RESEARCH REVIEW JOURNALS
Volume-03
Issue-11
November -2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Problem with Hidden data in image by Using LSB Technique and Diffie-Hellman Encryption

Ms. Nirmal Kaur

Assistant Professor, Computer Science and Applications Department, Sant Baba Bhag Singh University, Punjab, India

ARTICLE DETAILS

Article History
Published Online: 10 November 2018

Keywords
violator, LSB Technique, numerous Technique, Stego Image, Stego Key

ABSTRACT

This research paper provides information on a strategy used to hide data inside images to protect data from attackers. This encryption of data within an image is commonly known as Image Steganography. This implementation was done with the help of MATLAB. The proposed system hides data inside the image using the LSB (Least Significant Bit) process. The results show that the original image is similar to that of the Stego Image which does not attract the attention of the criminal that something is hidden under it which is a great advantage of this process. In the proposed system, we have introduced the encryption key also known as the Stego Key and LSB methods that improve system security.

1. Introduction

With the rapid development of technology, the use of transmission methods is increasing. “As the IT sector grows, more and more confidential information will be sent using the transfer method. These types of data require some form of security to be transferred to a medium that can be provided with various techniques such as cryptography, authentication, steganography, and much more. Our research focuses on steganography which means putting one type of data in one place or another. In other words, steganography means hiding one type of data from the same type of data or another. The main advantage of steganography over other techniques is that it does not capture the attention of the participant as it is very difficult for them to trace that certain data is hidden within another path and cryptography means converting data into another method by distorting the data. in another case. In this program, the concept of steganography imagery is integrated with encryption technology to improve data security. There are many strategies to achieve this, but the proposed system uses the LSB method to encrypt the data inside the image and continues to use the Diffie-Hellman encryption algorithm to encrypt the data which makes the system more secure. In short, the proposed program is a combination of Image Steganography and Cryptography.

2. Image Steganography:

Image Steganography is about hiding data inside an image. Image Steganography is mainly divided into three strategies. Spatial Domain

1. Frequency Domain
2. Masking and Filtering

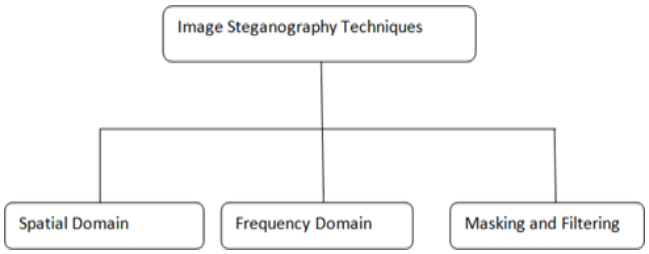

Figure 1: Image Steganography Techniques

Spatial Domain: Spatial Domain is the main technique that is used for hiding the contents of data into image. It uses the pixels intensity to hide the data within an image. It can be performed in many ways.

But LSB (Least Significant Bit). Dependent is the main technique that falls under spatial domain. It hides the data within the pixel values without any change in the original image [1]. It is further divided into three parts.” These are LSB Replacement, LSB Matching and Matrix Embedding.

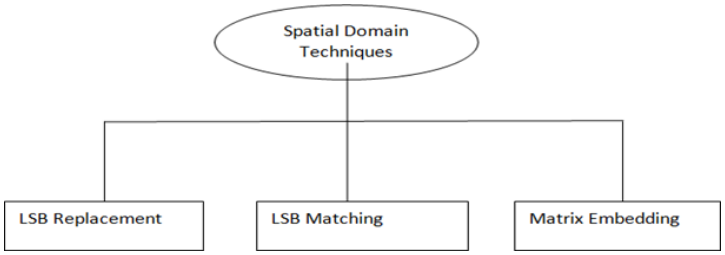

Figure 2: Spatial Domain Techniques

LSB Switch:" In this case, the encrypted message is replaced with the LSB pixel. This process works by converting fragments where LSB fragments are found [2].

LSB Match: It is an improved version of the LSB switch. It works by random deletion and increases the number of pixel covers [3]. Matrix Embedding: Uses debug method to embed a message in the first image. Bits are randomly embedded that increases the speed of the strategy.

Frequency Domain Steganography: This type of Image Steganography is usually done in a JPEG file format. In this case, the data is converted by image coefficients which increase the ability to hide information and provide additional data protection. It is also divided into three categories. "These are DWT (Discrete Wavelet Transformation), DCT (Discrete Cosine Transformation), and DFT (Discrete Fourier Transformation)."

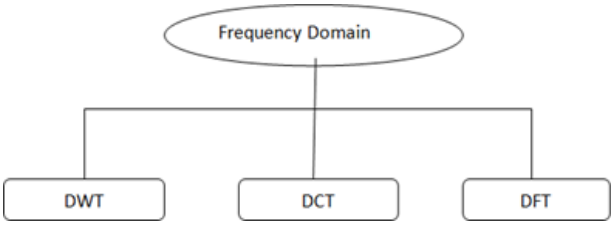

Figure 3: Frequency Domain Techniques

Different Wavelet Modifications: In Discrete Wavelet Transformation, the function is obtained from time to time which takes the average value as zero [4].

Unique Cosine Transformation: In Discrete Cosine Transformation, Cosine Transformation is used that converts 8 * 8 pixel block size to cosine 64 coefficient. Each 8 * 8 block has a value of F (x, y) as a coefficient of F (u, v)

Discrete Fourier Transformation: "In Discrete Fourier Transformation, the image is divided into cosine and sine values. Time and space information is converted into a frequency domain [6].

Masking and Filtration: This technique is applied on images which are in gray scale. This technique hides messages in significant areas not in the noisy part of an image.

Diffie-Hellman Encryption Algorithm: This algorithm is used to encrypt the data that is convert plaintext to cipher text. It is an algorithm that is based on exchanging the keys between two parties. It is an example of Asymmetric Encryption." This algorithm was discovered by Whitfield Diffie and Martin Hellman. Hence, this algorithm got its name from the last name of their developers.

Algorithm III Used: In this system, the algorithm was proposed on both sides of the sender side and the receiver side. The following is the sender-side algorithm.

On the sender's side, in the first step, the text file (private message) is encrypted with the help of the Diffie-Hellman Encryption algorithm using the secret key. The data is then converted into a binary form. During these steps, the image cover is also converted to binary form. Then this binary data with a secret message and cover image is exchanged using the Less Insignificant Bit process and a stego image is created that contains confidential information inside it. This algorithm is used on the sender's side when data is transferred to the transmission point to the recipient."

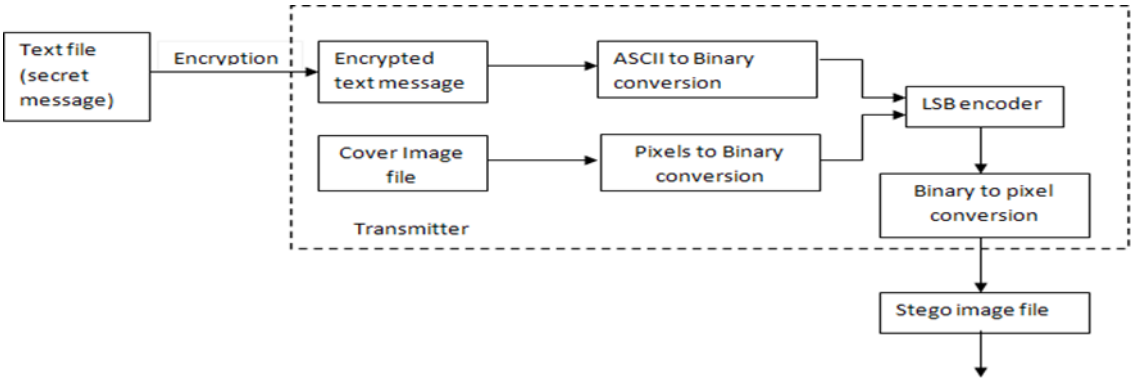

Figure 4: Algorithm Used at Sender Side

On the recipient's side, "the recipient receives a picture of stego and in this photo the recipient receives a private message sent by the sender. The pixels of this stego image are first converted to binary form so that the Slider Keyboard can record the message from the image. After that, the encrypted data and the cover image are separated from each other. Then the binary type of confidential information is converted to ASCII form and the binary type of image is converted into pixels. Finally, encrypted text is encrypted with the encryption algorithm using the secret key used during encryption." Then the cover photo and private message are removed.

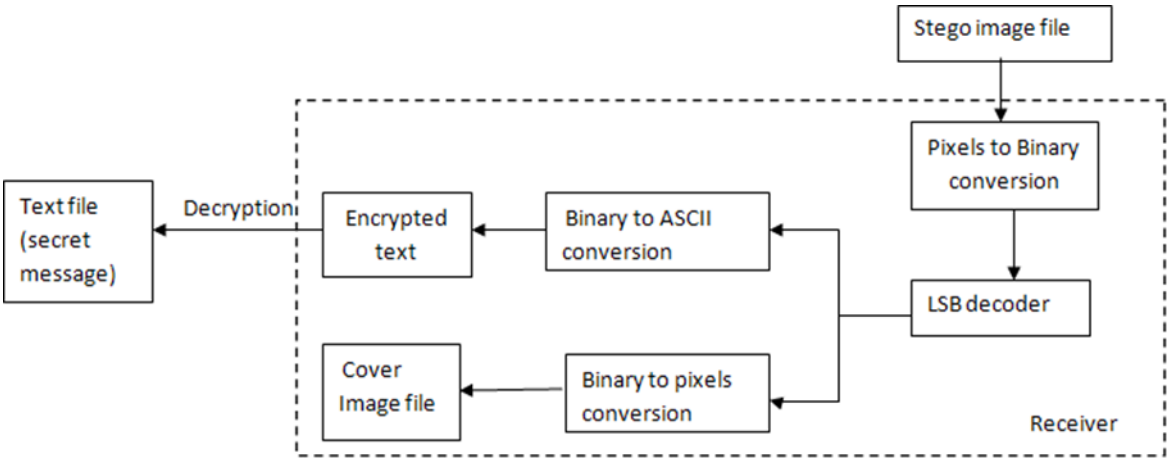

Figure 5: Algorithm Used at Receiver Side

3. Results:

"The proposed System helps in hiding confidential information from the intruder. The system is tested on 30 images and result shows that the data is successfully embedded into an images and retrieval of data takes place after applying a secret key. Figure 7 to Figure 12 shows the output given by the proposed system".

Step 1: Encryption of Message: In this step, the message is encrypted with the help of Diffie-Hellman Encryption algorithm.

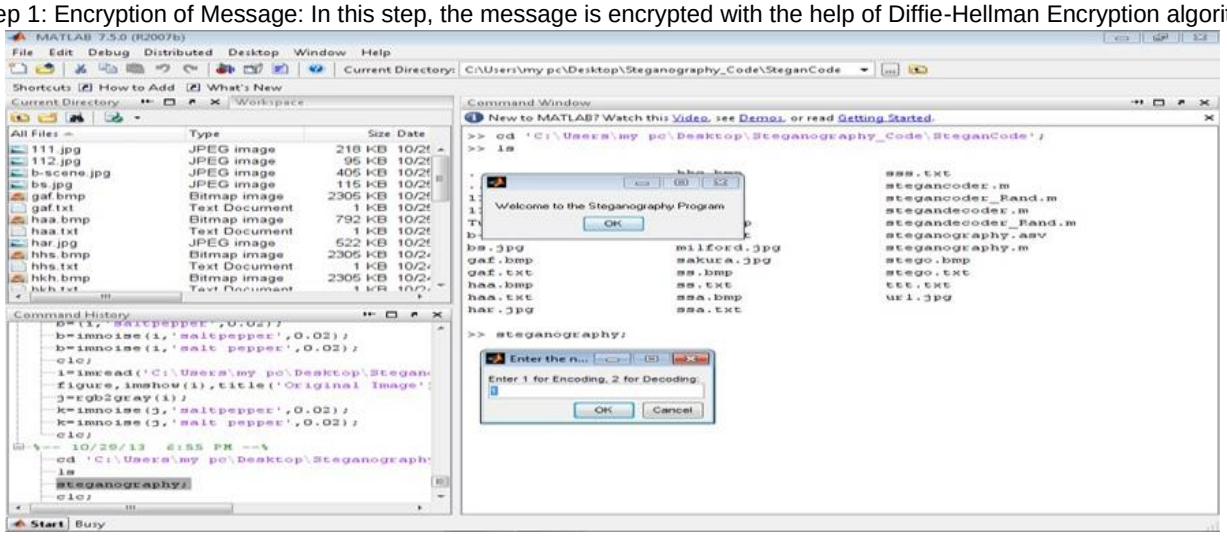

Figure 6: Encryption of Message

Step 2: Selection of Canvas Image: In this step, a cover image is selected under which a secret message is enclosed.

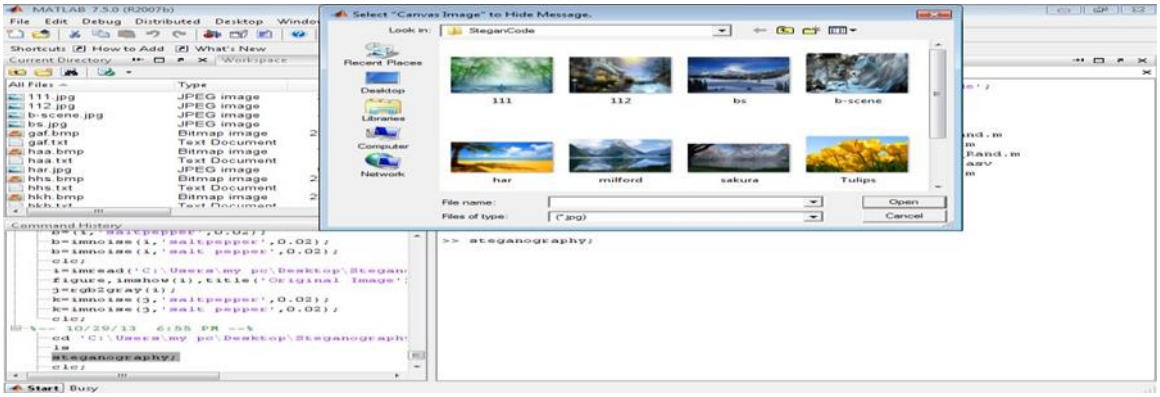

Figure 7: Selection of Canvas Image

Step 3: Selection of text message file: In this step, the file is selected in which our message is written.

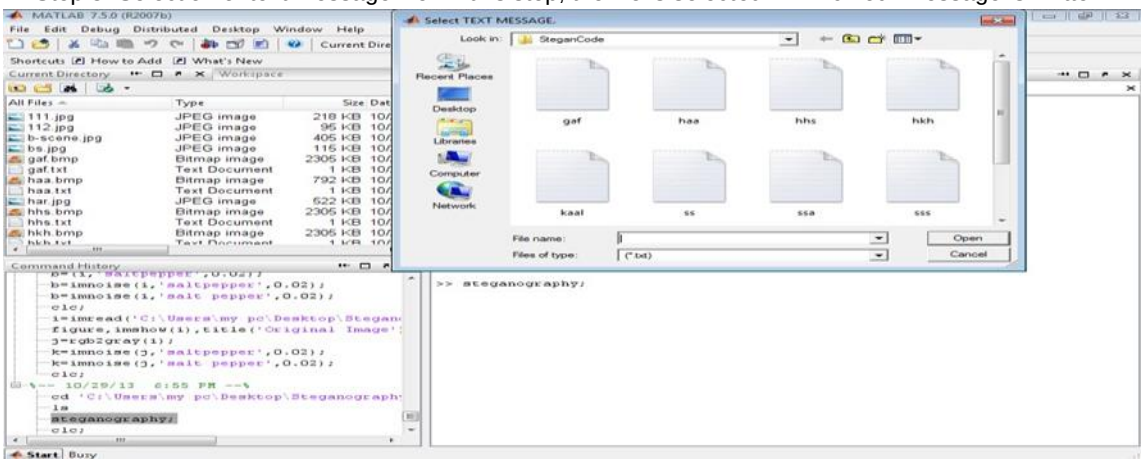

Figure 8: Selection of text message file

Step 4: Enter encryption Key: In this step, an encryption key value is selected which lies between 0 to 255.

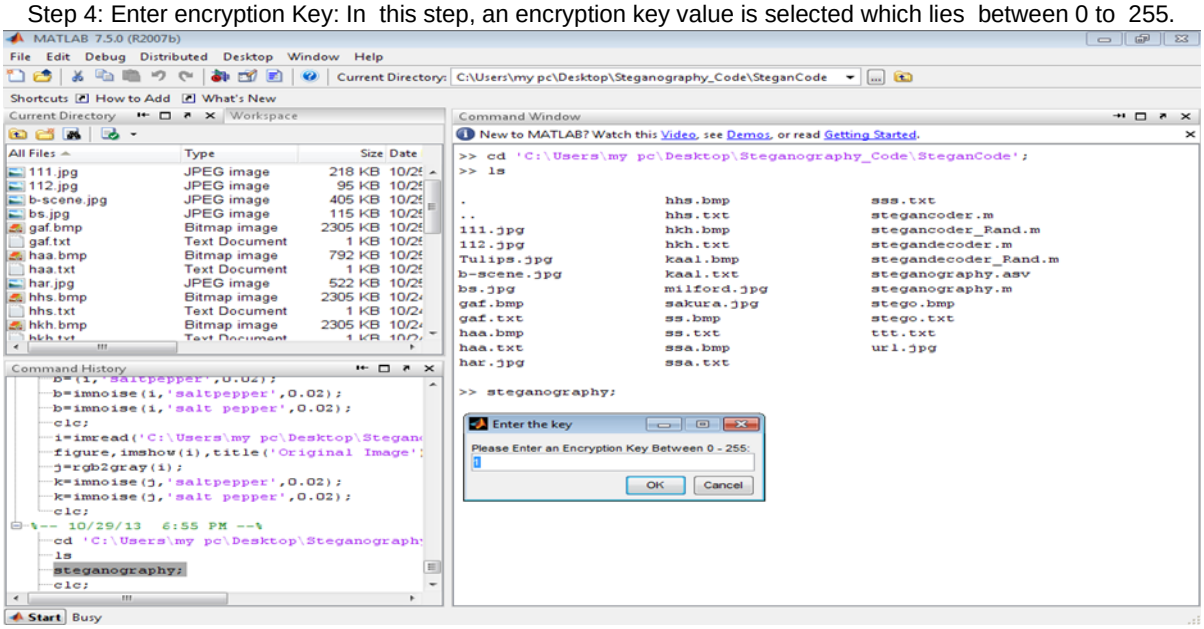

Figure 9: Enter Encryption Key

Step 5: Retrieval of Message: This step is performed at receiver side where the receiver enters the file name which contains an image having message.

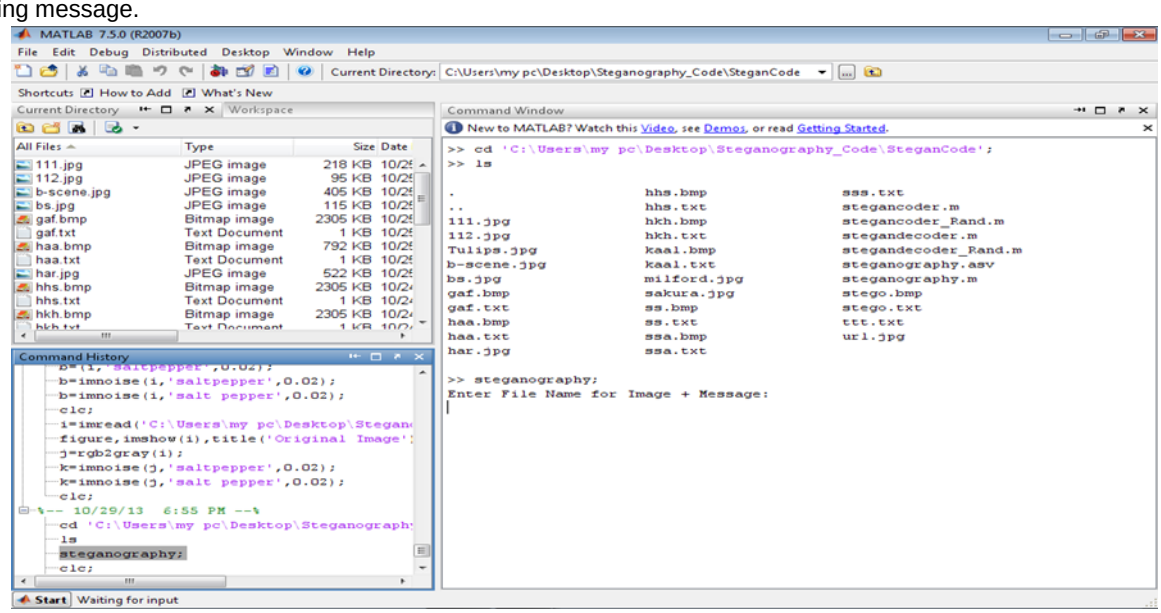

Figure 10: Retrieval of Message

Step 6: Enter Decryption Key: In this step, the receiver mentions the decryption key to decrypt the message. If the key matches with the encryption key then the message will be retrieved.

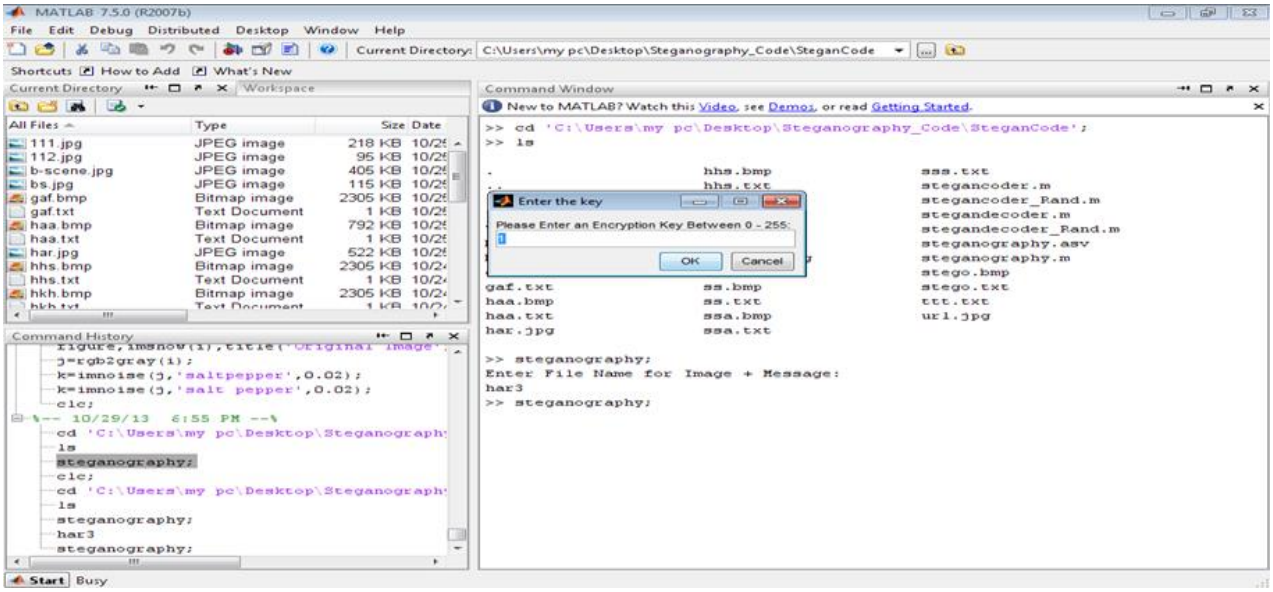

Figure 11: Enter Decryption Key

Step 7: Hidden Message is retrieved: At last, when key matches the secret message will be retrieved.

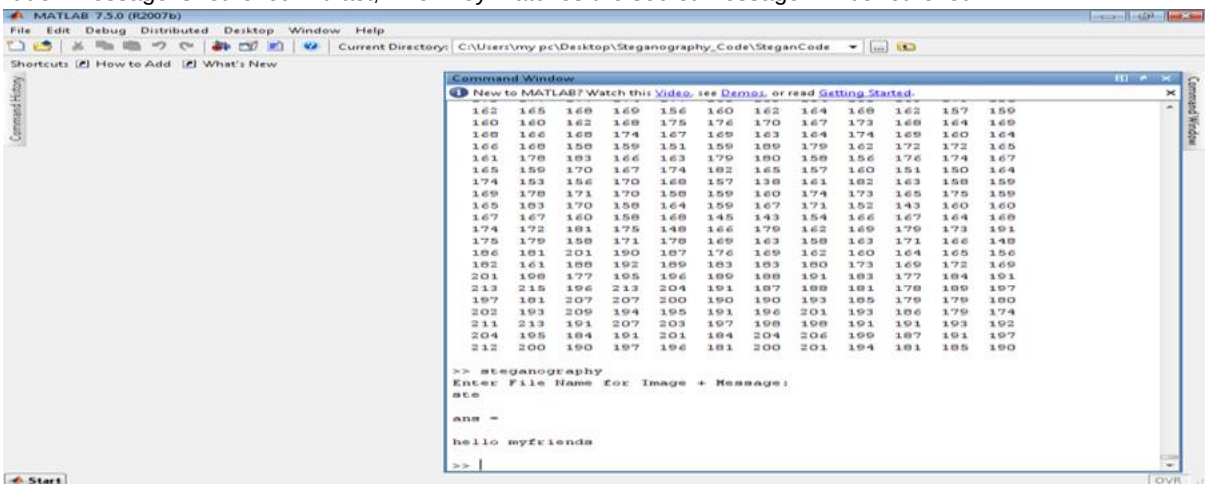

Figure 12: Hidden Message is retrieved

The result shows that the message was successfully recovered without data loss. The result is a success due to the integration of Image Steganography with an encryption key that enhances system security.

Table 1: Results comparison

Types of Techniques	PSNR	MSE
Image Steganography System	60.21 db	0.322
Proposed System	62.56 db	0.119

The above table revealed that if only image steganography is applied then its PSNR (Peak Signal to Noise Ration) is less as compared with the proposed system but for good result it should be higher.

However, the PSNR value of proposed system is higher with 62.56 db whereas MSE (Mean Square Error) should be less for better results. Hence, the proposed system has less MSE.

4. Conclusion:

"A basic idea of the proposed system is to provide additional security for the data that will be hidden within the image. The system is being tested in 30 images and the results show that the proposed system is able to provide data protection. The program works on colored images and gives 100% results. The PSNR (Peak Signal to Noise Ration) value for stego image is 62.56 db and the MSE (Mean Square Error) is 0.119." The encryption key is a key feature in this program, if someone forgets the secret encryption key, then the system does not work.

References

1. Diwedi Samidha & Dipesh Agrawal, “Random Image Steganography in Spatial Domain”, IEEE International Conference in Emerging Trends, VLSI, Embedded System, Nano Electronics and Telecommunication System, pp1-3, 2013.
2. K.A. Darabkh, I.F. Jafar, R.T. Al-Zubi, & M. Hawa, “An improved image least significant bit replacement method”, IEEE 37Th International Convention in Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp 1182-1186, 2014.
3. Lalit Kumar Vashishtha Tanima Dutta Arijit Sur, “Least significant bit matching steganalysis based on feature analysis”, IEEE National Conference in Communications (NCC), pp. 1-5, 2013.
4. G.Prabakaran & R.Bhavani, "A modified secure digital image steganography based on Discrete Wavelet Transform", IEEE International Conference In Computing, Electronics and Electrical Technologies (ICCEET), pp. 1096-1100, 2012.
5. D.R. Denslin Brabin, Dr.V.Sadasivam, “QET Based Steganography Technique for JPEG Images”, IEEE International Conference on Control, Automation, Communication and Energy Conservation, ISBN 978-1-4244-4789-3, 2009.
6. Discrete Fourier Transform (DFT). Available at: http://in.mathworks.com/help/matlab/math/discrete-fourier-transform-dft.html.
7. Monica Adriana Dagadita, Emil-Ioan Slusanschi, & Razvan Dobre, "Data Hiding Using Steganography ", IEEE 12th International Symposium in Parallel and Distributed Computing, pp. 159-166, 2013.
8. Dr. M.Chapman, G. Davida, and M. Rennhard, “A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography”, Proceedings of the Information Security Conference, October 2001, pp. 156-165.
9. Mohamed Amin, Muhalim and Ibrahim, Subariah and Salleh, Mazleena and Katmin, Mohd Rozi (2003) Information hiding using steganography. Project Report. Available at: http://eprints.utm.my/4339/1/71847.pdf.
10. Direct-sequence spread spectrum (DSSS), Frequency-hopping spread spectrum (FHSS) Wikipedia, the free encyclopedia, GNU Free Documentation License http://en.wikipedia.org/wiki/Direct- sequence_spread_spectrum.
11. Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal, "Steganography and Steganalysis: Different Approaches", International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1, June, 2008, Serial Publications.
12. J. Fridrich and M. Goljan, “Stegnalysis of LSB Embedding in color and Grayscale image”, in preparation for the special issue on security in Magazine IEEE Multimedia.
13. R. J. Anderson and Petitcolas, F.A.P., “On the limits of steganography”, IEEE Journal of selected Areas in Communications.
14. Curran, K. and Bailey, K. “An evaluation of image based steganography method”.International Journal of Digital Evidence, Fall2003.
15. Jakson, J.T.,Gregg, H., Gunsch, Claypoole, R.L., and Lamont, G.B. “Blind Steganography detection using a computational immune system: A Work in progress”. International Journal of DigitalEvidence.
16. Digital Image Processing using MATLAB by Gonzale Woods.
17. N. Provos and P. Honeyman,”Hide and seek: An introduction to Steganography”.
18. N.F.Johnson &Sushil Jajodia,”Exploring Steganography: Seeing the Unseen”,Survey PaperIEEE-1998.
19. K.B.Raja, C.R.Chowdary,”A Secure Image Steganography using LSB,DCT and compression Techniques on Raw Images”, IEEE -2005.
20. Mamta Juneja & Parvinder Singh Sandhu,”Designing of Roboust Image Steganography Technique Based on LSB Insertion and Encryption”, 2009 ICARTCC
21. Piyush Marwaha & Paresh Marwaha,”Visual Cryptographic Steganography in Images”, 2010 Second international conference on computing, communication and networking technologies.
22. Amitava Nag, Sushanta Biswas,”A Novel Techniques for image steganography based on DWT and Huffman Encoading”, IJCSS, Vol(4): Issue (6)
23. Hniels Provos & Peter Honeyman,”Hide & Seek : An Introduction to Steganography” IEEE Computer Society Pub-2003.
24. Feng Pan, & Jun Li,”Image Steganography Method Based on PVD and Modules Function”,IEEE- 2011.
25. Pfitzmann & Wesrfeld.A,”High Capacity Despite Better Steganalysis,” Kluwer Academic Publisher Boston Dodrecht London,2000.
26. Ming Chen,Z.Ru.N.Xin, “Analysis of Current Steganography Tools: Classification & Features”, Information Security & Tele.Comm. Beijing Dec-2006.
27. Hassan mathkour,Batool Ai,sadoon, “A New Image Steganography Technology” ,IEEE-2008
28. Ge Huayong ,Huang ,”Steganography and Steganalysis Based on Digital Image”, International conference & signal Processing-2011 IEEE.
29. Saeed Sarreshtedari & Shahrokh ,”High Capacity Image Steganography in Wavelet Domain”, IEEE CCNC 2010 Proceedings.
30. S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.
31. Sridevi R., Damodaram A., SVL.Narasimham, Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security, Journal of Theoretical and Applied Information Technology, 2009.
32. G. J. Simmons, "The prisoners' problem and the subliminal channel" in Proc. Advances in Cryptology (CRYPTO '83), pp. 51-67.Berglund, J.F. and K.H. Hofmann, 1967. Compact semitopological semigroups and weakly almost periodic functions. Lecture Notes in Mathematics, No. 42, Springer-Verlag, Berlin-New York.
33. Masoud Nosrati, Ronak Karimi, Mehdi Hariri, An introduction to steganography methods, World Applied Programming, Vol (1), No (3), August 2011. 191-195.
34. Bender W, Gruhl D & Morimoto N (1996) Techniques for data hiding. IBM Systems Journal 35(3): p 313–336.
35. Nedeljko Cvej, Algorithms for audio watermarking and steganography, Oulu 2004, ISBN: 9514273842.
36. Sos S. Agaian, David Akopian, Sunil A. D’SOUZA1, Two algorithms in digital audio steganography using quantized frequency domain embedding and reversible integer transforms, USA.
37. “audio steg: methods”,Internet publication on www.snotmonkey.com http://www.snotmonkey.com/work/school/405/methods.html.
38. Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, “A Tutorial Review on Steganography”.
39. Beixing Deng, Jie Tan, Bo Yang, Xing Li, A Novel Steganography Method Based on Modifying Quantized Spectrum Values of MPEG/Audio Layer III, Proceedings of the 7th WSEAS International Conference on Applied Informatics and Communications, Athens, Greece, August 24-26, 2007.

40. Alaa Ismat Al-Attili, Osamah Abdulgader Al-Rababah, New technique for hiding data in audio file, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.7, July 2010.
41. H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, Information Hiding in Audio Signals, International Journal of Computer Applications (0975 – 8887) Volume 7– No.9, October 2010.
42. Clair, B.; "Steganography: How to Send a Secret Message", 8 October 2001, http://strange horizons.com/2001/20011008/steganography.shtml .
43. Al-Khateeb, H.; "Introduction to Modern Steganography", 11 Jan, 2010, http://blog.creativeitp.com/posts-and-articles/cryptography/introduction-to-modern-steganography.

