 1. Text Steganography 2. Image Steganography 3. Audio Steganography 4. Video Steganography

In all of these methods, the basic principle Steganography is that a secret message is to be embedded in another cover object which may not be of any significance in such a way that the encrypted data would finally display only the cover data. So it cannot be detected easily to be containing hidden information unless proper decryption is used. Cryptography, where the goal is to secure communications from an eaves-dropper, steganographic techniques strive to hide the very presence of the message itself from an observer. The general idea of hiding some information in digital content has a wider class of

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

applications that go beyond steganography, The techniques involved in such applications are collectively referred to as information hiding. For example, an image printed on a document could be annotated by metadata that could lead a user to its high resolution version. In general, metadata provides additional information about an image. Although metadata can also be stored in the file header of a digital image, this approach has many limitations. Usually, when a file is transformed to another format (e.g., from TIFF to JPEG or to BMP), the metadata is lost. Similarly, cropping or any other form of image manipulation destroys the metadata. Finally, metadata can only be attached to an image as long as the image exists in the digital form and is lost once the image is printed. Information hiding allows the metadata to travel with the image regardless of the file format and image state (digital or analog).

**LITEATURE SERVEY**

There are currently three effective methods in applying Image Watermarking: LSB Substitution, Blocking, and Palette Modification. LSB (Least Significant Bit) Substitution is the process of modifying the least significant bit of the pixels of the carrier image. Blocking works by breaking up an image into "blocks" and using Discrete Cosine Transforms (DCT). Each block is broken into 64 DCT coefficients that approximate luminance and color—the values of which are modified for hiding messages. Palette Modification replaces the unused colors within an image's color palette with colors that represent the hidden message. With LSB Substitution I could easily change from Image Watermarking to Audio Watermarking and hide a zip archive instead of a text message. LSB Substitution lends itself to become a very powerful Watermarking method with few limitations. LSB Substitution works by iterating through the pixels of an image and extracting the ARGB values. It then separates the color channels and gets the least significant bit. Meanwhile, it also iterates through the characters of the message setting the bit to its corresponding binary value 3

**EVOLUTION OF WATERMARKING CODE BREAKERS :**

The idea of hiding data in another media is very old, as described in the case of steganography. Nevertheless, the term digital watermarking first appeared in 1993, when Tirkel et al. (1993) presented two techniques to hide data in images. These methods were based on modifications to the least significant bit (LSB) of the pixel value

**DISSECTING WATERMARKING**

Watermarking is a term used for hiding messages within an image. Any color pixel is made of a combination of red –green-blue mode (RGB) wherein each RGB component consist of 8 bits. If letters in ASCII are to be represented within the color pixels, the rightmost digit, called the least significant bit (LSB), can be altered. Any variation in the value of this bit leads to very minimal variation in color. If we have to hide the word 'digit' in the image, we take the LSB of every color and hide each bit of the word in its RGB combination. To insert the letter 'D' we modify three color pixels with three bits in each color pixel, we utilize 14 color pixels to hide the entire word with only 1 bit in the 14th pixel. STEPS FOR HIDING AN IMAGE USING WATERMARKING 1.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

start s-tool and window explorer using the later as drag and drop interface for the software. 2. drag and drop the image to be used as the carrier file from the explorer onto the actions window in s-tool. 3. drag and drop the data file on the carrier file. 4. give pass phrase and encryption algorithm when prompted. Pass these to receiver too. 5. the hidden file is ready. Receiver has to click on the "reveal" button to extract the data.

**Techniques for Image Watermarking :**

Given the proliferation of digital images, and given the high degree of redundancy present in a digital representation of an image (despite compression), there has been an increased interest in using digital images as cover-objects for the purpose of steganography. Therefore we have limited our discussion to the case of images for the rest of this tutorial. We should also note that there have been much more work on embedding techniques which make use of the transform domain or more specifically JPEG images due to their wide popularity. Thus to an attacker the fact that an image other that that of JPEG format is being transferred between two entities could hint of suspicious activity. There have been a number of image steganography algorithm proposed, these algorithm could be categorized in a number of ways: • Spatial or Transform, depending on redundancies used from either domain for the embedding process. • Model based or ad-hoc, if the algorithm models statistical properties before embedding and preserves them, or otherwise. • Active or Passive Warden, based on whether the design of embedder-detector pair takes into account the presence of an active attacker

**RELATED WORK**

K. Joshi, et.al., drew up watermarking methods on spatial domains using the XOR operator. Message insertion is performed with two first XOR operations imposed on the 1st and 8th bits and the second is on the 2nd, 7th bit. The result of the operation is then compared and used as a rule for inserting the message. The cover image used is a 512 * 512 grayscale image and three message sizes, 1024 bits, 2048 bits and 4096 bits. The value of PSNR obtained is about 69 dB with a message length of 4096 bits.

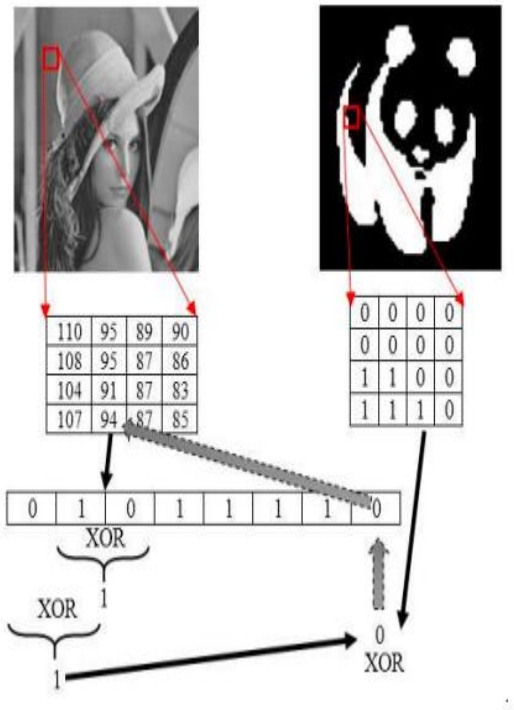
A. U. Islam, et.al., proposing watermarking on the image using the differencing bits technique on the 5th and 6th bits. If there is a difference in the 5th and 6th bits equal to the bits of the secret information then no change is made. Meanwhile, if there is a difference in value, the value changes to the 5th bit so that the value of the difference corresponds to the bit value in the secret information. The cover image used is grayscale image and color image with size 512 * 512. With this method obtained PSNR 51.17977 dB on Lena grayscale image and PSNR 52.3438 on Lena color image, with a payload capacity of 262144 bits message.

C. Irawan, et.al. proposed a combination of steganographic and cryptographic methods, with messages encrypted using the OTP method before being embedded on the LSB. To improve imperceptibility and secure embedding of messages is done on the image edge area. Image edge area detection is done by the Canny method. The cover image used is type JPEG with the size of 11035 bytes, while the message pinned 1024 bytes obtained PSNR 69.1106 dB. In addition, the stego image quality is also measured by a histogram, where the

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

cover image histogram and watermarking image are identical.

E. J. Kusuma, et. al also proposes embedding message in the image edge area. In his research combined steganography techniques using LSB and cryptographic techniques using DES. Before the image message is inserted, the message is encrypted using the DES method. The cover image used is a color image with the size 1024 * 1024, while the message is also a color image with size 64 * 64. The encrypted message is embedded in the image edge area detected by the Canny method. Based on the results of this research, the average value of PSNR 72.21584 dB, which is obtained from five kinds of imagery




**DESIGN AND IMPLEMENTATION**

Embedded scheme In the method we propose, there are two main schemes, namely message embedding and message extraction. For more details can be seen in the sub-section below. A. Embedding Scheme In the embedding, scheme required input in the form of gray-scale cover image and image of the message in the form of a binary image with the exact same size. While the output obtained is a watermarking image. For more details can see the visualization in Figure below

Here are the steps for the embedding process:

Step 1: Read the cover image (A) and message image (B).

Step 2: Change the pixel value to binary.

Step 3: Perform XOR operations on the 7th and on the 6th bit.

Step 4: Perform XOR operation on bit 8th with XOR operation result on the 7th and on the 6th bits

Step 5: Perform XOR operations on message bits with three MSB bits (8th, 7th, and 6th bits). Step 6: Save the XOR operation result in the message bit, then convert again to uint8, the result of this conversion being the watermarking image pixel value.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

**Extraction Scheme**

In the extraction scheme only required input in the form of watermarking image. While the output of the recovered message in the form of a binary image.

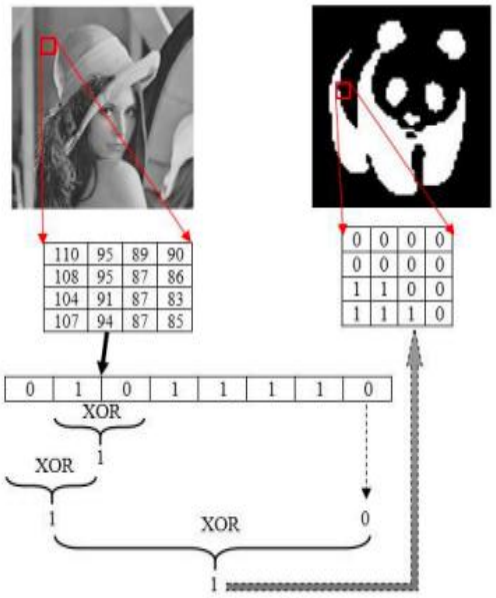



Figure 2 shows the visualization of the extraction process, in detail, the steps in the extraction process are as follows:

Step 1: Read the watermarking image (S).

Step 2: Change the pixel value to binary.

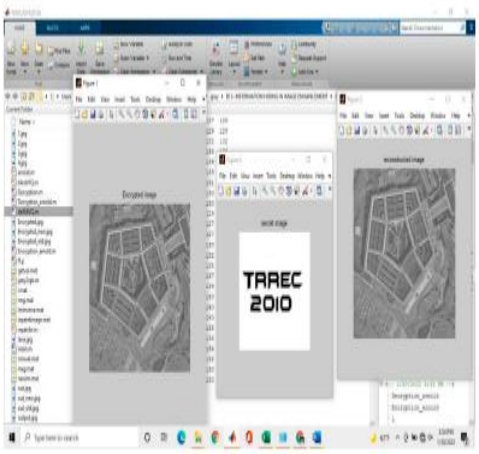
Step 3: Perform XOR operations on the 7th and 6th bits.

Step 4: Perform XOR operation on the 8th bit with XOR operation result on the 7th and on the 6th bit.

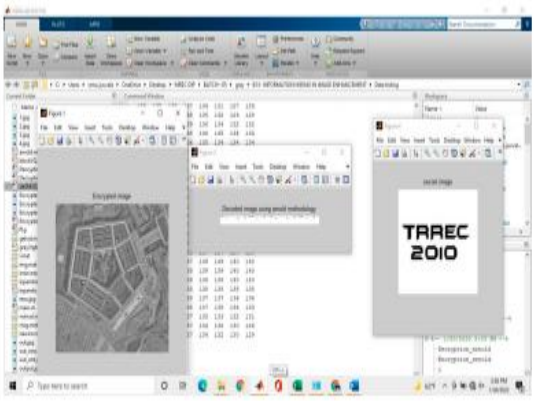
Step 5: do the XOR operation on the LSB with three bits MSB (bits 8th, 7th, and 6th).

Step 6: Save and collect the results of the XOR operation on the LSB, then convert again to uint8, the result of this conversion being a recovery of the message image

**EXPERIMENTS AND RESULTS**




INPUT AND ENCRYPTED IMAGE




DISCRYPT AND SECRET IMAGE

**CONCLUSION**

The method proposed in this study has an advantage in the aspect of imperceptibility as evidenced by the excellent value of PSNR and MSE. Where all PSNR values are more than 50dB, so does the MSE value not more than 0.3. This method is also very simple and safe because with XOR operation watermarking process can be done quickly and easily.

With the XOR operator, the embedded bits cannot be directly guessed. Moreover, there are three keys used, with three times

the XOR operation. The use of an integrated key in the cover image also keeps the watermarking file the same size, and no key delivery is required to the receiver so it can speed up the messaging process as the file size is maintained. However, based on histogram analysis there is a distinct pattern difference between the cover image and watermarking image.

**REFERENCES**

[1] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi and h. A. Sari, "A Good Performance OTP Encryption Image based on DCT-DWT Steganography," TELKOMNIKA (Telecommunication Computing Electronics and Control) , vol. 15, no. 4, pp. 1987-1995, 2017.

[2] R. D. Ardy, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi and E. H. Rachmawanto, "Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5)," in International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICONSONICS), Yogyakarta, 2017.

[3] A. Winarno, D. R. I. M. Setiadi, A. A. Arrasyid, C. A. Sari and E. H. Rachmawanto, "Image Watermarking using Low Wavelet Subband based on 8×8 Sub-block DCT," in International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, 2017.

[4] G. Ardiansyah, C. A. Sari, D. R. I. M. Setiadi and E. H. Rachmawanto, "Hybrid Method using 3-DES, DWT and LSB for Secure Image Steganography Algorithm," in International Conference on Information Technology, Information System, and Electrical Engineering (ICITISEE), Yogyakarta, 2017. [5] A. Setyono, D. R. I. M. Setiadi and Muljono, "StegoCrypt Method using Wavelet Transform and OneTime Pad for Secret Image Delivery," in International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, 2017.

[6] A. U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood, A. Khan, U. Ali and M. Naeem, "An Improved Image Steganography Technique based on MSB using Bit Differencing," in International Conference on Innovative Computing Technology (INTECH), Dublin, 2016.