

# Arithmetic and Wavelet Based Information Security Using Image

Shiv Prasad\*<sup>1</sup>, Prasenjit Maji<sup>1</sup>

<sup>1</sup>Department of CSE, Bengal College of Engineering & Technology, Durgapur, West Bengal, India

## ABSTRACT

### Article Info

Volume 8, Issue 3

Page Number : 428-434

### Publication Issue :

May-June-2022

### Article History

Accepted: 10 May 2022

Published: 25 June 2022

The enhancement of information technology extensively changes the communication system in society. The information is rapidly shared through the internet or other electronic message delivery system without proper security measures. The IPR (Intellectual Property Right) of digital content or digital multimedia has to face the main challenge with the fear of distortion of the contents. Steganography and Cryptography are two widely used techniques for online digital contains authentication. Here we are using both of them together to make it more powerful with the help of simple Arithmetic and Binary operations and embed the same in the frequency domain using the wavelet function. Mainly target to provide a secure text information transmission with cryptex and stegano approach with high payload. The standard metric Peak Signal to Noise Ratio (PSNR) and MSE or Mean Squared Error measures the robustness of the proposed method.

**Keywords:** Cryptography, Steganography, Information Security, IPR, PSNR, MSE.

## I. INTRODUCTION

Watermarking and Steganography have been intensively studied in recent years. In a digital data hiding system, an encoder E embeds a digital message M (e.g., a stego image) into a cover object C (e.g., a digital photo) by slightly modifying the cover object without changing its semantics in a given application scenario. On the other hand, a decoder D extracts, or detects the existence of the message M from an object C, which could be the cover object C, or a slightly distorted version of it due to noise in the transmission channel. These techniques can be very useful in many scenarios, including authentication, fingerprinting, and tamper detection. Due to the requirement of high

fidelity, degradation in the quality of cover image data obtained irreversibly is not acceptable. Reversible data hiding techniques are designed for such scenarios, where the decoder not only extracts the embedded message but also restores the original cover object to a “clean” state. JPEG images are very good candidates for cover objects when applying data hiding techniques due to their very high compression ratio.

Cryptography is the technique to convert plain text into algorithmic text or cipher text and vice-versa so that only the known sender and receiver can extract the secured message with the help of an encryption or decryption algorithm. The cryptanalysis may break the encrypted messages, although modern

cryptography techniques are virtually unbreakable. The receiver must have the associated key to decode or decrypt the message. The cryptographic technique is shown in figure 1.

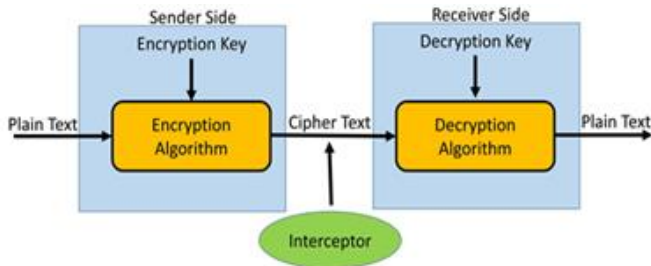


Figure 1 : Cryptography Technique

The data hiding technique which permits the hiding of text or image behind the cover image so that the main message is invisible is called Steganography. Steganography provides secret communication for security purposes. Cryptography provides the means for secure secret communication. A combination of steganography and cryptography would be the most secure way to data hiding. The existence of encrypted communication requires attention to it, hiding it in another image that is called a cover image. The steganography is having the following types as shown in figure 2.

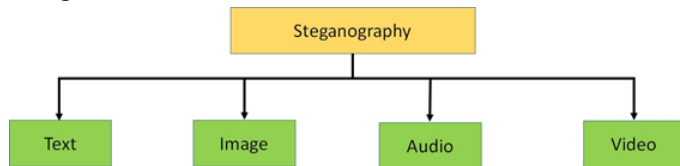


Figure 2 : Types of Steganography

In the text message, the “text cover” should be cover media. The main advantage of text Steganography is that it requires less memory and Steganography communication. The cover media that can use for the stego algorithms are text, images, video, and audio. Our proposed algorithm deals with image cover media with maximum payload capacity. The salient contributions are:

- This provides dual security by using the concepts of cryptography and Steganography.
- Maximize the payload since we hide the text information under the color images which are in jpeg or bmp format and use the size of the image.

- The given process is hundred percent reversible. Since we are hiding text data, so there is no loss is granted.

The rest of the paper is divided into a literature review in section II followed by the proposed algorithm and methodology in section III and section IV represents the result and discussion, the conclusion is in section V.

## II. RELATED WORK

Information hiding is obtained in four phases as preliminary phase, embedded phase, transmission phase, and extraction phase. In preliminary phase encryption, the technique is applied and in the embedded phase researchers use information hiding algorithms. Combining Steganography and cryptography methods is more efficient for providing security and data protection to communication [1]. Image steganography is a method, which uses the images as a carrier for a secret message since the Internet, acquires a large number of digital images and offers ease in dealing with images [2, 3]. Payload facing electronic attacks by hackers. Many algorithms have suggested concealing data in images because of the huge amount of digital images on the web and the simplicity of dealing with images in a hiding process [4-6]. Nowadays, researchers have focused on improving the hiding process in images by using different techniques like LSB and EMD. Many researchers have also developed techniques that embed text messages or another image behind the image. There are various methods for data hiding [4] such as frequency-domain spatial domain and compressed data domain. In the frequency domain data hiding [7, 8] images are first converted into the frequency domain, and then data embedding is done by modifying the transformed coefficients of the frequency domain. In spatial domain messages, image pixels are arranged to incorporate the data to be embedded. This technique is simple to implement and offers a high hiding capacity [9, 10]. The quality of

the image in which the data embedding is done can be easily controlled. Whenever the data transmission is done on the network, it must be in compressed form and a compressed domain data hiding technique is used [11-13]. The compressed information is used for embedding the data in the compressed domain where the compressed data coefficients are manipulated to embed data [14, 16]. The proposed algorithm is working with both steganography and cryptography techniques with maximum payload.

### III. PROPOSED ALGORITHM & METHODOLOGY

#### A. Text Embedding

```

Begin
Inputs cover image 'img' with dimension X×Y and
Read Text file as 'data'
for i=1 to length(data)
    ASCII (i) =data (i)
    If ASCII (i) is greater than 0
        Max=ASCII (i)
    End for
    M=Max.
for i=1 to length(data)
    Binaries (ASCII(i)) and complement then again
    converted to decimal
    Normalize the updated ASCII (i) with Arithmetic
    operation with the help of M as NORM
End for
[cA1, cH1, cV1, cD1] = DWT2 (img)
Hide length (data) as n and Max value M in cH1.
for i = 1 to length(data)/2
    Hide NORM (i) in cV1
End for
for i = length(data)/2+1 to length(data)
    Hide NORM (i) in cD1
End for
Scrt_Img = IDWT2 (cA1, cH1, cV1, cD1)
Regenerate the Scrt_Img for communication
End
    
```

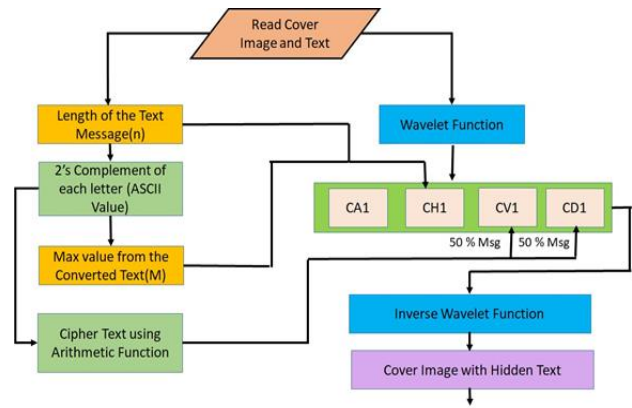


Figure 3 : Flowchart for Text hiding

#### B. Text Extraction

```

Begin ( Scrt_image)
[cA11, cH11, cV11, cD11] = DWT (Scrt_image)
Extract n and M from cH11
for i=1 to n/2
    Extract text (i) = cV11 (i, y) y as column size of cV11
End for
for i= n/2+1 to n
    Extract_text(i) = cD11(i,y) y is the column size of
    cD11
End for
Regenerate the normalized text by Arithmetic
operation with the help of M as REV_NORM
for i=1 to n
    Binaries REV_NORM(i) and complement then and
    again converted to decimal
    Write the equivalent text of the extracted decimal
End for
Save the extracted text as the target file.
    
```

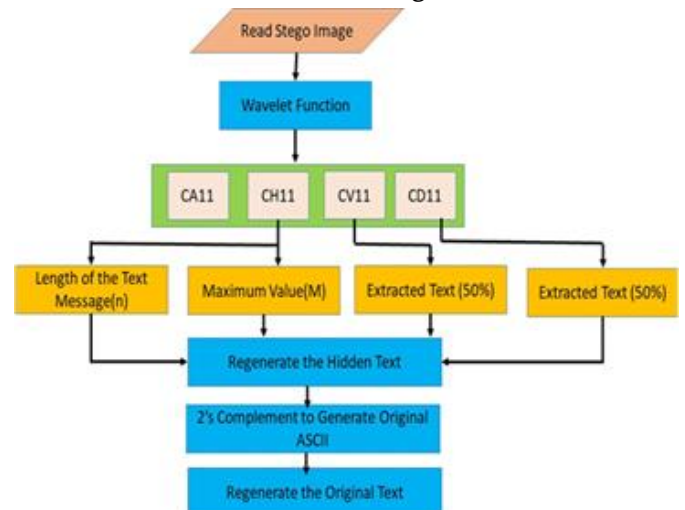


Figure 4: Flowchart for Text extraction

**C. Discrete Wavelet Transformation (DWT)**

There are many discrete wavelets transforms like Coiflet, Daubechies, Haar, Symmlet, etc. Haar wavelet is the first known and simplest possible wavelet. Haar Wavelet can also be described as a step function  $f(x)$  shown in Eq 1

$$f(x) = \begin{cases} 1 & 0 \leq x < 1/2, \\ -1 & 1/2 \leq x < 1, \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

Decomposition step

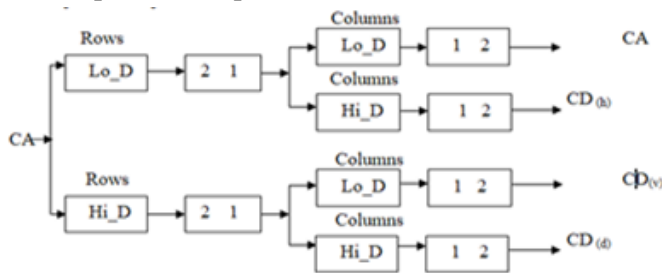


Figure 5: DWT Decomposition Step

Two's complement is the process of finding the negative value of a binary number. To find the 2's complement of a binary number, first, we have to change all 1's with 0 and all 0's with 1 and add 1 in LSB. If we again calculate the 2's complement of the number (already in 2's complement) we get the original number, working example is below

$$(14)_{10} \xrightarrow{\text{Binaries}} (1110)_2 \xrightarrow{\text{2's comp}} (0010)_2 \xrightarrow{\text{2's comp}} (1110)_2 \xrightarrow{\text{Binaries}} (14)_{10}$$

**D. Mean Squared Error (MSE)**

The mean squared error is a metric that measures how near a regression line is to a set of data points. It achieves this by squaring the distances (error) between both the points and the regression line. Squaring is needed to remove any negative signs. It also provides substantial variances in weight. Because of calculating the average of a group of numbers, it has termed the mean squared error.

Suppose that we would like to estimate the value of an unobserved random variable  $X$  given that we have

observed  $Y=y$ . In general, our estimate  $x^\wedge$  is a function of  $y$ :

$$x^\wedge = g(y) \quad (2)$$

The error in our estimate is given by

$$X^\sim = X - x^\wedge = X - g(y) \quad (3)$$

Often, we are interested in the mean squared error (MSE) given by

$$MSE = \frac{1}{n} \sum_{i=1}^n (y_i - \bar{y}_i)^2 \quad (4)$$

Where  $n$  is the total no of data points  $y_i$  is the observed value and  $\bar{y}_i$  is the predicted value.

**E. Peak Signal to Noise Ratio (PSNR)**









The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is used as a quality measurement between the original and a compressed image. Higher PSNR means the better the quality of the compressed or reconstructed image.  $R$  represents the peak value.

$$PSNR = 10 \log_{10} \left( \frac{R^2}{MSE} \right) \quad (5)$$

The mean-square error (MSE) and the peak signal-to-noise ratio (PSNR) are used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The minimum value of MSE means the minimum error.



TABLE1: SHOWS THE COVER IMAGE, TEXT MESSAGE WHICH WILL BE EMBEDDED AND TEXT EMBEDDED IMAGE OR STEGO IMAGE

Cover Image	Text Message	Text Embedded Image
	Welcome to the world of Computer Science. Now a day we have more options for research in today has required technology. (.docx format)	
	In a pandemic situation like COVID-19, Computer Science provide so many platforms for online activities like online classes, online payments, etc. (.docx format)	
	Welcome to the world of Computer Science. Now a day we have more options for research in today has required technology. (.txt format)	
	In a pandemic situation like COVID-19, Computer Science provide so many platforms for online activities like online classes, online payments, etc. (.txt format)	

IV. RESULTS AND DISCUSSION

Matlab 9.4.0 is extensively used for the implementation of the proposed algorithm. We are considering different image formats like jpg, .png, .bmp, .gif, etc., and two types of text files for embedding purposes i.e. .docx and .txt to check

the robustness of the proposed algorithm.

Table1 shows the cover image. the message with the file type and the image after embedding the message with cover and we can see visually there is no such effect on the stego image and check the standard parameter (MSE, PSNR) in between the cover and

stego image we check and mention it on Table2. As we are using the color image as a cover that is why the PSNR value is so high, we also calculate the same in gray level.

TABLE 2 : MSE AND PSNR FOR DIFFERENT IMAGES AND TEXT FILE FORMAT FOR COVER IMAGE AND STEGO

Sl No	Cover image format	Text file format	IMAGE		
			MSE	PSNR (Color)	PSNR (Gray Scale)
1	JPEG	DOCX	$3.94 \times 10^{-4}$	161.7579	80.7445
2	JPEG	TXT	$2.38 \times 10^{-4}$	175.0005	85.4357
3	BMP	DOCX	$7.54 \times 10^{-4}$	164.7989	78.3432
4	PNG	DOCX	$6.34 \times 10^{-4}$	157.7958	73.1355
5	GIF	TXT	$4.06 \times 10^{-4}$	105.0870	57.5264

## V. CONCLUSION

This paper introduced the hiding of information besides the cover images with the help of combining concepts of Cryptography and Steganography. To overcome the problem of electronic attacks on payload we use the arithmetic encryption method and then hide encrypted text within the cover image. In the proposed algorithm, we use a green channel from the color cover image to hide the information. By using Discrete Wavelet Transformation green channel is divided into four frequency domain and use the two most noisy parts for hiding and the algorithm is independent of the size of the image so according to the requirement. We can use red and blue channels too. It is a text-hiding algorithm so it is 100 percent reversible by nature. Therefore, there is no issue of data loss. In future perspective by using this algorithm we are considering video as a cover with text, we can hide images as information.

## VI. REFERENCES

- [1]. Sahu, Aditya Kumar, Swain, Gandharba and Babu, E. Suresh. "Digital Image Steganography Using Bit Flipping" *Cybernetics and Information Technologies*, vol.18, no.1, pp.69-80, 2018.
- [2]. Kuo, Wen-Chung and Wang, Chun-Cheng and Huang, Yu-Chih., " Binary power data hiding scheme". *Int. J. Electron. Commun.* Vol 69 issue 11, pp 1574–1582, 2015.
- [3]. K. Sathish Shet, A. R. Aswath, M. C. Hanumantharaju, and Xiao-Zhi Gao. "Novel high-speed reconfigurable FPGA architectures for EMD-based image steganography". *Multimedia Tools Appl.* Vol 78, issue 13, pp 18309–18338, July 2019.
- [4]. C. Chang, W. Tai, and K. Chen, "Improvements of EMD Embedding for Large Payloads," *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007)*, pp. 473-476, 2007.
- [5]. Abbas Cheddad and Joan Condell and Kevin Curran and Paul {Mc Kevitt}, " Digital image steganography: survey and analysis of current methods". *Signal Process*, Vol 90, pp 727–752, 2010
- [6]. Pascal Maniriho, Tohari Ahmad," Information hiding scheme for digital images using difference expansion and modulus function".*Journal of King Saud University - Computer and Information Sciences*, Volume 31, Issue 3, Pages 335-347,2019,
- [7]. Anjali A. Shejul, Umesh L. Kulkarni, "A Secure Skin Tone based Steganography Using Wavelet Transform," *International Journal of Computer Theory and Engineering* vol. 3, no. 1, pp. 16-22, 2011.
- [8]. Saha, S., Ghosal, S., Chakraborty, A., Dasgupta, S., Sarkar, R., Mandal, J., "Improved exploiting modification direction-based steganography

using dynamic weightage array”. Electron. Lett. Vol 54 issue 8, pp 498–500, 2018.

- [9]. Houda JOUHARI, “New Steganographic Schemes Using Binary and Quaternary Codes”, Le 1er Juillet, 2013.
- [10]. Mekha Jose, Kottayam Dst, “Hiding Image in Image Using LSB Insertion Method with improved Security and Quality”, International Journal of Science and Research , Volume 3 Issue 9, pp 2281 – 2284, September 2014.
- [11]. Padmini. K, Radhika .D. K.,” Least Significant Bit algorithm for image steganography “, International Journal of Advanced Computer Technology (IJACT), Volume 3, Number 4, 2014.
- [12]. Sneha Bansod, Gunjan Bhure, “Data Encryption by Image Steganography”, International Journal of Information and Computation Technology. Vol 4, Issue 5, pp. 453-458, 2014.
- [13]. Chi-Kwong Chan, L.M. Cheng, 2004. “Hiding data in images by simple LSB substitution”. Pattern Recogn. Vol 37, Issue 3, pp 469–474, 2004
- [14]. Anjali A. Shejul, Umesh L. Kulkarni, "A Secure Skin Tone based Steganography Using Wavelet Transform," International Journal of Computer Theory and Engineering vol. 3, no. 1, pp. 16-22, 2011.
- [15]. Xinpeng Zhang, Shuozhong Wang, “Efficient stenographic embedding by exploiting modification direction”. IEEE Commun. Lett. Vol 10, Issue 11, pp 781–783, 2006.
- [16]. C. Lee, Y. Wang, and C. Chang, "A Steganographic Method with High Embedding Capacity by Improving Exploiting Modification Direction," Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 497-500, 2007

### Cite this Article

Ch. Esther, S. Nayana Sai, S. Sushma, B. V. R. Gupta, Mr. G. Srinivasa Rao, "Disease Prediction Based on Symptoms By Using Decision Tree And Random Forest In Machine Learning ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 3, pp. 419-427, May-June 2022. Available at doi :

<https://doi.org/10.32628/CSEIT2283105>

Journal URL : <https://ijsrcseit.com/CSEIT2283105>