DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4528

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

HIGH DATA EMBEDDING USING LSB AND PIXEL INTENSITY BASED METHODS

Rasmi.A
Research Scholar
KarpagamUniversity, Karpagam Academy of Higher Education, Tamilnadu

Dr.Mohanapriya.M.
Professor Department of Computer Science
KarpagamUniversity Karpagam Academy of Higher Education, Tamilnadu

Abstract: This paper proposes a high capacity data embedding based on the basic principles of least significant bit method and pixel intensity features of spatial domain steganography techniques. The designed methods will boost the embedding capacity as well as the safety of the embedded information without degrading the quality of the stego file. Data hiding can be implemented by embedding an electronic file into another electronic file for ensuring security through the existing transmission modes. Because of the wide spread use of an open network for transmitting the data from one person to an intended party ,intruders can easily recognize the presence of data, hence necessary measurements should be taken in order to avoid it. This paper describes the background and features of newly reworked LSB method and pixel intensity based method, so it will be more helpful for researchers to develop novel techniques for data hiding by combining factors like high payload and data security. Based on the experimental calculations, the proposed methods can conceal more amounts of data than the conventional steganographic methods and thus ensures more security.

Keyword: Steganography,Spatialdomain,Embeddingcapacity,Robustness,datahiding,stego,cover image, LSB,Pixelintensity,Gray scale image.

1. INTRODUCTION

The rapid development of web technology enables the transmission of data files through internet in a speedy manner irrespective of the traditional transfer methods. Data hiding is a technique that masks the embedded secret information for transmitting over long distances tenaciously. Information concealing procedures can be graded into irreversible information hiding schemes and reversible (lossless) information hiding schemes. Nowadays information technology and security plays a vital role in our modern world. So to ensure security different information hiding methods have been evolved, they can be classified as watermarking, cryptography, finger printing and steganography. The purpose of data hiding is to provide improved secret communication. The word Steganography is derived from Greek words Steganós, and Graptos which means "concealed writing".In today's world everyone desires some safety measures to information exchanged through telephone, internet or any digital media. So up to a certain extent security can be ensured by using different data concealing ways .Data concealing means hiding the data into digital files like image, audio, video, text etc. Hiding of data can be implemented with the help of a set of rules, which will help the sender to insert the secret information into digital objects. The characteristics of hiding techniques are defined by features like capacity, robustness and imperceptibility. Imperceptibility closely related to the term security, which facilitates the data to be unnoticed by the human eye. Some of the existing data masking methods are watermarking, finger printing, cryptography and steganography. The mode of selection of these methods are based on certain criterion like security measures and the amount of data to be hidden without noticed by an intruder or spy, because the leakage of information may cause severe impact on the society. As the amount of information being transferred through web increases day by day, shielding of data from unauthorized access is crucial, so it can be implemented by the effective use of a well-designed security system which enhances the confidentiality and integrity during transmission.[1,3,6,16].

Cryptography method uses encryption and a decryption algorithm, encryption algorithm encrypts the message before sending and at the receiver section decryption takes place. The message before encryption is called plain text and after encryption it is known as cipher text. Cryptography is a widely used overt secret writing and thus makes a message unreadable by a third person .Steganography is an art of communication embedding secret information into the cover medium, so only the permitted person can access the hidden message. Original image without modification is known as cover image, after embedding data, cover image becomes stego image, that is stego=cover + information. Steganographic techniques use files like image, audio, video and text as the cover object. This method does not alter the content of secret data, but just conceals it inside a cover file. Steganographic terminologies can be described as the cover medium, secret data and the stego medium. The data is the secret message that wants to be transmitted confidently. Cover image is used as a carrier to hide the secret data. Data is the message to be transmitted; it may be image, audio, video or text file. Actual data to be embedded is known as payload. Images are the more reliable forms for steganographic communication. Steganography is mainly applicable in the area of military and intelligent agents [3, 4, and 5].

2. RELATED WORK

The main goal of steganography is to hide the data inside other risk free information in such a way that doesn't allow any spy to perceive the presence of a secret data. The main

challenges in hiding techniques are based on how effectively embedding can be done in a cover image, without altering the visual appearance. So before embedding certain measurements should be taken such as the embedded message size should never exceed the cover size, otherwise it might be easily detectable by third one. Depending on the type of cover file used steganography can be categorized as image steganography, network steganography, video steganography, audio steganography and text steganography. In image steganography the cover medium is an image file, whereas in network steganography network protocols like TCP, UDP, IP etc acts as the carrier file. When taking video as a cover file for data hiding it is called video steganography.In audio steganography audio file acts as a carrier ,but in text steganography information is hidden in text files that is text file acts as a cover medium. The most commonly used steganography format is image. Main components of an image steganography are cover image, data, embedding algorithm, extracting algorithm and the stego image. Using the embedding algorithm messages are embedding into the cover file at the sender part, while at the receiver section the embedded message is extracted from the stego file with the aid of an extraction algorithm. Key is optional based on procedures used for embedding and extraction process. A digital image can be represented as I (j,k), j=1,….n, and k=1,…..m, is a set of n×m matrix of pixels, where each pixel is an element of the image . Generally an image is a group of pixels, the number of bits in an image is indicated as the pixel depth.[2,4,5,6,7].

The performance and efficiency of steganography can be evaluated by certain factors like security, data embedding capacity and robustness. Embedding capacity is the maximum size of data that can be hidden into the cover without affecting the features of cover medium. Robustness attribute helps to maintain the data intact even though the stego has undergone modifications like cropping, filtering and scaling. The main criterion for determining the steganographic performance is mainly based on the quality of stego image, so a better stego provides good security and imperceptibility for the concealed data. Steganography techniques can be partitioned into spatial domain technique and transform domain technique. In spatial domain image pixels are modified directly, whereas in transform domain modifications are done indirectly .Spatial domain based steganographic techniques can be classified as least significant bit method(LSB), pixel value differencing technique(PVD),random pixel embedding technique(RPE),edge based data embedding technique(EBE),pixel indicator method, and pixel intensity based method. The most common image formats on internet are Graphics interchange format (GIF) and Joint photographic experts group (JPEG), but the most trendy image format is JPEG, because of its better concealment power .Gray scale images are entitled as monochromic, because of the absence of colour information. Security of the inserted data mainly depends upon factors like the size of cover file and the amount of information to be hidden, if the payload exceeds the cover image, then the modifications will be detected easily, otherwise it offers high imperceptibility. Steganographic security could be enhanced by using certain factors like proper selection of cover image, reducing the payload distortion and improving the message embedding capacity.

The stego image quality could be evaluated by applying the peak signal to noise ratio (PSNR).It is generally expressed in the logarithmic decibel unit dB. Peak signal to noise ratio is expressed as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

In the above representation MAX_I is 255 for gray scale images, and MSE denotes the mean squared error. MSE computes the difference between the cover file and stego image and it is calculated by using the following expression.

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where I (i,j) is the cover image ,K(i,j) is the stego image, ‘m’ denotes the height and ‘n’denotes the width of the image. [6, 8, 9, 10, 15].

A. LSB Based Steganography

Steganography is the art and science of covert secret communication. There exists a variety of spatial domain techniques for data hiding in steganographic field, but the most well-known type is least significant bit method. The LSB method doesn’t alter the content of data, it merely hides the data inside another file known as cover image. The most commonly used method for data covering is LSB ,in which the least significant bit of the cover file is directly replaced by the data to be sent .Consider the pixel value of an image is represented as Pi, and its equivalent binary values are given below:

$Pi = (b_7b_6b_5b_4b_3b_2b_1b_0)_2$

Where b_7 is the most significant bit and b_0 is the least significant bit. Based on the type of LSBemployed, we can insert data bits in between b_7 and b_0, by replacing the corresponding bit with the secret data. LSB replacement is based on the number of bits of pixel present in an image, in the case of gray scale images each pixel is represented as a group of 8 bits, so the least significant bit of each pixel is modified by the bit of secret data to be embedded, whereas in colour image it uses 24 bits to represent the pixel, so we can store 3 data bits in each pixel. It is a simple and straight forward way of inserting data into the cover medium. For example consider a 24 bit image format is as follows:

(10110011 01101100 10010110)
(10110110 11001101 00111110)
(10110101 01100011 10001110)

The message to be embedded into the least significant bit of the image is 11010110,so after applying LSB technique we get the resulting stego as shown below:

(10110011 01101101 10010110)
(10110111 11001100 00111111)
(10110101 01100010 10001110)

The main advantage of this method is its simplicity and ease of use, makes it more suitable for many application areas. In this case the stego image changes are less noticeable by the human visual system so the secret data cannot be easily identified. The major drawback of this method is that it can

be easily detectable by an intruder, based on the value of least significant bit.

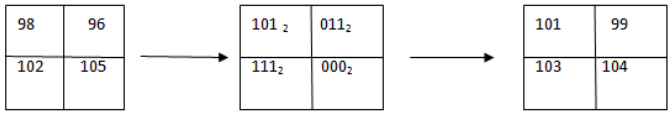

Figure: 1 LSB using 3 bit replacement method

Figure (1) shows the LSB using 3 bit replacement.In this technique the last 3 bits of cover image is replaced by the secret bits, so we get the stego image. For example consider the pixel value of cover image as 102, then convert into the corresponding binary bits, so the resulting value is $(01100110)_2$, next step is replacing the last 3 bits of the cover image with the secret data, here message is $(111)_2$, so after replacing with secret data, the binary representation becomes $(01100111)_2$, and its decimal value is 103. In this way the stego image is formed. Figure (2) represents LSB using 2 bit replacement.

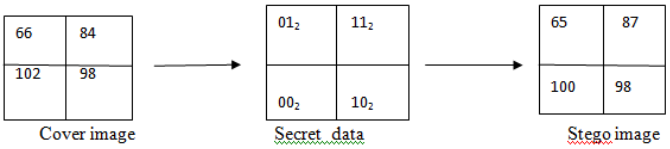

Figure: 2 LSB using 2 bit replacement method

LSB using 2 bit replacement is same as 3 bit replacement method. In this case the least 2 bits of the cover file is modified using message bits so we the stego image [11, 12, 13, 14, 15].

B. Proposed Method in LSB

In this proposed method the pixel in cover image is divided into two parts, such as least significant part and most significant part. Least significant part consists of 4 bits, including the least significant bit. Most significant bit and the following 3 bits are used as the most significant part, it is also 4 bits. The least significant part is also represented as lower part and most significant part is known as upper part. Each part is a group of 4 bits .After this grouping compare the upper and lower parts with the message bits to find out the resemblance between them, and based on it we can decide which part is more closure to the information bits and then choose that part to store the data, the unused part is used as an index to identify the stored data position. Data may be stored either in least significant part or in the most significant part. Similarly index value part may be upper or lower part, based on the data storage location .Index values are kept in an index table. So with the aid of the index table data extraction can be implemented in an efficient manner. Compared to the existing LSB it offers more security and embedding capacity.

Embedding Algorithm:

1. Choose the cover image and the message bits. Divide the cover image pixel into 2 sections namely least significant part and most significant part.
2. Compare the message bits with the 2 parts to find out which part could be used to store data.
3. If least significant part is more closure, choose that part to store the data.
4. So the remaining part is used as an index part and these are stored in an index table.
5. After placing data into the cover image we get the stego image.

Extraction Algorithm:

1. Select the stego image to retrieve the message bits.
2. Check the index table to trace out the location of data bits. Based on the index value we can easily identify the location.
3. Then retrieve the data bits from stego image, so we get the original message without any distortion.

C. Pixel Intensity Based Technique

The term pixel intensity is used to denote the value of a pixel, the pixel may be gray or colour based on the selection of image file. In gray scale images, each pixel has its own intensity levels or values, and it uses gray intensity based image steganography techniques. In this case each pixel is represented by 8 bits that is it uses 8 bits to denote each pixel so it is capable of showing 2^8 shades of grey level, which ranges from 0 to 255, total 256 gray shades are possible. The lightest possible shade is white and darkest possible shade is black its intensity varies from 0 to 1, whereas zero represents the total absence of black and one indicates the total presence of white. In this method the embedding of data is based on the intensity of pixels, so based on the degree of intensity, payload capacity also varies. The range of gray scale image is 256,where the darkest colour value equals to zero and the brightest colour value is 255.In digital colour images, each pixel is a group of 24 bits ,which consists of three primary colours like red ,green and blue ,each colour is denoted by 8 bits, so it is capable of displaying 2^{24} different shades of these primary colours.[11,12,14,16].

D. Proposed Method Using Pixel Intensity

In this paper a new algorithm is suggested to measure the intensity level of the pixel and then conceal information in the properly selected portions. In the proposed method data embedding is based on the intensity level of the cover file, so to accomplish this cover image is divided into 3 sections based on the pixel intensity value. The three sections are low level, middle level and high level .In order to conceal the message into cover ,message is first converted into bits format, or a byte of array ,then the data is encrypted at the sender side by embedding data in to the lower ,middle and higher levels of the cover image .If the intensity value is in low level ,we can alter the last two bits of the cover image pixel, but one bit must be same as in cover file and data bits, that is one bit remains constant ,then only two bit alteration is possible. In the middle level data insertion can be done by using up to three last bits, but one bit must be same in both cover image and data, then only we could alter three bits, otherwise two changes are possible in the cover pixel. But in higher intensity level, we can change up to the 4 last or least bits in a pixel, whereas one bit in data should be same as the cover image pixel bit. To ensure more security for the embedded message we are inverting the same single bit

present in both files, then we can easily identify the bit. Second level can accommodate more data than the low level, similarly third level inserts more data than the low and middle levels. After selecting stego divide it into three levels based on intensity value then extract the inserted secret message bits from the low region, the middle level and high level region, but based the pixel intensity degree the number of bits may vary from two to four, then combine all bits, and compare with the data bits, so we get the original secret message. Figure (3) depicts the pixel values of a gray scale image. The proposed method offers more capacity and efficiency than the conventional methods.

11	16	23	19	34	79	88	84	210	213
215	145	26	85	28	24	44	84	71	215
23	46	48	90	113	126	118	18	77	81
79	64	66	84	30	211	200	245	138	174
15	93	69	206	155	109	219	135	31	88
45	47	147	98	87	96	35	135	141	104
202	215	115	83	53	43	96	11	47	65
96	68	35	64	74	46	32	16	86	66
23	16	18	85	43	214	210	106	11	101
52	48	29	16	84	47	65	35	38	50

Figure (3) Gray level values of an image

Embedding Algorithm:

1. Select the cover image and secret data to be inserted, and then divide the cover image into three regions such as low level, middle level and high level, based on the intensity value of the pixel.
2. In low level 2 bits can be embedded by the alterations of last 2 bits but one data bit must be same as cover image bit.
3. In middle level, last 3 bits are modified by the data bits,but one bit must be same in both file, otherwise 2 alterations are possible.
4. In high level, the last 4 bits are replaced by message bits, so four alterations are possible, but one bit must be same in both cover and secret data.
5. For identifying the similar bit we are inverting it.
6. So we get the stego image.

Extraction Algorithm:

1. Select the stego image
2. Divide it into 3 intensity regions, like low level, mid-level and high level.
3. First consider low level, then remove the last 2 bits of the pixel.
4. In the middle level extract the last 3 bits
5. Similarly at the high level remove the last 4 bits of the stego.
6. Combine all the extracted bits and then compare with the message to get the original data bits.

3. RESULT ANALYSIS

The proposed steganographic algorithms are compared with the existing methods to evaluate the performance of stego image using PSNR value and data embedding capacity. To study the features of proposed system, it uses Baboon, Elaine and Lena as test images, shown in figures,(a) to (c) represent the cover image and (d) to (f) denote the stego image , here secret data is also in image format. These images are in gray scale format and different experiments have been conducted using the test images to evaluate the efficiency of the proposed system .The analyzed results are summarized in the Table (1) given below. The quality of extracted message depends on PSNR value, that is higher the value of PSNR means better will be the resultant image.

TABLE 1 : PSNR VALUE COMPARISON

Cover image	LSB Method PSNR(dB)	Proposed Method PSNR(dB)	Pixel intensity based Method PSNR(dB)	Proposed Method PSNR(dB)
LENA	39.33	43.34	35.96	38.89
BABOON	36.48	40.45	36.43	39.34
ELAINE	39.89	44.33	34.95	36.98

4. CONCLUSION

This paper proposes an improved version of LSB and pixel intensity based methods to strengthen the security and embedding capacity of transmitted message. The method uses different encoding mechanisms to enhance the performance of stego image in a fruitful manner. The proposed methods have been tested against the traditional image steganography methods and the result analysis demonstrates that the proposed method provides higher embedding capacity with high PSNR value and better image quality .

5. REFERENCES

[1] Tseng, Y.C. , Chen Y.Y. Pan H.K.:'A secure data hiding scheme for binary images', IEEE Trans. Commun., 2002, 50,pp. 1227-1231 .

[2] Pawan R Sharma, Jitendra Mishra“ A Comprehensive Survey on Data Hiding Technique” IRJET e-ISSN: 2395 -0056 Volume: 02 Issue: 04 July-2015.

[3] Gurpreet Kaur, Kamaljeet Kaur “Digital Watermarking and Other Data Hiding Techniques” IJITEE ISSN: 2278-3075, Volume-2, Issue-5, April 2013 ,181.

[4] Provos, N. &Honeyman, P., “Hide and Seek: An introduction to steganography”, IEEE Security and Privacy Journal, 2003.

[5] Y.K. Lee, L.H. Chen, “High capacity image steganographic model”, IEEE Proceedings on Vision, Image and Signal processing, Vol. 147, No.3,pp. 288-294, 2000.

[6] X. Liao, Q. Wen and J. Zhang, ”A steganographic method for digital images with four-pixel differencing and modified LSB substitution”, Journal of Visual Communication and Image Representation, vol 22, no 1, pp. 18, 2011 .

[7] A. Rashid and M. K. R. Rashid, “Stego-Scheme for Secret Communication in Grayscale and Color Images”, British Journal of Mathematics and Computer Sciences, vol. 10, no, 1 (2015), pp. 1-9.

[8] Sandeep Kaur ,Arunjot Kaur &Kulwinder Singh” A Survey of Image Steganography” IJRECE, Volume 2-Issue 3 June 2014, e-ISSN 2321-3159 p-ISSN 2321-3159.

[9] C.-H. Yang, C.-Y. Weng, H.-K. Tso, and S.-J. Wang, “A data hiding scheme using the varieties of pixel-value differencing in multimedia images,” Journal of SystemsandSoftware, vol. 84,no.4, pp. 669–678, 2011,

[10] Pradhan A, Sharma DS, Swain G. Variable rate steganography in digital images using two, three and four neighbor pixels. Indian Journal of Computer Science and Engineering. 2012; 3(3):457–63.

[11] VikshitRabara,Vatsal Shah “ IMAGE BASED STEGANOGRAPHY REVIEW OF LSB AND HASH-LSB TECHNIQUES”, IJAERD-2014, ISSN : 2348-6406

[12] Amanpreet Kaur, RenuDhir and GeetaSikka, “A New Image Steganography Based on First Component Alteration Technique”, IJCSIS, Vol. 3, No. 6, 2009.

[13] Abdul MonemS.Rahma ,MatheelE.Abdulmunim, Rana J.S. Al-Janabi “New Spatial Domain Steganography Method Based On Similarity Technique” International Journal of Engineering and Technology Volume 5 No. 1, January, 2015, ISSN: 2049-3444.

[14] Souvik Bhattacharyya and GautamSanyal. PMM (Pixel Mapping method) Based Bit plane complexity segmentation (BPCS) Steganography. 978-1-4673-0126-8/11/$26 2011 – IEEE.

[15] Arun Kumar Sonaniya, Rajesh Kumar Rai “A Review on Comparison between Different Image Steganography Methods” IJAECE, Volume 3, Issue 8, November 2014, pp.355-358 ISSN 2278 -141.

[16] Hussain, M. Hussain, M, “Pixel intensity based high capacity data embedding method”, IEEE International Conference Information and Emerging Technologies (ICIET), Pakistan, June 2010.