|| Volume 5 || Special Issue SBPCOE || June 2020 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

STEGANOGRAPHY WITH IMPROVED EMD BASED METHOD AND PARAMETER VERIFICATION

Neha Vardekar[1], Isha Thakurdesai[2], S.K.Moon[3], Poonam Shingade[4]

Department of Electronics and Telecommunication Pune Institute of Computer Technology Pune, India

nehavardekar19@gmail.com,ishathakurdesai8@gmail.com,skmoon.pict.edu, poonamshingade1509@gmail.com

---------- ***----------

Abstract: The work presented is based on the popular steganographic method Exploiting Modification Direction (EMD). Data can be recovered from the Steganographic image only when the embedding EMD equation is known; therefore, its detectability is low. The improved EMD method can achieve excellent image quality due to the minimized modification of cover pixels. The proposed method uses (m^2+3) as the embedding equation. It reaches the largest embedding capacity when m=1. However, the embedding capacity decreases drastically when the value of m increases. Also, some external attacks can distort the steganographic image while transmitting. Therefore, to ensure security at the decoder side, parameters of the steganographic image are getting checked to find the originality of the received steganographic image and recovered data.

Keywords—*Steganography, Image processing, Exploiting Modification Direction, Parameters of image*

---------- ***----------

I INTRODUCTION

Steganography refers to hiding secret data in a cover object such that it is imperceptible to any external interceptor. Among many introduced methods over the years, EMD provides better security as only both involved parties know the correct equation to decode the message hidden. Still, due to external noise or interceptions, the steganographic image faces distortion. These attacks can be detected by verifying the steganographic image parameters on the transmitter and receiver side and comparing them. Parameters like image intensity, cross-correlation, embedding capacity, and histogram are verified in the proposed method. If these parameters differ, then it can be concluded that the image received is corrupted.

II. IMPROVED EXPLOITING MODIFICATION DIRECTION (EMD)

The method proposed by Zhang and Wang [18] was fully exploiting modification directions. Ki-Hyun Jung and Kee-Young Yoo proposed [4] an improved method of the EMD to embed more secret data while achieving higher PSNR value. Their proposed method can embed a secret bit on every pixel of cover data. The results of this method demonstrated that the proposed method has a high capacity and better visual quality. Their equation is as follows:

$$f = (gi + x) \bmod (2n + 1) \quad \ldots(1)$$

where gi is the message image pixel and x varies from $0 \leq x < 2n+1$ and $-(2n+1) < x \leq 0$ respectively.Each secret digit in a (2n+1)-ary notational system can be carried by one cover pixel.

III. IMPROVED EMD BASED PROPOSED METHOD

One of the most appealing qualities of improved EMD for security is that an encryptor can create an equation and only share it with a decryptor so that no other unwanted source will be able to decrypt. Improved EMD increases the embedding capacity but works with (2m+1)-ary only. Inspired by this technique, a different ary equation is used in this paper.

3.1Embedding Process

Assume message to be S.Firstly, S is converted to binary, which is then converted to (m2 + 3)-ary stream,S'. Read one (m2 + 3)-ary digit 'f' from S'.Consider img(i,j) to be the cover image. If (img (i,j) +x)mod(m2 + 3) = =f, then the new value saved will be img(i,j)+x. If not then the value of x will be changed. After all cover pixel units are processed, the secret data is completely embedded and the stego image is generated. This embedding process can have m values from 0 to 1.Values of x are taken to be -2 to 1 as we require (m2 + 3)-ary neighboring pixels.

if , f = (img(i, j) + x)mod(m2 + 3) then,

Stego(i, j) = img(i, j) + x, ...(2)

For example, let m = 1, img(i,j) = 157, and f = 2. In the first case, stego(i,j) is calculated by f= (img(i,j) + x) mod ((m2)+3) = (157+(-2)) mod 4 = 3, (157 +(- 1)) mod 4 = 0, (157 + 0) mod 4 = 1, (157 + 1) mod 4 = 2, for each x value. Then, since stego(i,j) is equal to f when x = 1, a new pixel value stego(i,j)= img(i,j) + x = 157 + 1 = 158 is obtained.

3.2 Extraction Process

recovered(i, j) = stego(i, j)mod(m2 + 3) ...(3)

Form each pixel unit stego(i,j) in a steganographic image, to gather the message divide a steganographic image by (m2+3), and then take mod.

For example, for m = 1 and stego(i,j) = 158, recovered(i,j) = (158) mod (4) =2.After all digits of message are collected in S', it is converted back to the binary secret stream S thus the secret message is successfully extracted.

IV. QUALITY ANALYSING PARAMETERS

Though improved EMD assures the security of message coded, it does not provide protection against external noise effects. Geometrical attacks like cropping and rotation, compression attacks like JPEG compression, image processing attacks like histogram equalization, and various noises like gaussian, speckle, salt, and pepper, Poisson, etc. affect the steganographic image which further affects the extraction process. These noises and attacks, along with the quality of the transmitted image, can be detected by verifying parameters. Therefore this paper encourages analyzing parameters of a steganographic image on the receiving channel.

The parameters selected in this paper are:

1) PSNR: Peak Signal to Noise Ratio is an important criterion to evaluate the quality of the image. People cannot distinguish the difference between two images when PSNR is more than 30dB. Therefore, the value of PSNR is checked to be above 30dB.

2)Embedding Capacity: The embedding capacity (EC) is measured by the number of secret bits carried into a cover pixel. Therefore its unit is bits per pixel. Here as all the secret bits must be embedded, its value is verified as 1.

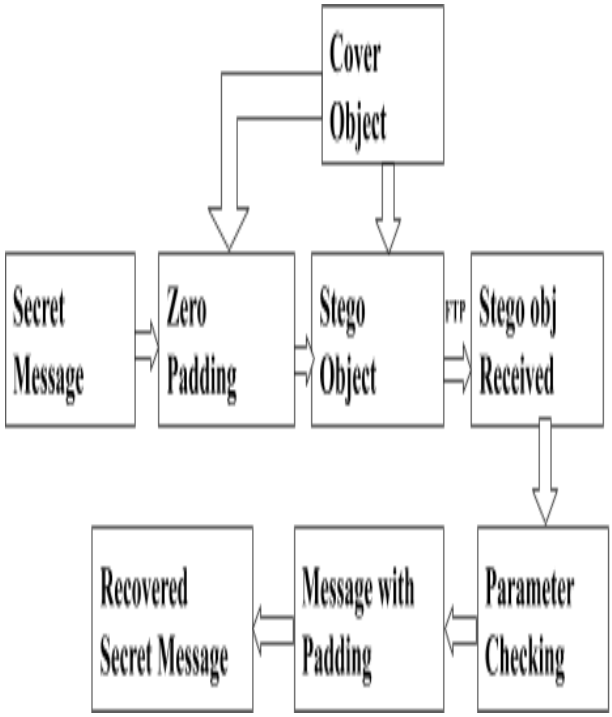
3)Cross-correlation: The correlation between two signals is a standard technique for evaluating the degree to which two signals are identical. In practice, a correlation coefficient is greater than about 0.7 or 0.8 indicates a good match.

4)Critical Value of m: In the proposed scheme, the m-pixel unit in a cover image can hide an (m2 + 3)-ary secret digit by modifying the only one-pixel value. The limitation of m in the implemented scheme is from 0 to 1

5)Histogram Comparison: The histogram plots the number of pixels for each tonal value. The highest peak of the histogram signifies the tonal value with the highest number of pixels. Thus the tonal values of two images, i.e., cover and steganographic, are compared. If the tonal values of the highest peak are approximately identical, they are considered to have the maximum number of pixels for the same tonal value. Therefore it is proved that the required cover image has smoothly encoded the message.

6) Image intensity: Intensity is the value of pixels in an image. Various noises like Salt and pepper, Gaussian, Poisson, etc. can be detected by checking the value of image intensity.

V. BLOCK DIAGRAM



The above block diagram explains the detailed procedure of embedding secret message into a cover image. Zero padding is done to make the message and cover of the same size.

VI RESULTS AND DISCUSSION

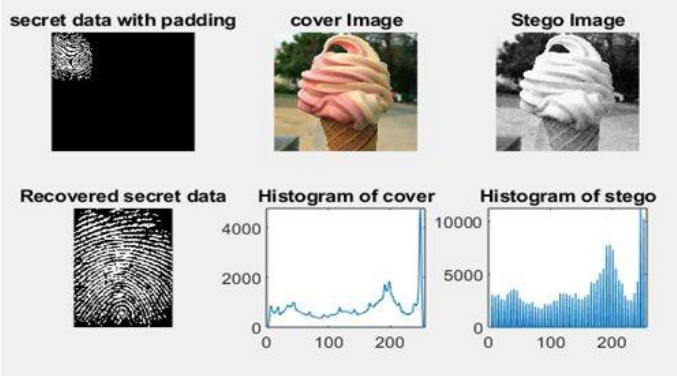


Fig.(a) icecream.png

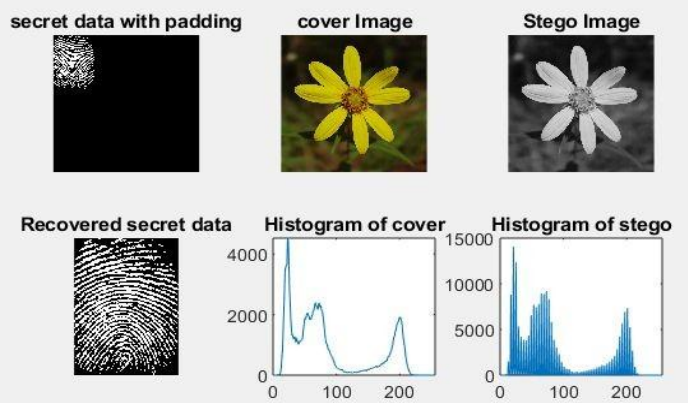
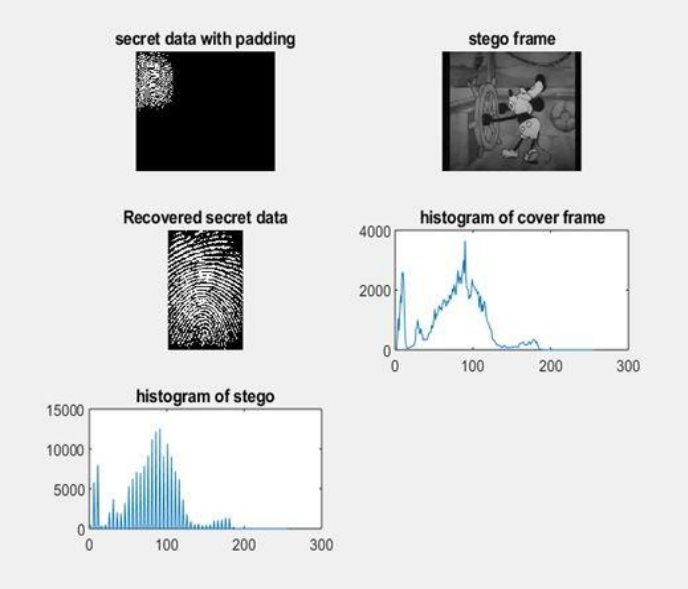


Fig.(b) sunflower .png



Fig(c) micky.mp4

Here Fig (a) and Fig (b) show outputs of hiding image inside the image with the proposed method process. Fig (c)shows the output of hiding image inside a single frame of video.

This method hides one pixel of binary message image inside one pixel of the cover image, and here due to zero padding message and cover, both images are of the same dimensions. EC i.e., embedding capacity, is 1, which is ideal in this case. The correlation coefficient compares the cover image and steganographic image to find out imperceptibility. In steganography, it is essential to ensure that hidden data should not be visible. The ideal value of the correlation coefficient is 1. Here this algorithm achieved it closer to 1. PSNR is a peak signal to noise ratio. Here PSNR is above 40dB. To check the smooth embedding in the cover image and also transmission without interference, the highest peak value of cover and steganographic image should be checked; ideally, they should be the same. As shown in the table below, they are approximately the same. Below is a table that mentions our results obtained by embedding images within image and image within a frame of video.

Examples	**Parameters**				
	Peak Signal to noise ratio	**Recovered mean image intensity**	**Cross-correlation**	**Histogram peak difference**	**Embedding capacity**
Fig(a) icecream .png	46.38 dB	0.3989	0.9503	0	1
Fig(b) sunflower .png	46.35 dB	0.3989	0.9998	2	1
Fig(c) micky.mp4	46.3140 dB	0.3989	0.9995	1	1

Table (a) Result after analyzing parameters with the proposed method

Parameters	LSB	Proposed solution
Correlation coefficient	1	0.9998
PSNR	13.2565 dB	46.3140 dB
Embedding Capacity	1 bpp	1 bpp

Table (b) Comparison between LSB and the proposed method

If the PSNR ratio is high then images are considered to be less affected by noise. The PSNR value in the comparison table shows that the improved EMD scheme has a high PSNR value compared to the Least Significant Bit (LSB) technique.LSB technique is based on hiding data by altering only the least significant bit of cover image. With the above PSNR values, it can be stated that less distortion is obtained using improved EMD as compared to LSB technique.

Examples	Parameters			
	Peak Signal to noise ratio		Histogram peak difference	
	Improved EMD	Proposed method	Improved EMD	Proposed method
Fig (a) icecream.png	45.0451	46.38	3	0
Fig (b) sunflower.png	45.0642	46.35	2	2
Fig(c) micky.mp4	45.1288	46.3140	1	1

Table (b) Comparison between Improved EMD and the proposed method

The table above mentions the results obtained by our comparison with improved emd and proposed method.As per the above observation, the proposed equation also works as effectively as the original emd equation.Improved EMD increases the embedding capacity but works with (2m+1)-ary only. By using the applied method ((m^2)+3)-ary can also be used.Range of m varies from 0 to 1.

VII CONCLUSION

The proposed method will help in verifying the originality of data after transmission using parameters verification. Only if data is unaltered it is successfully accepted. To ensure embedding of full message number of pixels in message should be less than or equal to number of pixels in cover. Also, the value of PSNR can be increased using a different noise-prone and robust algorithm. Many other different parameters can also be checked for ensuring complete security of the secret message.

REFERENCES

[1] Harpreet Kaur and Jyoti Rani, “A Survey on different techniques of steganography”, 2016.

[2] Klimis Ntalianis and Nicolas Tsapatsoulis ,“Remote authentication via biometrics:a robust video-object steganographic mechanism over wireless networks”,February,2015.

[3] Manjit Sandhu, Jaipreet Kaur and Sukhdeep Kaur ,“ Encoding and decoding of image using steganography technique”, June, 2016.

[4] Ki-Hyun Jung and Yoo Kee-Young,“Improved exploiting modification Direction by Modulus operation”,19 March,2015.

[5] Mohammad Imran, Dr.AbdulrahmanA.Algamdi and Bilal Ahmad “Role of firewall technology in network security”,December,2015.

[6] C.R. Kim, S.H. Lee, J.H. Lee and J.-I. Park, “Blind decoding of image steganography using entropy model”,May ,2018

[7] Hetal R. Patel, Khushboo Sawant and Krishnakant Kishore, “ Fingerprint based image steganography in transform domain”,January,2015.Harpreet Kaur, Jyoti Rani “A Survey on different techniques of steganography”, 2016.

[8] Yanjun Liu,Chin-Chen Chang andPeng-Cheng Huang,“Extended exploiting-modification-direction data hiding with high capacity”,2017.

[9] Yanping Zhang,Juan Jiang,Yongliang Zha.,Heng Zhang and Shu Zhao,“Research on embedding capacity

and efficiency of information hiding based on digital images",February25,2013.

[10] Le Quang Hoa,Nguyen Huy Truong andCheonshik Kim Ching-Nung Yang,"Data hiding scheme for searching in hidden text with automata",August ,2015.

[11] Wenhao Chen,Yangxiao Wang,Yong Guan,Jennifer Newman,Li Lin and Stephanie Reinders,"Forensic analysis of android steganography apps".2018.

[12] Xuejing Niu,Meng Ma,Rui Tang and Zhaoxia Yin"Image steganography iva fully exploiting modification direction",2015.

[13] Xinpeng Zhang and Shuozhong Wang,"Efficient steganographic embedding by exploiting modification direction",November,2006.

[14] Y.Raghavender Rao,Nikhil Prathapani, E.Nagabhushanam, "Application of normalized cross correlation to image registration",May,2014.

[15] Arup Kumar Pal,Kshiramani Naik,and Rohit Agarwal,"A Steganography scheme on JPEG compressed cover images with high embedding capacity",January,2019.

[16] A.N.Pimpale and prof.Anoop Khambra,"Review on median filter in image filtration",February,2016.

[17] Omprakash Patel,Yogendra P.S.Maravi and Sanjeev Sharma,"A Comparative study of histogram equalization based image enhancement techniques for brightness preservation and contrast enhancement",October,2013.

[18] S.Suryanarayana,Dr.B.L.Deekshatulu,Dr.K.Lal Kishore and Y. Rakesh Kumar,"Estimation and removal of Gaussian noise in digital images",2015.

[19] Zhang, X. and Wang, S. 2006. Efficient steganographic embedding by exploiting modification direction. IEEE Commun. Lett. 10, 11 (Nov. 2006), 781-783. DOI=10.1109/LCOMM.2006.060863.

****

Shahajirao Patil Vikas Pratishthan's

S. B. PATIL COLLEGE OF ENGINEERING,

Indapur, Pune – 413106

Organized

An E-National Conference on

"SCIENCE AND TECHNOLOGY"

2K20

on **15th and 16th June 2020**

****