Improving LSB Steganography using Filtering approach along with AES and RSTEG

Sumayya P I, Sheena Kurian K

Department of Computer Science and Engineering, KMEA Engineering College, Ernakulam, India
sumayya123@gmail.com
Department of Computer Science and Engineering, KMEA Engineering College, Ernakulam, India
sheenakuriank@gmail.com

Abstract: In steganography, sending a secret message securely through the network is done by hiding the message in a cover media. Variant techniques are available for steganography according to the specific needs and the world is competing to develop much efficient techniques than the present methods. A new way of securing the data is proposed here which makes use of the combination of two data securing techniques. The technique improves the security, as the message is not directly embedded in the cover image, instead a filtering based approach is done. Accordingly a status is provided in the LSB of the pixel, which helps in retrieving the hidden message. The proposed method uses the MSB bits of pixels for decision making. Multilevel steganography is done by incorporating retransmission steganography. The embedded message is encrypted before embedding which improves the security level. It is effortful for a snooper to retrieve the actual message as it is very different from the common LSB method. It is being found out that the proposed method hides large data in a single image retaining the advantages and discarding the disadvantages of the traditional LSB method. The Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) and the histogram differences can be used to measure the image quality and efficiency of the technique.

Keywords: Filtering Based Steganography, AES Cryptography, Network steganography, Status bit

1. INTRODUCTION

Immense amount of confidential data is being lost every year by cause of interruption by the snoopers. It must be assured that data is not exposed to attack during transmission across the network. Physical security is the best line of protection in order to keep data safe from illegitimate access. However, physical security is not always an option due to cost and efficiency considerations. Most of the computers in a network are interconnected with each other openly, thereby unveiling their communication and the communication channels that they use. The problem can be tackled by taking into account the important requirements that must be addressed by an encryption algorithm.

The requirement includes confidentiality, authentication, authorization, data integrity and non-repudiation. Confidentiality is the process of keeping the information, private and secret ensuring that only intended recipients can receive it. Authentication is the process of assuring the proof of identity of sender to recipient attempting access to the confidential information. It ensures that the communicating parties are what he or she claims to be. Authorization is the process of providing assurance that one who tries to access the information, has the permissions to access the data. Data Integrity assures that information is not tampered with and an object is not altered illegally during transit. Non-Repudiation is a method of ensuring that the information cannot be disowned. This provides assurance against a party denying a data or a communication that was initiated by them.

Cryptography, Steganography, Digital watermarking are some of the techniques to improve the security features in data transfer over internet. Sometimes encrypting the data itself is not providing needed security and the hiding of information is needed more. Steganography is a technology where modern data compression, information theory, spread spectrum, and cryptography technologies are brought together to satisfy the need for privacy on the Internet. Cryptography is the state in which security engineering meets mathematics which provides the tools that underlie most modern security protocols. It is probably the key enabling technology for safeguarding distributed systems. Cryptography is the lore of securing data whereas the science of analyzing and breaking secure communication is cryptanalysis. For the concealment of information within computer files, a suitable carrier such as text, image, voice, video, or protocol is needed. Digital images are one of the common and most popular cover images due to their frequency on the Internet.

Digital file formats with high degree of redundancy are used for steganography. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. A general classification for the steganographic methods are shown in the Figure 1.1.

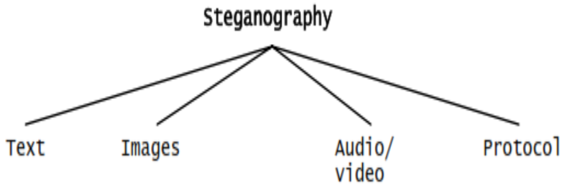


Figure 1.1. Common Steganography methods

Except protocol steganography, all other steganographic methods are independent of the communication protocols used to transmit the data. Multi-level-steganography is based on combining more than one steganographic techniques such that a method is the carrier of another method. Network steganography is based on manipulating the features of a communication protocol in order to send the data secretly. Network steganography is classified into three, Packet modification, modification of packet stream structure and the hybrid methods.

2. PREVIOUS WORKS

There are lots of techniques available that implement steganography on different electronic mediums. N.F. Johnson and S. Jajodia, in their work [5] explains the basic concepts of an image according to a computer. Ira. S. Moskowitz et.al introduced the method of using cryptography and steganography in conjunction in their work [6]. Some of the traditional and novel techniques of data hiding are described by W.Bender et.al. in their work [7]. The development of a packet length based covert channel by using real time packet lengths is explained by Sujata Edekar and Rajeswari Gaudar in their work[8]. Data hiding in communication networks employing the TCP/IP is proposed by D.D.Dhobale et.al. in their work[9]. Stream control transmission protocol is the transport layer protocol that can replace TCP and UDP in the network communications.

3. FILTERING BASED STEGANOGRAPHY COMBINED WITH RSTEG

A digital image consists of several pixels. In the proposed method color image is used as cover image. A colored pixel can be represented as a mixture of red, green and blue color components in appropriate proportions. In binary notation, a color level is represented by a stream of 8 bits. Thus an image is an array of many bytes each representing a single color information lying in a pixel. A pixel is denoted by 24 bits. In the proposed technique the default LSB technique is improved. MSB bit is used for filtering the pixel, to find whether it is eligible for hiding message bit or not. For more security, AES encryption technique is used.

3.1 FINDING OUT THE IMAGE TYPE

A pixel with MSB bits of Red, Green, and Blue component containing atleast 2 bit 1's is a bright pixel, and atleast 2 bit 0's is a darker image. If brighter pixels is greater than darker pixels, select brighter pixels to embed message and vice versa.

3.2 EMBEDDING PROCESS

In an image, color information is arranged byte by byte. A pixel will be represented using 3 bytes R-G-B. A status about the message bit is embedded in the LSB of such a byte. This byte is chosen from a block of spatially adjacent 3 bytes corresponding to a pixel. The binary representation of the ASCII value of alphabets is embedded in the cover image. ASCII value of 'A' is 65. Thus "A" will be embedded in the cover image as "01000001", the binary representation of 65. The choice where the message bit embedded is determined by the MSB of the 3 bytes.

3.2.1. Algorithm for Embedding

1. Get the cover image.
2. Find out the image type.
3. Get the Original message.
4. Encrypt the original message using AES.
5. Convert the cipher bit on consideration into binary number based on its ASCII value.
6. Select the color components of the pixel to which the message to be Embedded (R/G/B/All).
7. Select the first pixel from the cover image.
8. Collect the MSB bits from the pixel's color component bytes.
9. From the MSBs, for lighter image if it contains two bits 1 and for the darker image if it contains two bits 0, select this pixel for hiding message bit. Otherwise, skip this pixel.
10. Convert MSB into decimal number P_n
    a. Compare the value in P_n bit position of the selected color component(s) with the message bit
    b. If it matches, change the LSB of selected pixel's color component(s) as 1(indicate status true).
    c. Else, change the LSB of selected pixel's color component(s), 0(indicate status false).
11. Get the next pixel.
12. Repeat steps 8 to 11 until reached the end of message.
13. Save the stego image.

3.2.2 Embedding Flowchart

The flowchart for embedding an encrypted message in an image using the proposed steganographic method is shown in Figure 3.1.

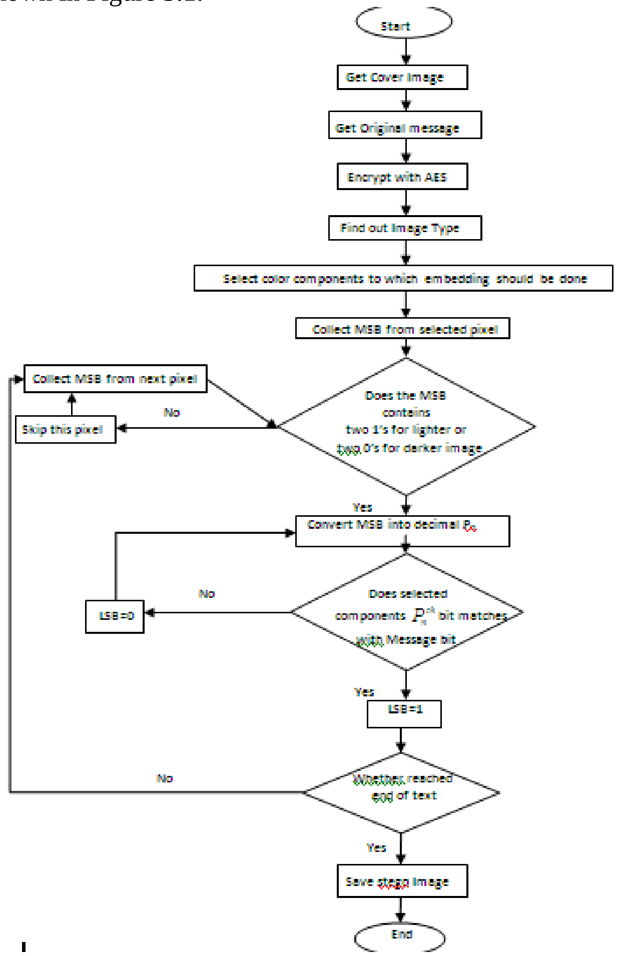

Start
Get Cover Image
Get Original message
Encrypt with AES
Find out Image Type
Select color components to which embedding should be done
Collect MSB from selected pixel
Collect MSB from next pixel
Skip this pixel
No
Does the MSB contains two 1's for lighter or two 0's for darker image
Yes
Convert MSB into decimal P_n
No
LSB=0
Does selected components P_n^{th} bit matches with Message bit
Yes
LSB=1
No
Whether reached end of text
Yes
Save stego Image
End

Figure 3.1. Flowchart for embedding

3.3 EXTRACTING PROCESS

At first collect the Stego image saved after the embedding process. For the extraction process the procedures for embedding should be reversed.

3.3.1. Extraction Algorithm

The algorithm to do extraction of the message from the Stego Image is as follows,

1. Get the stego image.
2. Find out the image type.
3. Get the first pixel of the stego image.
4. Collect the MSBs of the color component bytes.
5. If MSBs contains two bits 1 for a lighter image and two bits 0 for the darker image, select this pixel for extracting the message bit, else skip the pixel.
6. Convert MSB into decimal number, P_n.
   a. Check the LSB of the selected color component.
   b. If it is 1, collect the P_n bit of the selected pixel component as the cipher bit.
   c. If it is 0, collect the cipher bit by toggling the P_n bit of the selected pixel component.
7. Get the next pixel.
8. Repeat steps 4 to 7 until the whole cipher text is extracted.
7. Decrypt the cipher text using AES to get the original message.

3.3.2 Extraction Flowchart

The flowchart for extracting the embedded message from the cover image using the proposed steganographic method is shown in Figure 3.2.

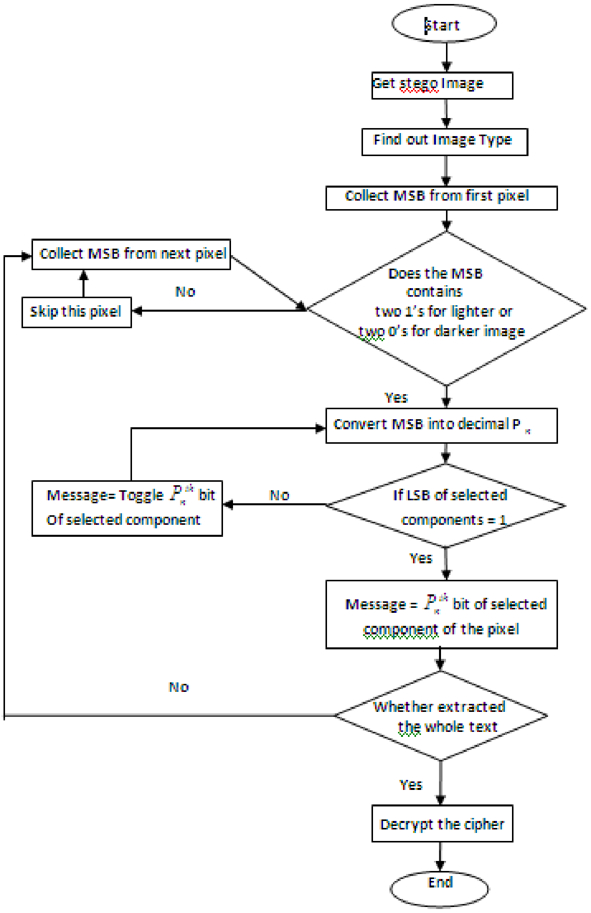

Start
Get stego Image
Find out Image Type
Collect MSB from first pixel
Collect MSB from next pixel
Skip this pixel
No
Does the MSB contains two 1's for lighter or two 0's for darker image
Yes
Convert MSB into decimal P_n
Message= Toggle P_n^{th} bit Of selected component
No
If LSB of selected components = 1
Yes
Message = P_n^{th} bit of selected component of the pixel
No
Whether extracted the whole text
Yes
Decrypt the cipher
End

Figure 3.2. Flowchart for extraction

3.4 MULTILEVEL STEGANOGRAPHY

Multilevel steganography is the process in which atleast two steganographic techniques are utilized. The idea behind is that even after detection of the upper level method which is the carrier of the lower level method, the secret message is left unreadable to an intruder. Network steganography, is a branch of steganography, based on manipulating the features of the communication protocol. Retransmission steganography is introduced to transmit the stego image obtained from the proposed MSB based method.

3.5. RETRANSMISSION STEGANOGRAPHY

To add more efficiency, a multilevel steganography is introduced using the retransmission steganography. RSTEG uses a retransmission mechanism to exchange steganograms. Sender and receiver, aware of the steganographic procedure reliably exchange packets during their connection. At some point during the connection the receiver intentionally doesn't acknowledge a successfully received message. In the context of RSTEG, a sender replaces original payload with a steganogram rather than sending the same packet again during retransmission. TCP/IP protocol is used to transmit the stegoimage from sender to receiver. Whenever a different acknowledgement comes, the stego image is sent instead of retransmitting the previously sent image. As the sender and receiver parties are agreed with the fact that retransmission is transmitting the stego image, they can process it as such. When the retransmitted packet reaches the receiver at an agreed upon time, the receiver can extract the hidden information using the proposed extraction method. But an intruder, if listens to the network thinks that it is just the retransmitted data and do not take more interest in that particular image.

4. EVALUATION MEASURES

Commonly used measures of image quality for comparing stego images with cover results are Mean Square Error, Peak Signal-to-Noise Ratio and histogram.

- **Mean Square Error (MSE)**

MSE is a risk function which measures the average of squares of difference between the estimator and what is estimated. Thus the estimator quality can be assessed by the mean square error. MSE between two images can be given by

$$\text{MSE} = \sum_{i=1}^{x}\sum_{j=1}^{y}\frac{(|A_{ij}-B_{ij}|)^{2}}{x*y}$$

Where A(x,y) and B(x,y) are the images.

- **Peak Signal-to-Noise Ratio (PSNR)**

PSNR is a performance measure for evaluating image distortion. It is classified under the difference distortion matrices and can be applied on stego images.

$$\text{PSNR} = 10\log_{10}\left(\frac{C_{\max}^{2}}{MSE}\right)$$

where, $C_{\max}^{2}$ holds the maximum value in the image.

The PSNR value of the proposed technique will be better than other methods providing an efficient way to embed a message into the image without producing clear distortion. In most cases cover image will be of less significance. Thus a suitable cover image according to user's choice to carry the message can be chosen.

5. IMPLEMENTATION AND RESULTS

The algorithms are implemented using the MATLAB version R2015a. MATLAB provides easier application development and a well-defined user interface. To find out whether the image is lighter or darker, count the pixel values in the image. A pixel value between 0 and 127 is considered as a darker pixel and others are considered as a lighter pixel. To conclude with the image type find out which type of pixels are more in the selected cover image. AES encryption of 128 bit key and 128 bit block is considered.

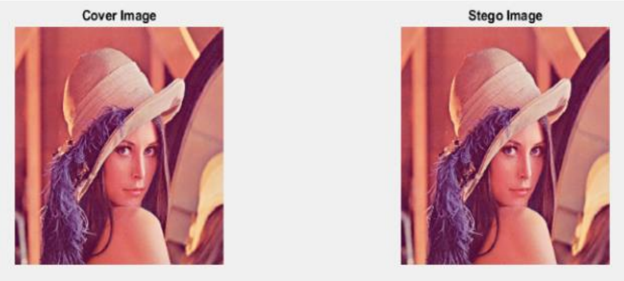
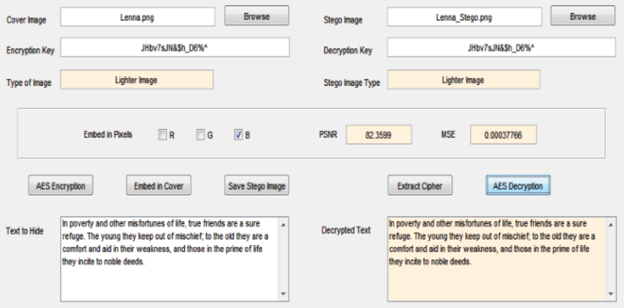


Figure 5.1. Cover image and Stego image Lenna.png



Cover Image: Lenna.png

Stego Image: Lenna_Stego.png

Encryption Key: JHbv7sJN&$h_D6%^

Decryption Key: JHbv7sJN&$h_D6%^

Type of Image: Lighter Image

Stego Image Type: Lighter Image

Embed in Pixels ☐ R ☐ G ☑ B

PSNR: 82.3599

MSE: 0.00037766

Text to Hide: In poverty and other misfortunes of life, true friends are a sure refuge. The young they keep out of mischief; to the old they are a comfort and aid in their weakness, and those in the prime of life they incite to noble deeds.

Decrypted Text: In poverty and other misfortunes of life, true friends are a sure refuge. The young they keep out of mischief; to the old they are a comfort and aid in their weakness, and those in the prime of life they incite to noble deeds.

Figure 5.2. Working with Cover image Lenna.png

On taking the cover image, Lenna.png, it is evaluated as a lighter image. With the Blue component chosen for embedding it comes out with a PSNR of 82.3599 and a MSE 0.00037766. When all the three color components, R-G-B is chosen PSNR comes out to be 78.4245 and MSE 0.0009346. The difference between histograms of original image and the stego image are also negligible.

5.1. Results

The efficiency of the proposed method is analyzed by finding out the Mean squared error and Peak signal to noise ratio and the histogram differences between the original cover image and the processed cover image. Even if the three components of a pixel is used to embed the data, the values of MSE and PSNR comes out to be better than other common algorithms. Values of Mean square error, Peak signal-to-noise ratio for different images and the difference in histograms of cover image and stego image, when embedding is done in only blue component and in all the three components are shown in the Table 5.1.

Table 5.1 : Calculated evaluation measures

Image	Component	PSNR	MSE	Histogram
Lenna	B	91.468	0.000186	0
Lenna	R G B	87.165	0.000503	0.000195
Butterfly	B	81.458	0.000358	0
Butterfly	R G B	74.143	.0019329	0.000378
Baboon	B	86.305	0.000118	0
Baboon	R G B	73.4803	0.0022716	0.000478

6. CONCLUSION AND FUTURE WORK

A new concept of Steganography is introduced in the proposed system. The algorithm does not just replace the message bit but it would replace the status of the message bit. Moreover, Cryptography is merged with it so that the secret message can be secured by two security layers. Instead of inserting the message bits in the cover image, here based on the MSB bits the status is set in the LSB of the pixel. A multilevel steganography is introduced by implementing a retransmission steganography method. In cases where a specific cover image itself is needed to hide the data, checking for the amount of space present to hide the image should be taken into consideration. If the amount of lighter pixels is equivalent to the amount of darker pixels, the space present to hide the text will be less. Such cases where a specific cover image must be used will be rare, however it should be taken into consideration as a future work. Also combining the proposed method with an advanced network steganography method also improves the security and is considered as a future work. The proposed technique fulfills the requirement of steganography technique and is evaluated using MSE, PSNR and histogram.

REFERENCES

[1] Sumayya P I, Sheena Kurian. K, “Two layer security combining MSB based steganography and RSTEG with cryptography, International Journal of Research and Development Organization on 30thseptember 2015, ISSN: 3785 – 0855.

[2] Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin Ashis Kumar Mandal and Md. Delowar Hossain, “*An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography”,* 3rd international Conference on informatics, electronics & vision 2014

[3] T. Morkel, J. H. P. Eloff, and M. S. Olivier, "*An overview of image steganography*" New Knowledge Today Conference Sandton, pp. 1-11, 2005.

[4] J.J.Roque and J.M.Minguet, "*SLSB: Improving the Steganographic algorithm LSB*," Proceedings the Ibero-Americanz Congress on Information Security (CIBSI), Montevideo, pp. 398408, 2009.

[5] N.F. Johnson and S. Jajodia, “*Exploring Steganography: Seeing the Unseen*”, Computer Journal, 1998.

[6] I. Moskowitz, G. Longdon and L. Chang, “*A New Paradigm Hidden in Steganography”,* Proc. 2000 Workshop on new security *paradigms*, Ireland, pp. 41-50.

[7] W. Bender, D. Gruhl, N. Morimoto and A. Lu “*Techniques for data hiding*”, IBM Systems Journal, vol. 35, nos. 3&4, 1996.

[8] Minati Mishra, Priyadarsini Mishra and Flt. Lt. Dr. M.C. Adhikary , “*Digital image data hiding techniques: a comparative study*”, ANSVESA, 7(2), 105-115, 2012, ISSN-0974-715X

[9] J. Lubacz, W. Mazurczyk, and K. Szczypiorski, “Princi*ples and Overview of Network Steganography”,* IEEE Communications Magazine • May 2014 , 0163-6804

[10] Sujata Edekar and Rajeswari Goudar , “*Capacity boost with data security in Network Protocol Covert Channel”*
,
Computer Engineering and Intelligent Systems, ISSN 2222-1719 (Paper),ISSN 2222-2863 (Online)Vol.4, No.5, 2013

[11] D. D. Dhobale, Dr. V. R. Ghorpade, B. S. Patil and S.B.Patil, “*Steganography by hiding data in TCP/IP headers*”, 2010 International conference on advanced computer theory and engineering(ICACTE)

[12] Rupali Gawade, Priyanka Shetye, Vaibhavi Bhosale, and P N.Sawantdesai, “*Data Hiding Using Steganography For Network Security*”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014

[13] W. Bender, D. Gruhl, N. Morimoto and A. Lu “*Techniques for data hiding*”, IBM Systems Journal, vol. 35, nos. 3&4, 1996.

[14] M. Owens, “*A discussion of covert channels and steganography”*,SANS Institute, 2002 .

[15] J. K. Mandal and M. Sengupta, “*Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF)*.”, Proceedings of Second International Conference on Emerging Applications of Information Technology, IEEE Conference Publications, pp 298–301, 2011.

[16] Adam Berent,“*Advanced Encryption StandardSimplified*”, ABI Software Development

[17] Kawaguchi, E. and Eason R., “*Principle and applications of BPCS-Steganography*”, Proc. Multimedia Systems and Applications Conference,USA,vol3528, pp.464-473, 1998.