IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN IMPROVED EXPLOITING MODIFICATION DIRECTION ALGORITHM FOR ENHANCING MEDICAL IMAGE SECURITY USING STEGANOGRAPHY

Vedant Misal, Shrawasti Kamble, Pratiksha Kinge, S. K. Moon

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

Abstract: Data hiding technology advances with the algorithms that are fast, secure and provide more capacity. In order to provide better security an improved VSEMD is proposed in this paper. The contribution of this method is without complicating embedding steps secret data can be embedded and extracted. Embedding bits by replacing pixel's least-significant bit (LSB) is simple but security is improved by modifying only selective pixels directive. We provided an approach that exploits pixels in a particular area of the image thus adding security to the encryption method.

Index Terms - **Data hiding, Cover image, Stego image, EMD, Steganography**

I. INTRODUCTION

Data hiding strategies are critical for the information security field, the primary method wants to pass secret information that is being embedded into the cover image and then generates the stego image which contains secret information that can not be observed by people. In short,the task is not only to improve embedding capacity but also to maintain good quality of the image. However, we cannot take into account each other at the same time.

Nowadays medical images are transferred for a variety of purposes from one place to another. This transfer of images needs security as they contain sensitive information. Hence we are trying to embed some secret information in it in order to verify the integrity in the transmission and reception process of data transfer.

The initial method was altering the least significant bits (LSBs) of the cover image with the secret data. This was the simplest method but not most secure. Later several advancements were done such as selecting more than one significant bit, exploiting in particular direction, etc.

Matrix embedding is another useful method which embeds n bits into 2^n-1 pixels that causes less than one modification of LSB(least significant bit). Though it has high embedding efficiency it came with less embedding rate.

In 2006, Zhang and Wang proposed a modulo method in which directional characteristics were modified based on Exploiting Modification Direction (EMD). In this scheme, only one pixel out of two was modified in either upward, downward, forward, reverse or no direction. Since then, many scholars and experts have suggested and given different EMD-type data hidden techniques.

The rest of this paper is organized as follows. Section II, we will roughly introduce the Zhang-Wang scheme, and Kuo-Wang scheme. The proposed scheme and experimental results are detailed in Section III and Section

IV, respectively. Finally, conclusions are given in Section V.

II. RELATED WORK

A. Exploiting Modification the Direction Method

In 2006, Zhang and Wang proposed a method to embed the secret data into image.[1]In this method during each embedding stage, at most one pixel's value would be altered by one, then there are 2n options for modification while 1 option is without any modification. Here N pixels are represented as the vector Gn=[g1,g2,g3,g4,...,gn]. For pixel grouping and conversion process, Zhang and Wang defined the extraction function as:

f1(Gn) = i=1n (gii) mod(2n + 1) (1)

If f1 equals secret digit d, no pixels are modified. If not, we calculate s = (d-f1) mod (2n+1). If s isn't greater than n , gs plus 1, otherwise, g2n+s-1 minus 1. Receiver can retrieve secret data easily by calculating f1 with modified pixels .

Embedding efficiency is the ratio of embedded bits and distortion, and embedding rate is the number of secret bits in each pixel. The secret digit in (2n+1)-ary notational system is embedded in n pixels, thus embedding efficiency p is calculated by,

p=(2n+1)log2(2n+1)2n (2)and the embedding rate q is given by,

q=log2(2n+1)2n (3)

The EMD algorithm has higher embedding efficiency as well as embedding rate than those of matrix embedding. However, there is still room for improvement in these two aspects. According to analysis the best hiding bit rate is in a 5-ary system(2n+1 for n=2). This is a serious drawback as the hiding rate affects when n is increased. Hence, we propose a new improved EMD embedding method for better results.

[2] Kuo, Wuu, and Kuo, "The high embedding steganographic method based on general multi-EMD" presents an innovative steganographic approach that uses general multi-EMD for high-capacity data embedding. The contribution of the work in terms of embedding capability, obfuscation and performance analysis makes it an important addition to the existing literature in the field of information security and steganography. The proposed method promises further development in this field and will be a valuable resource for researchers and professionals interested in steganographic techniques.

[3] Chang and Wu, "A Large Payload Information Hiding Scheme Using Two-Level Exploiting Modification Direction" presents an innovative information hiding scheme that uses the TLEMD approach. The paper's contribution in terms of carrying capacity, robustness and quality preservation make it a valuable addition to the existing literature in the field of information hiding and multimedia signal processing. The proposed system offers promising opportunities for further development and is a valuable resource for researchers and operators in the field.

[4] Hajizadeh, Ayatollah, and Mirzakuchak, "A new high capacity and EMD-based image steganography scheme in spatial domain" presents an innovative steganography combining EMD with spatial domain techniques. The paper's contribution in terms of capacity, concealment and robustness make it a valuable addition to the existing literature on image steganography and electrical engineering. The proposed system offers promising possibilities for secure information hiding applications and is a valuable resource for researchers and practitioners in the field.

[5] Yao and Wu's "Robust EMD-Like Steganographic Scheme" presents an innovative steganographic scheme based on the EMD-like algorithm. The paper's contributions to robustness, security, and secrecy make it a valuable addition to the existing literature on steganography and information security. The proposed system offers promising possibilities for secure information hiding applications and is a valuable resource for researchers and practitioners in the field.

[6] Kuo, Li, and Wang, "An Improvement Data Hiding Scheme Based on Formula Fully Exploiting Modification Directions and Pixel Value Differencing Method," presents an innovative data hiding scheme that combines the F-FEMD method and the PVD technique. The paper's contribution to embedding capability, security and tact makes it a valuable addition to the existing literature on data hiding and information

security. The proposed system offers promising opportunities for secure data transfer applications and is a valuable resource for researchers and practitioners in the field.

[7] "Improved EMD Steganography with Great Embedding Rate and High Embedding Efficiency" by Qu, Fu, Niu, Yang, and Zhang presents an innovative steganography that uses EMD to achieve high embedding speed and efficient information hiding. The contribution of the paper in terms of deployment speed and efficiency makes it a valuable addition to the existing literature on steganography and multimedia signal processing. The proposed system offers promising possibilities for secure information hiding applications and is a valuable resource for researchers and practitioners in the field.

III. PROPOSED SCHEME

For embedding secret data in an image we need to have all the files in the same format. For this, we have obtained a list of pixel values and values of secret data both in the decimal system.

1. Open the cover image file and secret data file.
2. Get the parameters of cover file and secret data.
3. Read all the pixels of the cover image and secret data as bytes.
4. Convert the cover and secret image bytes to the decimal array.
5. Calculate the index values based on the cover image and secret data size to be embedded into cover audio.
6. Check whether the secret data can be included in the cover image.
7. Try to embed the data into a cover image with chosen indices to have minimum distortion possible.
8. Convert the decimal values of the modified cover image pixels to bytes.
9. Write the modified cover image pixels to a new image file.
10. Now for extracting the secret data we need to perform the reverse logic we used while embedding.
11. We need to find the modified values and store them into an array then to convert it into the data file.

In figure 1, we observe that we need cover images and secret data converted into Decimals which can be used for further Data Manipulation. Using the EMD Algorithm the secret data is embedded in the cover image at random places.

1. Select a Carrier Image: Choose an image file that will serve as the carrier for embedding the secret information. Ensure that the carrier image is suitable in terms of complexity, length, and compatibility with the chosen steganographic technique.
2. Determine Modification Direction: Analyze the carrier image to identify its natural characteristics, such as no. of pixels, chromatic variations, or temporal patterns. Determine the optimal directionality for introducing modifications that align with thesecharacteristics.
3. Encode the Secret Data: Convert the secret information you want to embed into a suitable format for steganographic encoding. This may involve converting it into binary form, applying encryption techniques for security, or other suitable encoding methods.
4. Select Modification Locations: Identify Now for extracting the secret data we need to perform the reverse logic we used while embedding.regions within the carrier audio where modifications can be made while minimizing perceptual changes. Focus on lessperceptually significant areas or segments that are less likely to be noticed by observers. These regions should align with the modification direction determined in step 2.
5. Modify the Carrier Image: Apply the modification direction determined in step 2 to embed the secret data

into the carrier image. This can involve techniques such as modifying specific pixels, altering bits, etc. according to the selected modification locations.

6. Detection Avoidance Considerations: Analyze the modified image to identify potential vulnerabilities or detectability issues. Evaluate the modifications from the perspective of detection algorithms, ensuring that the embedded data remains robust against various steganalysis techniques.

7. Extraction and Decoding: Develop an extraction algorithm that can recover the embedded data from the modified carrier image. Reverse the modification process using the determined modification direction and extract the encoded secret information.

8. Evaluate Performance: Assess the performance of the implemented steganographic system. Measure parameters such as PSNR, imperceptibility, security, and resistance against detection. Compare the results with existing techniques and evaluate the trade- offs in terms of complexity and efficiency.

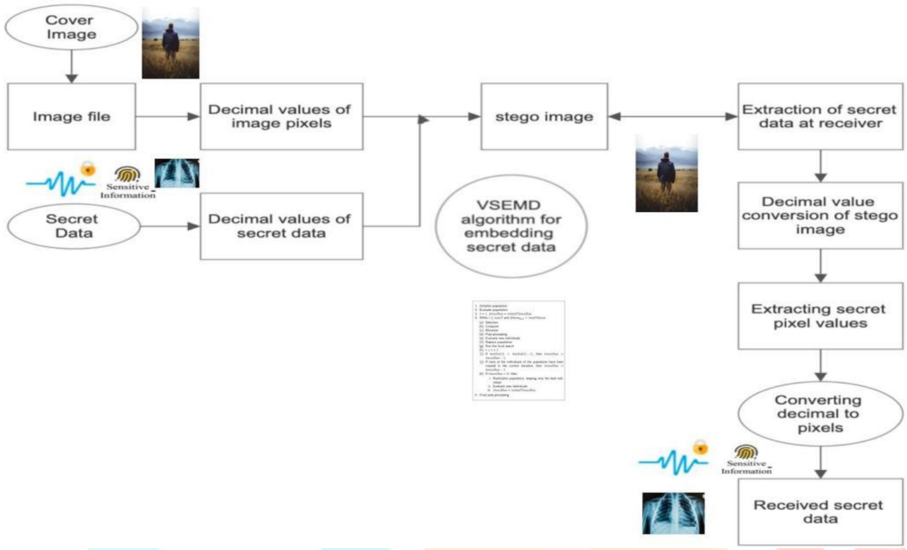

Cover Image
Image file
Decimal values of image pixels
stego image
Extraction of secret data at receiver
Sensitive Information
Secret Data
Decimal values of secret data
VSEMD algorithm for embedding secret data
Decimal value conversion of stego image
Extracting secret pixel values
Converting decimal to pixels
Sensitive Information
Received secret data

Figure 1 Block Diagram of VSEMD system architecture

Many EMD-type data hiding methods have been devised up to this point. Not only has the data concealment technology's security been improved, but the stego-image quality has also been improved. In order to overcome this problem,we will present a high embedding approach based on the generic Exploiting modification direction steganography algorithm.

IV. VSEMD ALGORITHM

Input: n consecutive pixels (pixel_1,pixel_2 ,pixel_3….pixel_n) and m number of bits and (nk+1) binary bits secret message in the form of digit value .

Output: n adjacent stego pixels

Step 1 :

Select any three consecutive pixel values of a image (pixel_1,pixel_2 ,pixel_3) and the secret data in the form of digit value,D

Step 2:

Compute the value for $Px=4m^2+3m+2$, (4) where m =Numbers of bits to be selected.

Step 3 :

Compute the value of F by using this formula,

F=(pixel_1*1+ pixel_2*2 +pixel_3*3) % Px (5)

Step 4 :

Now,Take input from the user for the value D , which means secret data in the form of a digit .

Step 5 :

Enumerate the values for A, B and C by using A=pixel_1/Kt ,B= pixel_2/Kt and C= pixel_3/Kt.**Step 6** :

Compute the values of new stego pixel values new_stego_1,new_stego_2,new_stego_3 by using the below formulae:new_stego_1=pixel_1+A new_stego_2=pixel_2+Bnew_stego_3=pixel_3+C**Step 7 :**

To produce a minimum error and obtain the new possible stego pixel values (new_stego_pixel1,new_stego_pixel2, new_stego_pixel3) ,The VSEMD generic four various conditions to obtain the three new stego pixel pixel values areCase 1 :

new_stego_1=(A+m) and new_stego_2=B+(m+1) and new_stego_3=C+(m-1)

Case 2 :

new_stego_1=(A-m) and new_stego_2=B-(m+1) and new_stego_3=C-(m-1)

Case 3:

new_stego_1=A+(m+1) and new_stego_2=B-m and new_stego_3=C+m

Case 4:

new_stego_1=A-(m+1) and new_stego_2=B+m and new_stego_3=C-m

Example 1 :

Step 1:

Select any three consecutive pixel values of a image (pixel_1, pixel_2, pixel_3)=(70, 60, 47) and m=1 and the secret data in the form of digit value, D=3

Step 2 :

Compute the value for Px=4m^2+3m+2, Px=4*1^2+3*1+2=21.

Step 3 :

Compute the value of F by using this formula, F=(pixel_1*1+ pixel_2*2 +pixel_3*3) % Px F=(70*1+60*2+47*3)%21 =16

Step 4 :

Now, Take input from the user for the value D , which means secret data in the form of a digit .where D=3

Step 5 :

Enumerate the values for A, B and C by using A=pixel_1/Kt ,B= pixel_2/Kt and C= pixel_3/Kt. A= 70/8=8 ,B= 60/8=7 ,C=47/8=5

Step 6 :

Compute the values of new stego pixel values new_stego_1, new_stego_2, new_stego_3 by using the below formulae:new_stego_1 = pixel_1+A

new_stego_2 = pixel_2+Bnew_stego_3 = pixel_3+Cnew_stego_1 = 70+8 = 78,
new_stego_2= 60+7 = 67,
new_stego_3= 47+5 = 52.

Step 7 :

Case 1: D=3, m=1, Fnew1= (9+9+5)%21= 23%21= 2

Case 2: D=3, m=1, Fnew2= (8+9+5)%21= 22%21= 1

Case 3: D=3, m=1, Fnew3= (10+8+6)%21= 24%21= 3

Case 4: D=3, m=1, Fnew4= (6+8+4)%21= 18%21= 18

Therefore, In the first case, D=3 and Fnew=3, Hence, we can say that secret data is recovered.

IV. RESULTS AND DISCUSSION

The proposed scheme based on VSEMD algorithm was tested on four rgb images(medical image1,medical image1 withpneumonia,medical image2,medical image2 with pneumonia) shown in below figure.2.

The stego images is shown in below Figure 3(m = 1), Figure.4(m = 2), and Figure.5(De-embedded images)

Figure 2. Cover images

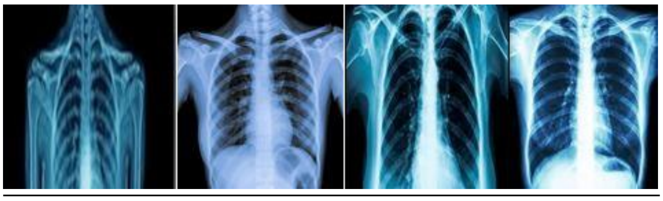


Figure 3. Stego images, m = 1

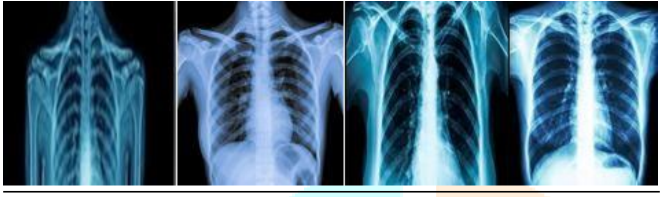
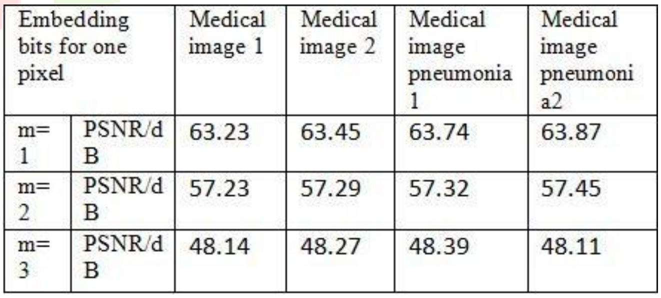


Figure 4. Stego images, m = 2

Figure 5. De-embedded image

According to proposed scheme results, there are no observable differences between cover images and stego images from human naked eyes. All stego (encrypted) images PSNR and MSE are shown in table 1 respectively

Table 1 PSNR values



Embedding bits for one pixel		Medical image 1	Medical image 2	Medical image pneumonia 1	Medical image pneumoni a2
m= 1	PSNR/d B	63.23	63.45	63.74	63.87
m= 2	PSNR/d B	57.23	57.29	57.32	57.45
m= 3	PSNR/d B	48.14	48.27	48.39	48.11

V. ACKNOWLEDGMENT

Project inspiration and motivation have always played a key role in the success of any venture. I express my sincere thanks to Dr. S. K. Moon, project guide, Pune Institute of computer technology. I pay my deep sincere thanks to HOD of electronics and telecommunication department Dr. M. V. Munot to encourage us to the highest peak and to provide the opportunity to prepare the project. I am thankful for providing the lab facilities and lab equipment in the time of need. Our appreciation also goes to our fellow batchmates who with their moral support and timely help made the journey a fruitful one. Last but not the least, special appreciation to the team members for the complete coordination, honest efforts and willingness to complete this project.

REFERENCES

[1] Xinpeng Zhang, Shuozhong Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction" IEEE Communications Letters (Volume: 10, Issue: 11, November 2006) DOI:10.1109/LCOMM.2006.060863

[2] Wen-Chung Kuo, Lih-Chyau Wuu, Shao-Hung Kuo, "The high embedding steganographic method based on general multi EMD" 2012 International Conference on Information Security and Intelligent Control. DOI: 10.1109/ISIC.2012.6449762

[3] Chin Chen Chang, Hsiao Ling Wu, "A Large Payload Information Hiding Scheme Using Two-Level Exploiting Modification Direction" 2014 Tenth International Conference on Intelligent Information Hiding and and Multimedia Signal Processing. DOI: 10.1109/IIH-MSP.2014.133

[4] Hamzeh Hajizadeh, Ahmad Ayatollahi,Sattar Mirzakuchaki, "A new high capacity and EMD-based imag steganographyscheme in spatial domain" 2013 21st Iranian Conference on Electrical Engineering (ICEE) DOI:10.1109/IranianCEE.2013.6599814

[5] Xiaoming Yao, Weihua WuA, "Robust EMD-Like Steganographic Scheme" Third International Symposium on Intelligent Information Technology and Security Informatics, IITSI 2010, Jinggangshan, China, April 2-4, 2010 DOI:10.1109/IITSI.2010.28

[6] Wen-Chung Kuo, Jyun-Jia Li, Chun-Cheng Wang, "An Improvement Data Hiding Scheme Based on Formula Fully Exploiting Modification Directions and Pixel Value Differencing Method" 2016 11th Asia Joint Conference on Information Security (AsiaJCIS). DOI:10.1109/AsiaJCIS.2016.20

[7] Qu Zhiguo, Fu Y, Niu Xinxin, Yang Yixian; Zhang Ru, "Improved EMD Steganography with Great Embedding Rate and High Embedding Efficiency" 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing DOI: 10.1109/IIH-MSP.2009.290

[8] Zeyad Safaa Younus, Mohammed Khaire Hussain, "Image steganography using exploiting modification direction forcompressed encrypted data" Volume 34, Issue 6, Part A, June

[9] Sourabh joshi1 , S.I.Nipanikar 1, "Analysis of Various Exploiting Modification Direction Techniques of Image Steganography:
A Review Paper" volume:3 | april-june 2007

[10] Xinpeng Zhang, Shuozhong Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction" IEEE Communications Letters (Volume: 10, Issue: 11, November 2006)DOI:10.1109/LCOMM.2006.060863

[11] A. Ker, P. Bas, R. Böhme, R. Cogranne, C. Scott, T. Filler, J. Fridrich and T. Pevny, "Moving steganography and steganalysis from the laboratory into the real world", ACM Information Hiding and Multimedia Security Workshop, (2013)June 45-58, Montpellier, France.

[12] Yanxiao Liu; Chingnung Yang; Qindong Sun, "Enhance Embedding Capacity of Generalized Exploiting ModificationDirections in Data Hiding" 28 December 2017 volume 6 DOI : 10.1109/ACCESS.2017.2787803

[13] E. A. Elshazly, Safey A. S. Abdelwahab, R. M. Fikry, "FPGA implementation of image steganography algorithms using generalized exploiting modification direction and pixel segmentation strategy" 2018 35th National Radio Science Conference (NRSC) DOI : 10.1109/NRSC.2018.8354371

[14] Xuejing Niu, Meng Ma*, Rui Tang and Zhaoxia Yin, Image Steganography via Fully Exploiting Modification International Journal of Security and Its Applications Vol. 9, No. 5 (2015), pp. 243-254 http://dx.doi.org/10.14257/ijsia.2015.9.5.24 ISSN:1738-9984 IJSIA Copyright ⓒ 2015 SERSC

[15] Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh, Sahel Alouneh "FPGA Hardware of the LSB Steganography Method" International Conference on Computer, information and Telecommunication System (CITS), 14-16 May 2016

[16] https://www.ni.com/en-in/shop/data-acquisition-and-control/add-ons-for-data-acquisition-and-control/what-is-vision- development-module/peak-signal-to-noise-ratio-as-an-image-quality-metric.html