Data Embedding Method Using Adaptive Pixel Pair Matching Algorithm

Mr. K. Nandha Kumar[1], Mr. R. Anandan[2]

[1]PG Scholar, Department of Electronics and Communication Engineering, Gojan School of Business and Technology, Chennai-52, India
[2]Assistant Professor, Department of Electronics and Communication Engineering, Gojan School of Business and Technology,
Chennai-52, India

Abstract- *Data Hiding or steganography has been an important communication network since people started communication in writing. The main aim in steganography is to hide a secret message within cover media in such a way that an observer cannot detect the presence of contents of the hidden message. Cover images/video are original images without secret data and after embedding secret data they are called as stego images. steganography and cryptography are the parts in digital security the obvious advantage of steganography over cryptography is that messages do not attract attention to themselves, to messengers, or to recipients. The progress in steganography has also led to many serious problems such as hacking, compression, reformat, etc. steganography finds its role in attempting to address these growing concerns, with the use of steganography techniques, it is possible to hide secret information within images, audio and video files which are statistically undetectable. This present work proposes a new data embedding technique which uses two pixels sequentially one after another which is known as pixel pair matching (PPM) technique. The two pixel is then replaced by the searched coordinate to store the digit. The APPM (Adaptive Pixel Pair Matching) method offers lower distortion than DE (Diamond Encoding) by providing more compact neighborhood sets and allowing embedded digits in any notational system.*

Key Words—Adaptive pixel pair matching (APPM), diamond encoding (DE), exploiting modification direction (EMD), least significant bit (LSB), optimal pixel adjustment process (OPAP), pixel pair matching (PPM).

1. INTRODUCTION

As need of Internet-based applications is highly increased, so it is required to use the secrecy in communication. To achieve this goal, there are mainly three techniques are available, cryptography, watermarking and steganography. Steganography is the art of embedding the information through original object in such a behavior that the continuation of the message is unknown. The term steganography is coming from Greek word Steganos, which means, "Covered Writing". The original objects can be referred to as covered/carrier objects. After inserting the secret message in to the cover image it is called as stego image. A stego key is used for hiding. Steganography is different from cryptography. The main objective of cryptography is to secure communications by using encryption techniques. But steganography techniques are used to hide the messages, which makes difficult for a third party / person to find out the message. Watermarking and fingerprinting related to steganography are basically used for academic property protection.

2. DIFFERENT KINDS OF STEGANOGRAPHY

The five main categories of file formats that can be used for steganography are:

2.1 Text Steganography

This method is used to hide a secret message in a text message for that number of tabs, white spaces, and capital letters, just like Morse code is used. In earlier day this technique is in very much boom but after booming of Internet and different type of digital file formats its importance gets decreased.

2.2 Image Steganography

Digital images are widely used over the internet as well as that are also popular. Now using this phenomenon, the digital images can be used as a cover images/objects for the steganography. In this technique a secret message is hided in a digital image through an embedding algorithm with the help of private key to generate a stego image.

2.3Audio Steganography

Audio stenography is another type of steganography in which the properties of the human ear is considered to hide information. An audible, sound can be made inaudible in the presence of another louder audible sound. Audio steganography uses only digital audio formats such as WAVE, MIDI, AVI MPEG or etc.

2.4Video Steganography

Video Steganography is a technique used to hide any kind of files or information into digital video format. Here video is used as carrier for hidden information. Video steganography uses following types of video files such as H.264, Mp4, MPEG, AVI or other video formats.

2.5Protocol Steganography

The term protocol steganography is to embedding information within network protocols such as TCP/IP. We can hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used. The protocol steganography uses the TCP, UDP, IP network protocols for data hiding.

3. STEGANOGRAPHIC TECHNIQUES

Digital image steganography techniques can be divided into following domains:

3.1 Spatial Domain Techniques

There are many versions present in spatial steganography that all are related to make changes directly with some bits of the digital image pixel values to hide data. Least significant bit (LSB) - based steganography is one of the simplest techniques/method that is used to hide a secret message in digital image. In this technique the pixel value of least significant bit (LSB) are get replaced with bits of secret message and all this is done without introducing many perceptible distortions. The embedding of message bits can be done either sequentially or randomly. In spatial domain following techniques comes these are as follows such as LSB substitution/replacement, LSB matching, Matrix embedding and Pixel value, differencing etc.

3.2 Transform Domain Techniques

This is a more complex technique of hiding information in an image. In this various transformation algorithms are used to hide data behind the image [4]. This technique also is termed as a domain of embedding techniques. In this technique a number of algorithms are exists. Most of the strong steganographic systems work in the transform domain because the process of embedding data in the frequency domain of a signal is much stronger than any other domain such as time or etc. Transform domain techniques are more advantageous than spatial domain because it hides information in such parts of image that are less exposed to image processing, cropping and compression. Transform domain techniques are mainly classified as follows:

1. Discrete Fourier transformation technique (DFT).

2. Discrete cosine transformation technique (DCT).

3. Discrete Wavelet transformation technique (DWT).

4. Lossless or reversible method (DCT)

5. Embedding in coefficient bits

3.3 Distortion Techniques

This technique works on the principle of differences between the cover image and the stego image and for that it needs to keep a track of cover image. While embedding the secret message by this technique the encoder adds a sequence of changes to the cover image i.e. way in which and how/where the secret message get embedded. For this process the difference in the signal distortion is considered. But before the embedding a secret message into the cover image it has to encode it for that the encoder chooses the pixels of cover image pseudo-randomly and changes that pixel bit with message bit in a such manner the statistical properties of the image are not get affected. However, this method has one drawback as cover image should never be used more than once. As well as an attacker can easily tampers the stego-image by cropping, scaling or rotating.

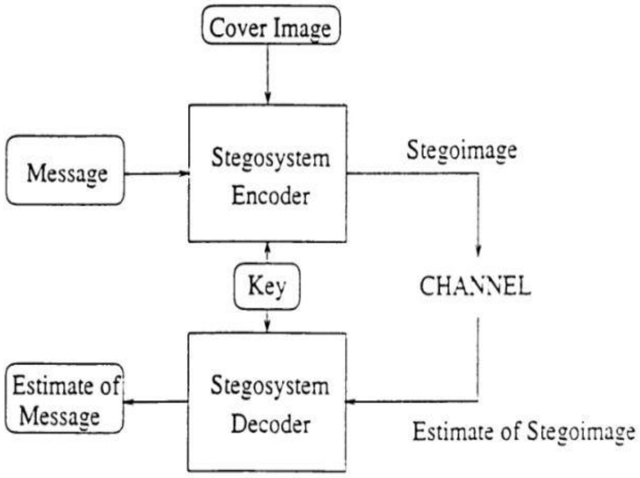


Fig.1. Block Diagram of Steganography

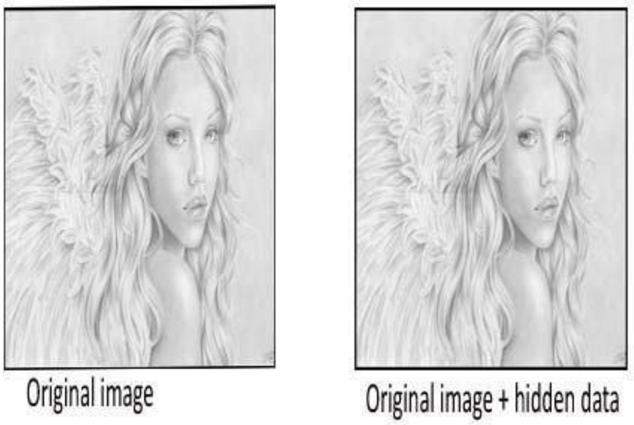


Fig.2. Cover and Stego Image

3.4 Masking and filtering

This technique has resemblance with the technique of paper watermark. In this technique information is get concealed by marking an image for that purpose it uses the noise levels of the cover images. The main advantage of this technique is that the hidden message is more integral to the cover image and watermarking techniques can be easily applied as well as there is no fear of image destruction. This method has one more advantage as it is much more robust than LSB replacement with respect to comparison made based on the following the categories such as compression and the information is hidden in the visible parts of the image. This technique also has the disadvantage as it only works on gray scale images.

4. LITERATURE SURVEY

This section provides the knowledge of different data hiding techniques are used to hide the data. These are as follows:

4.1 Pixel Value Differencing (PVD)

In Paper "An Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods" author proposed a Pixel value difference (PVD) and simple least significant bits scheme are used to achieve adaptive least significant bits data embedding. In pixel value differencing (PVD) where the size of the hidden data bits can be anticipated by difference between the two consecutive pixels in cover image using simple relationship between two pixels. PVD method provides a better imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. This method hides large data with the help of LSB substitution at edge area of image and uses the PVD for smooth region of image to hide the data. Though this technique provides larger capacity but has low visual quality as well as this method is complex.

4.2 LSB Substitution

In paper "Hiding Data in Images by Simple LSB Substitution" authors proposed an LSB substitution for hiding the data into the image. To achieve better visual quality of stego-image it takes care of noise sensitive area for embedding. This method intelligently differentiates normal texture and edges area of an image as well as it takes the advantage of these areas for the embedding. This method analyses the different LSB values as well as edges, texture masking and brightness of the cover image to calculate the number of k-bit LSB for secret data embedding. It also utilizes the pixel adjustment method for better stego-image visual quality through LSB substitution method. Optimal pixel adjustment process is also used to generate the stego-image which is obtained by the simple LSB substitution method. The proposed method also termed as OPAP (Optimal Pixel Adjustment Process). The overall result shows a good high hidden capacity with high image quality of the stego-image can be greatly improved with low extra computational complexity. The main shortcoming of this technique is the worst mean-square-error between the stego-image and the cover image is derived.

4.3 Exploiting Modification Direction (EMD)

In paper "Efficient Steganographic Embedding by Exploiting Modification Direction" author provides a new approach to data hiding scheme by introducing a novel method of steganographic embedding in digital images is described, in which each secret digit in a (2n+1) notational system is carried and hide by n pixels of the cover image. In this method at most only one pixel is increased or decreased by 1. It is not suitable for applications that requiring high payload is the main shortcoming of this technique.

4.4 Diamond Encoding (DE)

In paper "A Novel Image Data Hiding Scheme with Diamond Encoding" author provides a new approach to data hiding scheme by introducing Diamond Encoding. In this technique, first the process is portioning and embedding of the cover image into non-overlapping blocks of two consecutive pixels. Then it transforms the secret messages into a series of digits which are equivalent to those blocks. Afterward the diamond encoding technique is applied on those blocks to calculate the diamond characteristic values i.e. DCV to hide/concealed secret B-ary digits into the diamond characteristic values. After that the diamond characteristic value is gets modified by secret message digit and which can be done by adjusting pixel values in blocks. The main shortcoming of this technique is that it suffers from higher distortion for various lower payload with lower image quality and can be attacked by capacity in terms of payload and performance that can be improved. The PPM-based method, suppose a digit TB is to be concealed. The range of TB is between 0 and B-1, and a coordinate (p', q') in Ø (p, q) has to be found such that f (p', q') = TB. [2] Therefore, the range of (p, q) must be integers between 0 and B-1, and each integer must occur at least once. In addition, to reduce the distortion, the number of coordinates in Ø (p, q) should be as small aspossible. The best PPM method shall satisfy the following three requirements:

1) There are exactly B coordinates in Ø (p, q).

2) The values of extraction function in these coordinates are mutually exclusive.

3) The design of Ø (p, q) and f (p, q) should be capable of embedding digits in any notational system so that the best can be selected to achieve lower embedding distortion. The definitions of Ø (p, q) and f (p, q) significantly affect the stego image quality. The designs of Ø (p, q) and f (p, q) have to fulfill the following requirements: All values have to be

mutually exclusive and the summation of the squared distances between all coordinates in Ø (p, q) and f (p, q) has to be the smallest. This is because, during embedding, (p, q) is replaced by one of the coordinates in Ø (p, q). Suppose there are B coordinates in Ø (p, q), i.e., digits in a B-ary notational system are to be concealed, and the probability of replacing (p, q) by one of the coordinates in Ø (p, q) is equivalent. The averaged MSE can be obtained by averaging the summation of the squared distance between and other coordinates in Ø (p, q).

5 PROPOSED SECURED APPM METHODOLOGY

5.1 Encryption and Decryption Procedure

Before embedding or hiding the secret message in to the cover image it is inputted to encryptor for the encryption. As well as after the extraction process again this secret message is passed to decryptor for decryption and then the original message is obtain. The advantage of this methodology is that it protects the secret message from the attacker under the steganalysis attack. In addition to English language, this secured APPM technique is also able to hide data provided in different languages such as Marathi, Hindi etc.

5.2 Embedding Procedure

The embedding module accepts the encrypted secret message as input from encryptor module and process on it to embed that encrypted secret message in to cover image as a steganography for the secret communication. The output of this embedding module is the stego image which contains a secret message. Suppose the cover image is of size U × U and M is the message bits to be concealed. The size of is T is |T| and key Er.

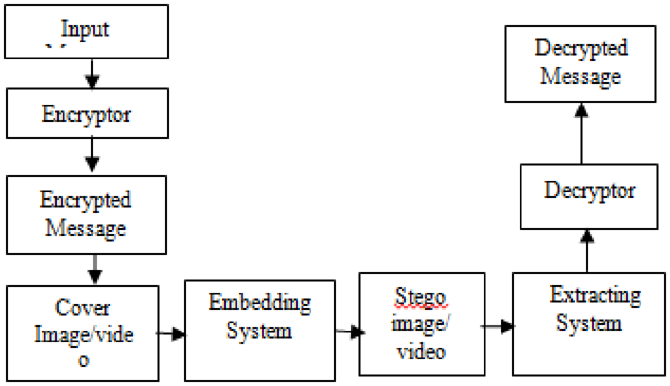


Fig.3. Proposed System

5.3 Extraction Procedure

The extraction module accepts the stego image which contains secret message as an input from the embedding module. The extraction module process on that input and generate cover image and encrypted secret message. This encrypted secret message is then pass to decryptor module to generate plain secret message. To extract the embedded message digits, pixel pairs are scanned in the same order as in the embedding procedure. The message digits which we were embedded in the previous phase is considered / forwarded as the parameter values of extraction function which is got from the scanned pixel pairs.

1) Construct the embedding sequence j using the key Hr.

2) Select two pixels (p', q') according to the embedding sequence j

3) Calculate f (p', q') and the result is the embedded digit.

4) Finally, the message bits *T* can be obtained by converting the extracted message digits into a binary bit stream.

5.4 Digital Watermark

In digital watermark module a digital watermark is implemented. A digital watermark is a kind of marker which is secretly embedded in a noise-tolerant signal such as image, video, audio and text etc. Digital watermarks may be used to verify the authenticity; integrity of the carrier signal as well as it shows the identity of its creator/owner. It gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (Authentication and non repudiation) and that the message was not altered in transit (i.e. to maintain integrity). As well as watermark gives integrity of message. The digital watermark gives authentication for secured communication. In this system message received from sender is in authenticated form and with security in communication. Due to this sender cannot deny about message sent by him and this also assures that message was not altered in transit.

6 RESULTS AND ANALYSIS

This section shows the various types of results of Secured APPM technique with different parameters. These results show improvement over previous APPM techniques with respect to Mean Square Error (MSE). The cover and stego images which do not show any artifacts after applying Secured APPM technique to the cover image to hide the secret message in to it.

Fig.4 Cover Image and Stego Images

(a) Cover Image (b) Stego Image

The Table 1 shows the comparison of MSE between the secured APPM technique with the previous technique such as APPM, DE, LSB and OPAP etc

Table 1 MSE comparison of proposed method (Secured APPM) with previous APPM method

bpp	B	CB	APPM	Secured APPM	MSE Improvement
			MSE	MSE	
1	4	2	0.375	0.25	0.125
1.161	5	2	0.4	0.1666666	0.23333
1.850	13	5	1.077	1.0660000	0.011
2.679	41	6	3.341	3.1666666	0.17433
3	64	14	5.203	4.8095238	0.39347
3.205	85	10	6.847	6.8333333	0.01366
3.410	113	31	9.071	8.6021505	0.46884
4	256	92	20.518	19.550724	0.96727

The Table 1 shows the improvement of Mean Square Error (MSE) as compared to previous APPM data hiding technique

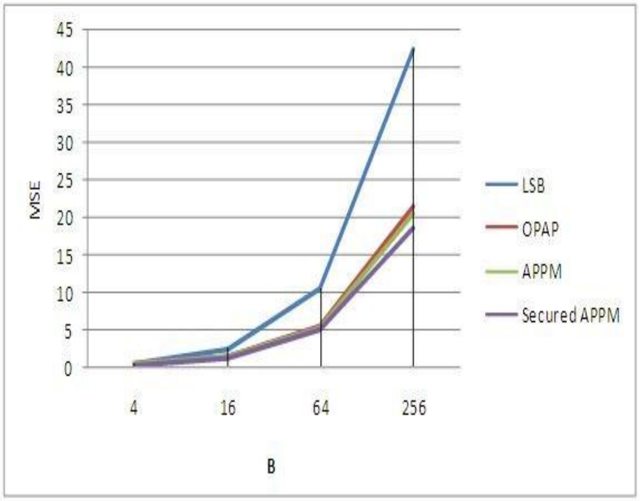


Fig.5. Payload - MSE Relationship Comparison of Various PPM-Based Methods

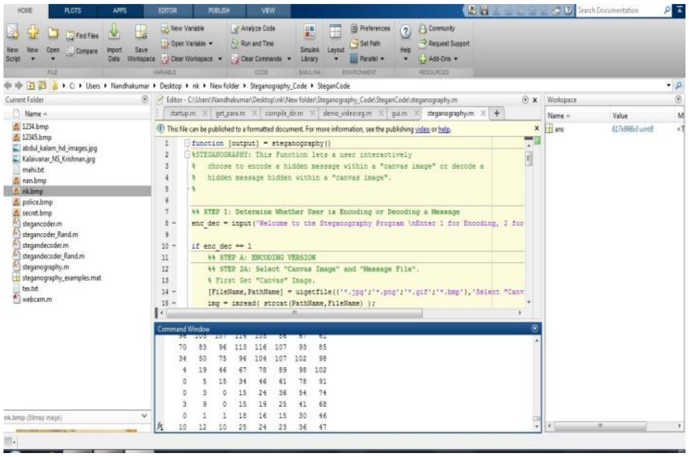
Table 2 MSE Comparison for various types of images

CB = 7, B = 32, payload = 2.480 bpp			
Images	APPM	Secured APPM	MSE Improvement
	MSE	MSE	
Lenna	2.604	2.466	0.138
Jet	2.609	2.466	0.143
Boat	2.598	2.59	0.008
House	2.6	2.53	0.07
Elaine	2.582	2.49	0.092
Average MSE	2.5986	2.5084	0.0902

CB = 3, B = 9, payload = 1.526 bpp			
Images	APPM	Secured APPM	MSE Improvement
	MSE	MSE	
Lenna	0.642	0.54	0.102
Jet	0.648	0.54	0.108
Boat	0.64	0.53	0.11

House	0.632	0.57	0.062
Elaine	0.638	0.57	0.068
Average MSE	0.64	0.55	0.09

The Table 2 shows the performance improvement of Secured APPM technique over the APPM technique. This table shows the performance improvement of MSE and with payload of 3.815 bpp, 2.480 bpp and 1.526 bpp.


Editor - C:\Users\Nandhakumar\Desktop\nk\New folder\Steganography_Code\SteganCode\steganography.m

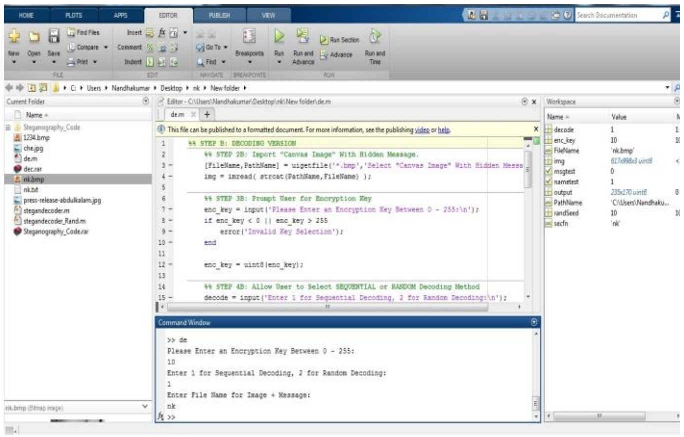
This file can be published to a formatted document. For more information, see the publishing video or help.

```
function [output] = steganography()
%STEGANOGRAPHY: This Function lets a user interactively
%   choose to encode a hidden message within a "canvas image" or decode a
%   hidden message hidden within a "canvas image".
%

%% STEP 1: Determine Whether User is Encoding or Decoding a Message
enc_dec = input('Welcome to the Steganography Program \nEnter 1 for Encoding, 2 for

if enc_dec == 1
    %% STEP A: ENCODING VERSION
    %% STEP 2A: Select "Canvas Image" and "Message File".
    % First Get "Canvas" Image.
    [FileName,PathName] = uigetfile({'*.jpg';'*.png';'*.gif';'*.bmp'},'Select "Canv
    img = imread( strcat(PathName,FileName) );
```

Command Window

```
   70    83    96   113   116   107    93    85
   34    50    75    96   104   107   102    98
    4    19    46    67    78    89    98   102
    0     5    15    34    46    61    78    91
    0     3     0    15    24    36    54    74
    3     9     0    15    19    25    41    68
    0     1     1    18    16    15    30    46
   10    12    10    25    24    23    36    47
```

Embedding Procedure Form


Editor - C:\Users\Nandhakumar\Desktop\nk\New folder\de.m

This file can be published to a formatted document. For more information, see the publishing video or help.

```
%% STEP B: DECODING VERSION
    %% STEP 2B: Import "Canvas Image" With Hidden Message.
    [FileName,PathName] = uigetfile('*.bmp','Select "Canvas Image" With Hidden Messa
    img = imread( strcat(PathName,FileName) );

    %% STEP 3B: Prompt User for Encryption Key
    enc_key = input('Please Enter an Encryption Key Between 0 - 255:\n');
    if enc_key < 0 || enc_key > 255
        error('Invalid Key Selection');
    end

    enc_key = uint8(enc_key);

    %% STEP 4B: Allow User to Select SEQUENTIAL or RANDOM Decoding Method
    decode = input('Enter 1 for Sequential Decoding, 2 for Random Decoding:\n');
```

Command Window

```
>> de
Please Enter an Encryption Key Between 0 - 255:
10
Enter 1 for Sequential Decoding, 2 for Random Decoding:
1
Enter File Name for Image + Message:
nk
>>
```

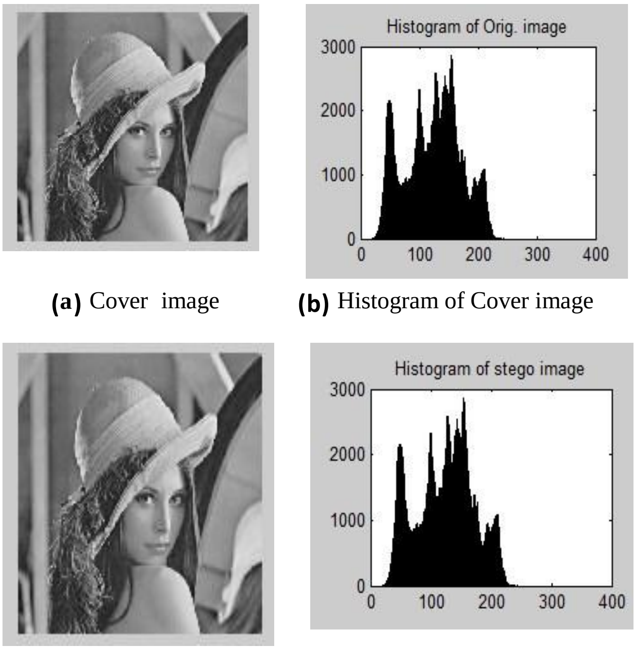
Extraction Procedure Form

7 PERFORMANCES AND SECURITY ANALYSIS

In this section, we analyze the security of Secured APPM under statistical steganalysis schemes, including the HVDH scheme. The HVDH [15] scheme is used to detect the presence of hiding message according to the distance between vertical and horizontal histograms. [15] The proposed a detection method based on the statistical analysis of histogram differences. Zhao *et al*. [15] observed that for many pair wise embedding methods, the difference between the horizontal difference histograms and vertical difference histograms are significantly altered. Zhao *et al.* [15] use the distance between H_h and H_v as a statistical detector to detect the abnormality of histogram. [15] The distance is defined as

$$D = \left(\sum_{i=-2T}^{2T} \left(\widehat{H}_h(i) - \widehat{H}_v(i) \right) \right)^{\frac{1}{2}}$$

T is a predefined threshold. A larger D indicates that H_h and H_v have larger differences and thus, the image is likely to have messages embedded. [2] The fig.8 shows the security analysis and comparison of histogram of stego and cover images. From these figures we can say that the histogram of cover and stego images are equal. To detect the presence of secret message we employ the security analysis and steganalysis attack on these images but the results produced from them shows that the Secured APPM technique is secure under the detection of some well lknown steganalysis techniques.



(a) Cover image **(b)** Histogram of Cover image

(c) Stego Image **(d)** Histogram of Stego image

Fig.8. Security Analysis and Comparison of Cover and Stego Images

8 CONCLUSION

This paper proposed a simple and efficient data embedding method named as Secured APPM based on APPM. In that two pixels are used as an embedding unit and a specially designed compact neighborhood set is used to embed secret message digits in to a smallest possible notational system by allowing users to select digits in any notational system for the data embedding. The proposed method not only resolves the low-payload problem in EMD, but also offers smaller MSE than OPAP, DE and APPM. It also provides a better image quality because Secured APPM does not produce any artifacts in stego images. The steganalysis results of stego images are similar to those of the cover images, which offer a secure communication under adjustable embedding capacity. It also contains additional features such as digital watermark and encryption of secret messages for the provision of more security. The secured APPM technique is also able to hide all different types of data provided to it in languages like English, Marathi, and Hindi etc. As well as this technique is secure under the detection of some well-known steganalysis techniques. All these various features made a Secured APPM technique a straightforward, economical embedding method for the data hiding. In future Secured APPM may have a chance to increase the capacity of data embedding in the cover images of it. Also there may be a chance of little improvement of MSE in it and chance to provide more security.

ACKNOWLEDGMENT

Sincerely thank the all experts who have contributed towards development of this paper.

REFERENCE

[1] W. Zhang, X. Zhang, and S. Wang, “A double layered plus-minus one data embedding scheme,” IEEE Signal Process. Lett, vol. 14, no. 11, pp. 848–851, Nov. 2007.

[2] Wien Hong and Tung-Shou Chen, “A Novel Data Embedding Method Using Adaptive Pixel Pair Matching”, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 1, February 2012.

[3] R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, “A novel image data hiding scheme with diamond encoding,” EURASIP J. Inf. Security, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.

[4] Swapnil S. Thakare and Niranjan L. Bhale, “A Review of Digital Image Steganography Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014, pp. 465-471, ISSN: 2277 128X.

[5] M. Lakshmi Prasanna and Sk. Mahaboob Basha, “Extended Adaptive Pixel Pair Matching”, International Journal of Engineering Research and Applications, Vol. 3, Issue 3, May-Jun 2013, pp.1484-1490, ISSN: 2248-9622.

[6] Pratap Chandra Mandal, “Modern Steganographic technique: A Survey”, International Journal of Computer Science & Engineering Technology (IJCSET) Vol. 3 No. 9 Sep 2012.

[7] Mehdi Hussain and Mureed Hussain, “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology Vol. 54, May, 2013

[8] Hsien-Chu Wu Na-I Wu Chwei-Shyong Tsai MinShiang Hwang, “An Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods”, National Science Council, Taiwan, Nov 2004.

[9] X. Zhang and S. Wang, “Efficient steganographic embedding by exploiting modification direction,” IEEE Commun. Lett. vol. 10, no. 11, pp. 781–783, Nov. 2006.

[10] K. Chan, L. M. Cheng, “Hiding data in images by simple LSB substitution”, Pattern Recognition, vol. 37, no: 3, pp: 469–474, 2004.

[11] J. Mielikainen, “LSB matching revisited,” IEEE Signal Process. Lett. vol. 13, no. 5, pp. 285–287, May 2006.

[12] J. Fridrich and D. Soukal, “Matrix embedding for large payloads,” IEEE Trans. Inf. Forensics Security, vol. 1, no. 3, pp. 390–394, Sep. 2006.

[13] W. Hong and T. S. Chen, “Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism,” J. Vis. Commun. Image Represent, Vol: 22, no. 2, pp. 131– 140, 2011.

[14] M. Tanvir Parvez and A. Abdul-Aziz Gutub, “RGB Intensity Based Variable-Bits Image Steganography”, IEEE Asia-Pacific Services Computing Conference, pp. 1322-1327. 2008.

[15] H. Zhao, H. Wang, and M. K. Khan, “Statistical analysis of several reversible data hiding algorithms,” in Proc. Multimedia Tools and Applications, 2009, DOI: 10.1007/s11042-009-0380