Use a multi-level system for Steganography

Hazim Salman Majeed[1], Yasir Ali Matnee[2], Ali Ahmed yaseen[3]

[1] College of Education for Human Science, University of Diyala, IRAQ

[2]Department of Computer Science, Basic Education College, University of Diyala, IRAQ

[3]College of Education for Human Science, University of Diyala, IRAQ

DOI: https://doi.org/10.5281/zenodo.8185901

Published Date: 26-July-2023

Abstract: **During the last decades, the revolution of modern technology starts with rapid change, so the world becomes a tiny village through the development of communication means especially electronic information by using some ways to keep secret data also it is to be noted that encryption is a vital case in this area of our universe. However there is a fatal phenomenon represented by hackers in which by any way try to obtain the information and alters its texts In this case, the complex system in modern technology is insisting need to cope with saving information. So the use of coverage system is a prominent step to send unseen information by hiding it inside the sent media, for example, image, video and audio. The research focuses on the idea of saving the information or hiding the layers to prevent the hackers to steal the data.**

Keywords: **modern technology, electronic information, Steganography.**

1. INTRODUCTION

Data can contain a form of knowledge such as images, sounds, e-mail, and text. Internet information contains free addresses. These arguments work by using a specific codec: marking encryption.[1] if someone thinks of a mysterious introduction, they can be considered to have succeeded in applying a simple form of data masking. Some people should reveal a hidden message "Birds fly midnight" If they discover that the paragraph contains a hidden message before someone tells them it exists, the researcher failed to hide the data.[2] The chances of a researcher's success are fairly large though most persons do not think there is more than one way to analyze something in a newspaper. The process of sending and receiving data by Internet users frequently requires storing this data. The best way to do this is to change the data to another different format. The output from this process can only be absorbed by people who know how to restore it to its original form.[3] The model to security data is known as encryption. The presence of non-hidden data is one of the most important drawbacks of encryption. The encrypted data is not readable, but it is present as data. It is possible to decode by a person if given enough time. The best solution to this deficit is to steganography.[4]

Historical review of steganography

Hide data in a manner to store data in a way that hides this data. In addition to the current methods of communication, it can be used to hide information to make subtle exchanges. Institutions are concerned with two types of hidden communications: Including supporting national security, which does not support.[5] Hiding digital information is enormous potential for both types. Companies may have an obsession Concerning business secrets or information about a modern product. Staying away from contacts in their known forms avoids leakage of information during transmission. Companies are increasingly gaining another advantage of data masking, known as watermarking. One of the most important uses of the watermark is to identify and include a distinct piece of data in a medium without a significant change in the medium. Example When designing a digital image, the image designer can be embedded as a watermark that you specify as the image designer.[6] The researcher can achieve this by processing image data using data hide, The result contains data that represents the name without significantly altering the image. So that others who receive the digital image cannot determine which information is hidden inside it. If the image is used without permission, the owner of the image can prove to be his property by extracting the watermark. The importance of the watermark is to protect copyrighted media such as a web page. Hiding data can also support privacy. The watermark is not a substitute for encryption, The data steganography provides a special way of communicating. When communicating by someone who does not want to be exposed to work control systems, steganography is the perfect solution for more private communication.[7]

Relation between steganography and cryptography

The purpose of concealing data is to prevent others from thinking about the existence of the information, not to prevent them from knowing the hidden information.[9] If the method of concealing information causes someone to think of the intermediary of the carrier, the method fails. Thus the success of concealing information depends on the naivety of humans.

Example The last time you checked your email for hidden messages, encryption and concealment of information achieved separate goals. Data encryption is based on not allowing the unintended recipient to define its intended meaning. Data masking makes the information unusable for the accidental recipient. Employees try to hide data to prevent the accidental recipient from suspecting the existence of data. Who is seeking for the best in communication combining encryption and data masking. Those looking for the best in communications combine data masking and encryption. Those looking for the best in communications combine steganography and encryption. Many stenograph tools encrypt data before hiding it in the selected medium.[10]

Limitations:

Restricts the concealment of information by the same assumption as encryption. If you want to send a hidden image to someone, you must first agree with the person on how to hide the data.[11] In encryption systems, it is necessary to obtain encrypted text. At the same time in cryptographic models, it is difficult to know when an image is deprived of information. illustrate this we assume someone has a digital camera and you must tell him to care for every 73 bytes in the image sent.[12] The more restrictions placed on the broker, the greater the ability to hide data. For example, this paragraph is restricted by the rules of the English language and a particular subject of debate.

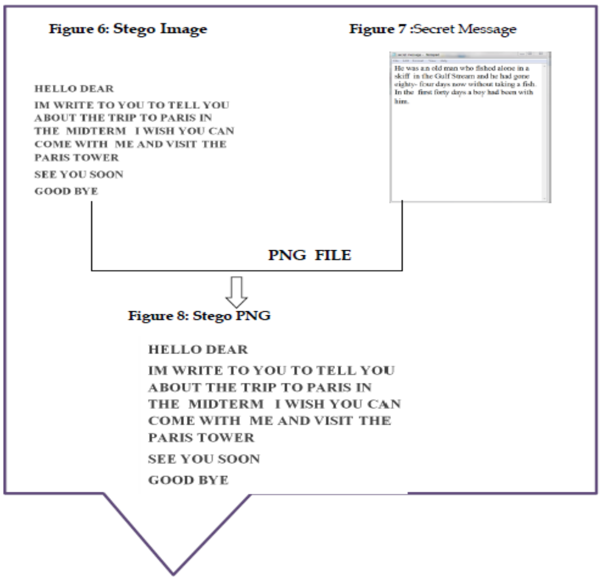
Because of the limited number of ways in which a text can reasonably be changed, it is difficult to hide a secret message in this paragraph. In contrast, the big picture illustrates both static and uncompressed More data can undoubtedly be included in this picture regardless of the fact the picture of the TV is fixed and questionable. Using the following method you can successfully hide a message.[13]

■ Excluding the black border, start at the pixel in the upper left corner of the image.

■ Set the color value of the current pixel to the ASCII value of the corresponding character in the message you want to hide.

■ Move two pixels to the right. If you are at the edge of the image, wrap around and skip a line.

■ Repeat the previous two steps until the entire message is coded.



HELLO DEAR
IM WRITE TO YOU TO TELL YOU
ABOUT THE TRIP TO PARIS IN
THE MIDTERM I WISH YOU CAN
COME WITH ME AND VISIT THE
PARIS TOWER
SEE YOU SOON
GOOD BYE

He was an old man who fished alone in a skiff in the Gulf Stream and he had gone eighty- four days now without taking a fish. In the first forty days a boy had been with him.

HELLO DEAR
IM WRITE TO YOU TO TELL YOU
ABOUT THE TRIP TO PARIS IN
THE MIDTERM I WISH YOU CAN
COME WITH ME AND VISIT THE
PARIS TOWER
SEE YOU SOON
GOOD BYE

Figure 1: shows data encryption to hide text in a image

Steganography methods

There are many applications available to hide data. Exploit technique restrictions are the most common method of formatting files. Many of the available applications use this technology on many media.[10]

Images as carriers

Images can be considered a good environment to hide data. If the image contains too much detail, there will be few restrictions on data that can be hidden before it becomes questionable. The JPHide/JPSeek pack employ the coefficients in a JPEG to hide data. The newer method involves the important parts of the data in the image visually.[14] Both of these manners vary the image The next manner to alter the image.

Therefore, it is possible to observe the dissolution of the image using different messages and images of different lengths. In exchange for, specified to GIF images, is to processing an image's palette in order to hide data. Gif Shuffle Her work is not to change the image in a visual way Actually.[15]

Audio file carriers

There are many applications to hide data in audio files. It MP3Stego effectively hides data and is a powerful tool for encoding audio file data. The Windows Wave initialize allows users conceal information using StegoWavor. Data Hide Stage alteration the Smaller section of the important information in the transmitter. Though the information is always equal, however the great size of significative audio files make them minimal diffuse than image files.[11]

Ordering of data

The order of the data does not work on the order of constraints but rather on the effective method of concealing the data. Each switch can be set to a positive number. This command can be used to encrypt hidden data by changing the order of objects that cannot be considered arranged by the carrier. These techniques do not change the quality of information mainly and if data is encoded again, data loss is likely.[16]

Image Steganography, Selection of Cover Image

To steganography, the confidential message in the cover photo, choose the appropriate cover photo. It is necessary to hide data in an image using a lossless compression algorithm because there is a chance of losing data at the time of the connection.[17]

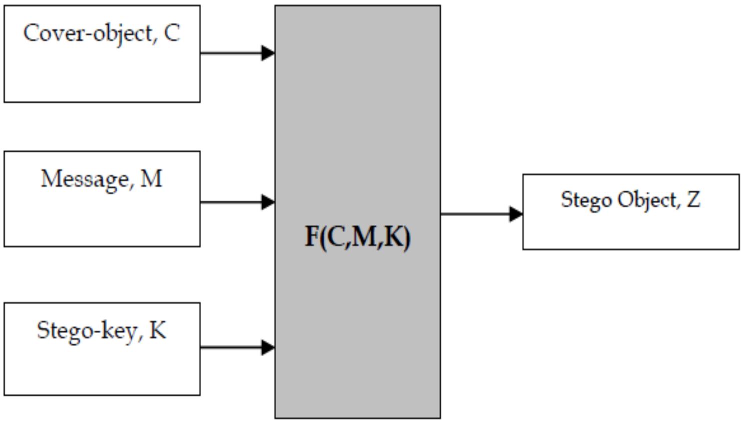
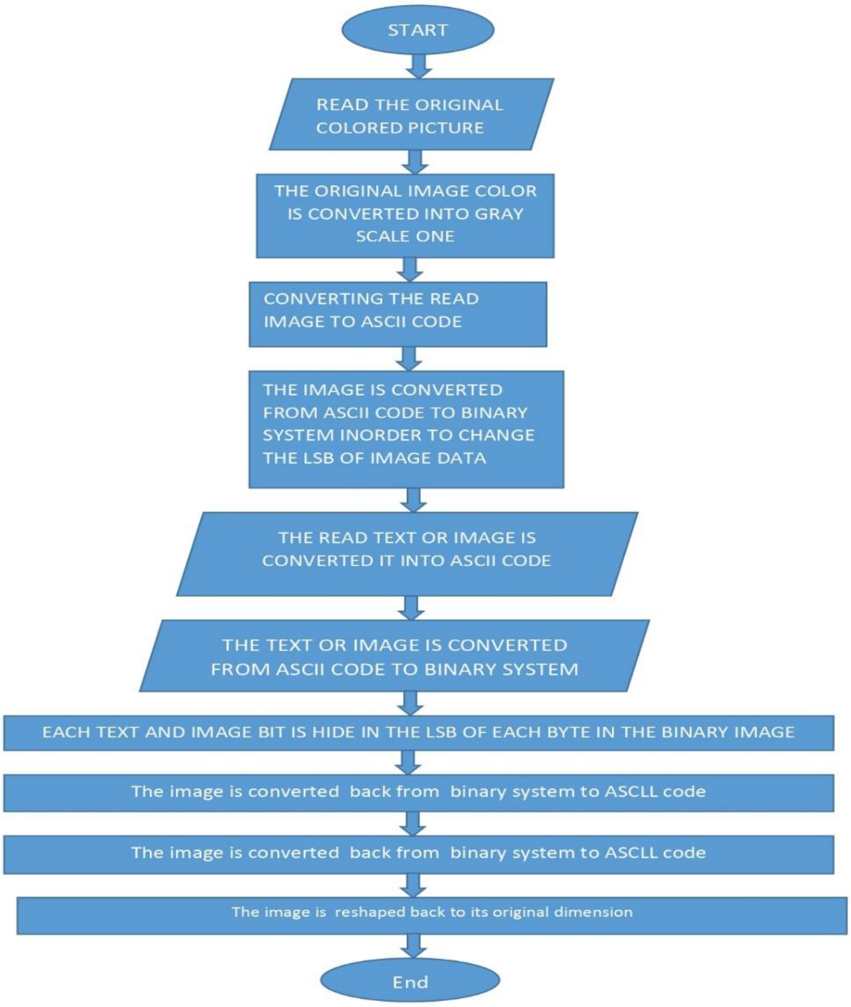


Figure 2: shows how to hide data in an image using the loss algorithm

Data hiding image based on LSB

LSB is a technique based on a simple way in which message its are merged into the least important bits in the cover image. In this technique the most important data in the image is used to hide confidential information.[18]

2. METHODOLOGY


START
READ THE ORIGINAL COLORED PICTURE
THE ORIGINAL IMAGE COLOR IS CONVERTED INTO GRAY SCALE ONE
CONVERTING THE READ IMAGE TO ASCII CODE
THE IMAGE IS CONVERTED FROM ASCII CODE TO BINARY SYSTEM INORDER TO CHANGE THE LSB OF IMAGE DATA
THE READ TEXT OR IMAGE IS CONVERTED IT INTO ASCII CODE
THE TEXT OR IMAGE IS CONVERTED FROM ASCII CODE TO BINARY SYSTEM
EACH TEXT AND IMAGE BIT IS HIDE IN THE LSB OF EACH BYTE IN THE BINARY IMAGE
The image is converted back from binary system to ASCLL code
The image is converted back from binary system to ASCLL code
The image is reshaped back to its original dimension
End

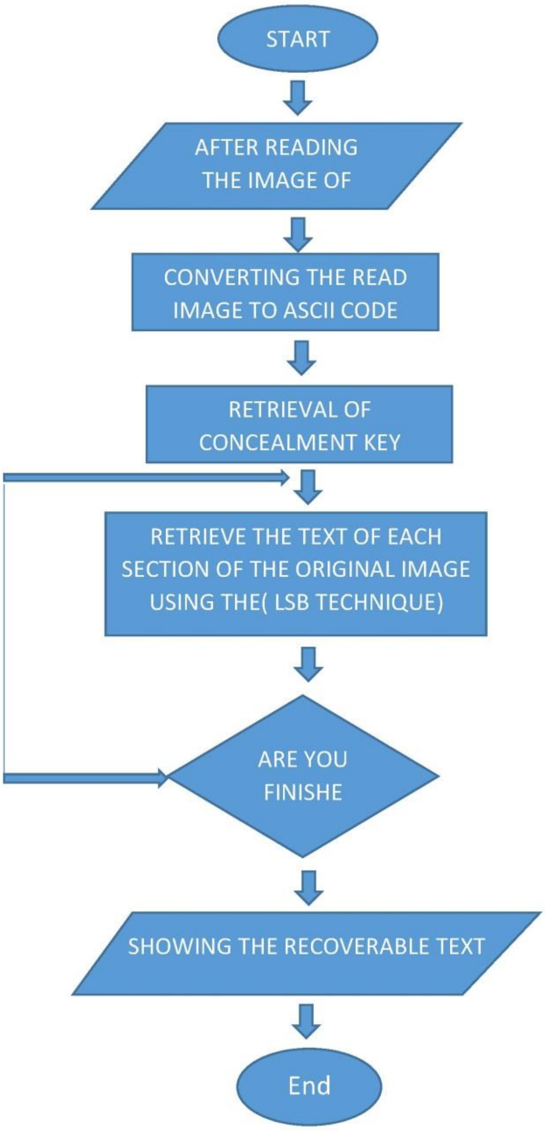
Flow chart 3: shows for the process includes the process for hiding text and image within a cover image

To create a project to hide a text in an image and hide it in a cover image algorithm.

The LSB algorithm is performed by hide the data exporter (text and image) in a gray cover image using an application visual c# program R2013. First, the grey scale image data which is 256 x 256 pixels is reading and Transformation into its identical ASCII code 256 X 256 data matrix. The data matrix is Transformation from ASCII code to binary system a 65536 x 7 binary data matrix is component where the number of rows equal to 256 x 256 = 65536 and number of columns is 7 in order to change the LSB of each byte of the cover image.

Each text letter is Transformation to ASCII code form and then to the binary system to hide each bit of the plain text into the LSB of each byte of the grey scale cover image.

Image data is read in grayscale 256 x 256 pixels and Transformation into its identical ASCII code 256 X 256 data matrix. The data matrix is Transformation from ASCII code to binary system a 65536 x 7 binary data matrix is construct where the number of rows equal to 256 x 256 = 65536 and number of columns is 7 in order to change the LSB of each byte of the secret image. reformation the image again from65536*7 the binary matrix to the original data ASCLL code. The image is designed before and after concealing the textual information in it.


START
AFTER READING THE IMAGE OF
CONVERTING THE READ IMAGE TO ASCII CODE
RETRIEVAL OF CONCEALMENT KEY
RETRIEVE THE TEXT OF EACH SECTION OF THE ORIGINAL IMAGE USING THE(LSB TECHNIQUE)
ARE YOU FINISHE
SHOWING THE RECOVERABLE TEXT
End

Flowchart illustrating the Text and image Hiding process in Gray scale image:- Flowchart for the process includes the process for hiding text and image within a cover image:

Steps to hide text or image in Ordinary Gray Scale cover Image using LSB

Step one: The color image is processed and converted to gray and then find the dimensions of the matrix where it helps to retrieve the image to its original form after storing the text inside. The image is processed and converted into a code matrix

Step Two: The image is then converted to a binary system where the eighth bit can be changed LSB. When converting the matrix into binary system each number transforming into an 8-bit Turns entire row and turned the 4 * 4 to16 * 8 matrix where each number filled the entire row No. 161, for example, the store in the first row column fill here on the front row and Transforming into the whole system the first Binary format 101000011

Step Three: Get in the text or image be hide it and convert it to ASCII Code and of which the binary system and find the number of rows and number of columns, Where bytes of each character can be moved to the LSB bit in the image where all bytes of characters will be stored, eighth left to a given site in the picture. The text to be hidden into the gray scale

Step Four: Every seven bits are hoard as a character in an arranged row of LSB represents the transition to determine the match in the second word It will last until another letter and then return to the second bit first and then the second word, Second-bit word continues. The greatly the size of the text difficult decryption code not know the objector what is inside the image and what bits of text.

Step Five: The hidden to text in image and presser her of binary system to ASCII system and convert to dimension matrix in elementary dimensions, the image has changed the first number in arrangement use

functioning8of information and return to from decimal number eight bit.

Step six: The picture drawing before and after the text department store.

Decryption phase for the text from the image

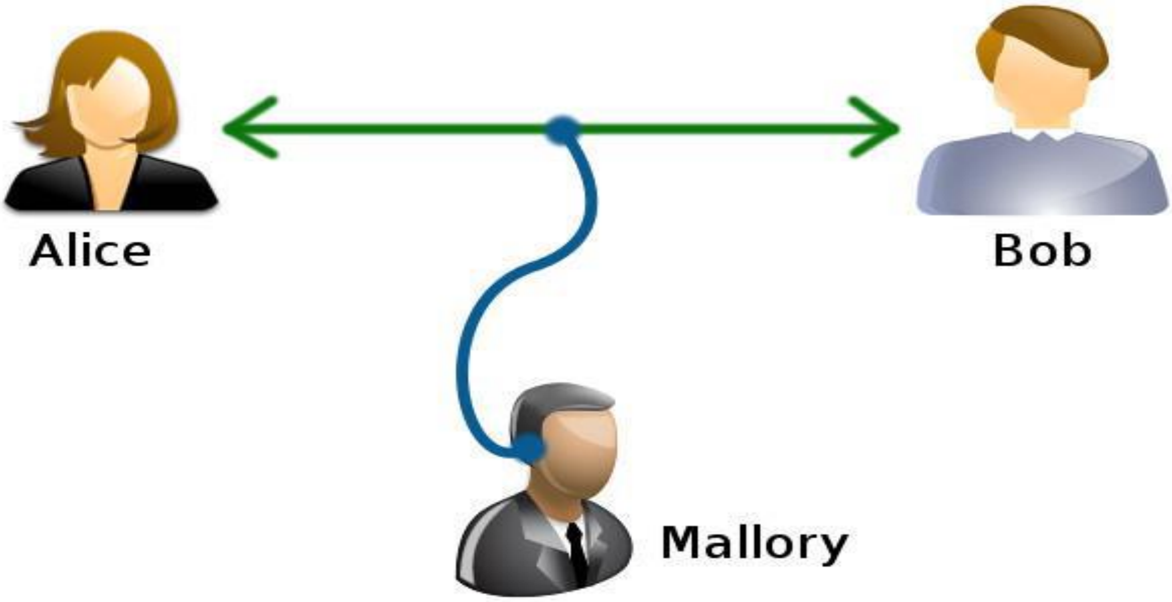


Figure 4: Shows hiding data effectively in a specific medium

The picture conversion to binary system. Step one:

Step two: the order 8 bit each row and storage in matrix whoever to resound send dispatch encryption message the number of rows and number of columns cypher text is where to start encryption within the image until it is takes it out.

Step Three: head for replace the matrix text to form elementary binary system format and transformation of the binary system to the decimal system.

Step Four: The information to convert to decimal system to letters.

Evaluation

During the conduct measurement for hiding of message, the well-known peak-signal-to noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stage images. It is defined as: PSNR = 10log(C max)2=*MSE:* MSE = mean - square - error; which is given as: MSE = 1/MN((S-C)2)*:* C max = 255:

Where M and N are the dimensions of the image, S is the resultant stego-image, and C is the cover image.

PSNR values below 30 dB indicate low quality (i.e., deformity occasion by embedding is high). A high-quality stego image should strive for a PSNR of 40 dB, or higher.

Namely as a diagram representation of the tone division in a digital image. It graphical number of pixels for each tonal value. During looking at the histogram for a qualitative image a view shall able to judge the entire tonal distribution at a glance. and here we use this technique to Performance Analysis in image steganography.

3. RESULT AND DISCUSSION

We showing gray scale/RGB image as covering image as

The Different between cover noisy image

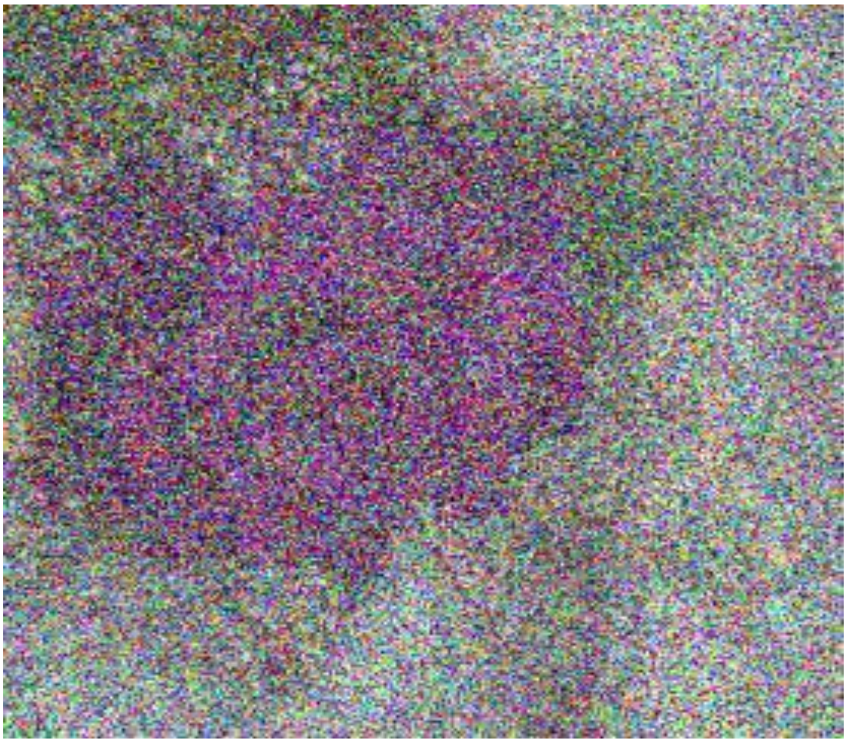


Figure 5: cover noisy

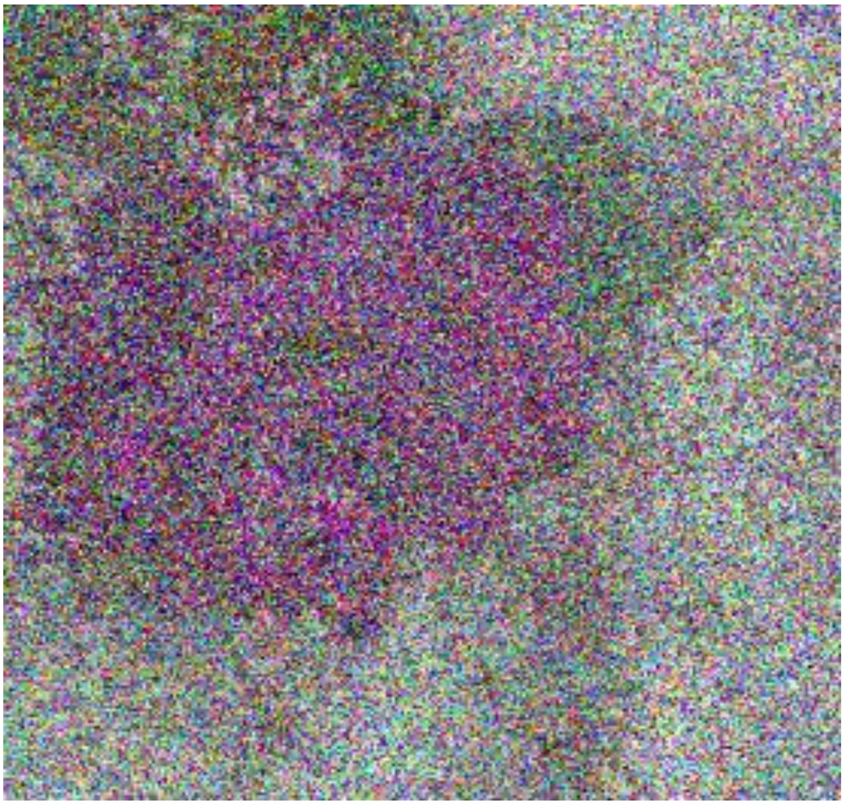
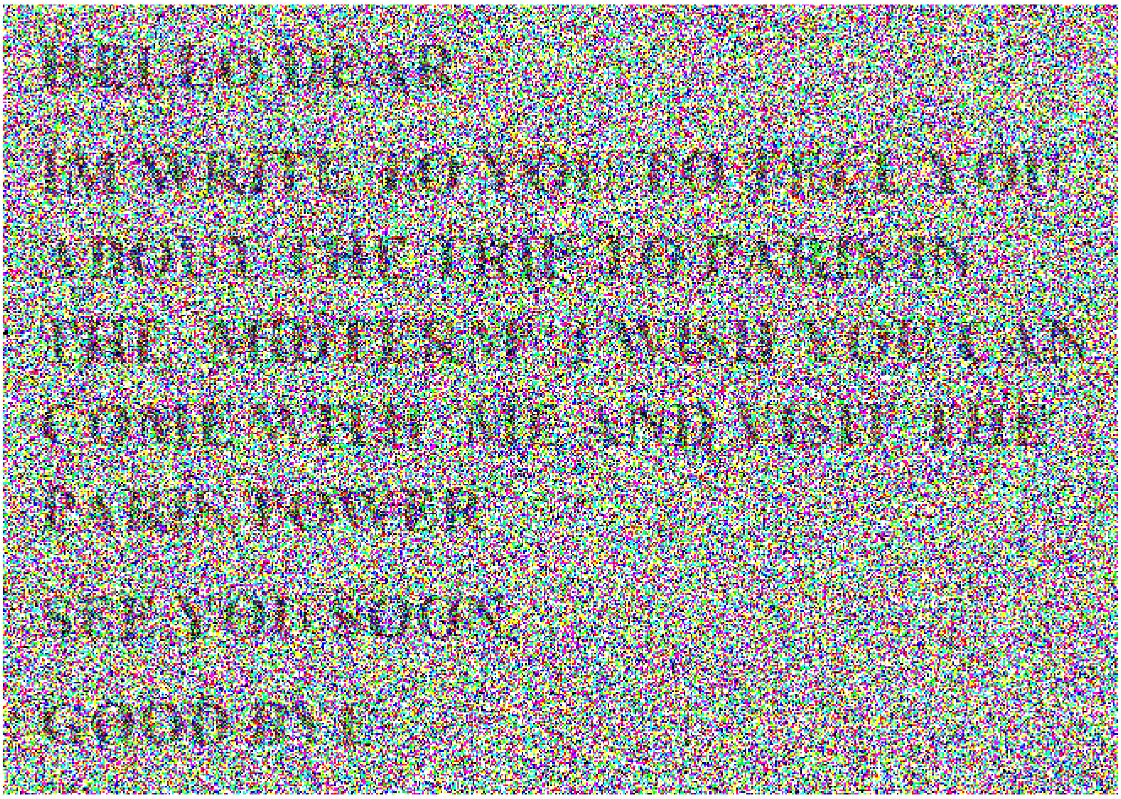


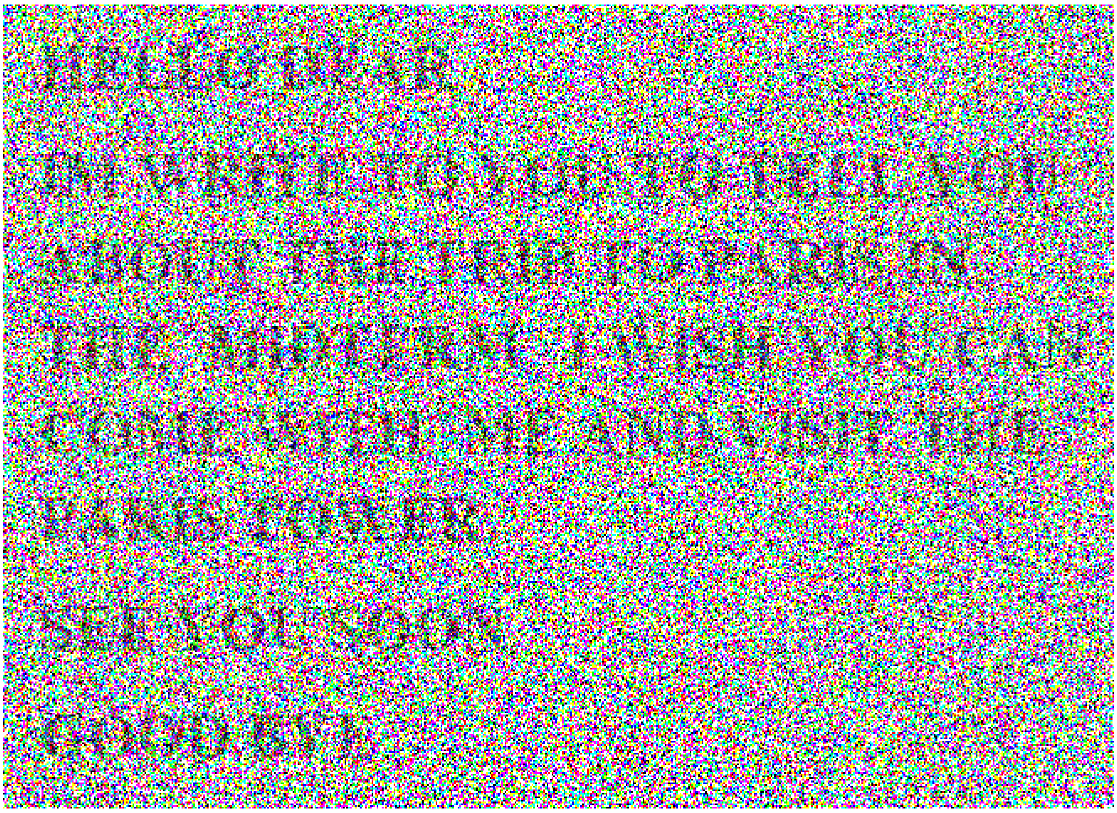
Figure 6: cover png noisy

The Different between stego noisy image



HELLO DEAR
IM WRITE TO YOU TO TELL YOU
ABOUT THE TRIP TO PARIS IN
THE HOLIDAYS. I WISH YOU CAN
COME WITH ME AND VISIT THE
PARIS TOWER
SEE YOU SOON
GOOD BYE

Figure 7: stego noisy



HELLO DEAR
IM WRITE TO YOU TO TELL YOU
ABOUT THE TRIP TO PARIS IN
THE HOLIDAYS. I WISH YOU CAN
COME WITH ME AND VISIT THE
PARIS TOWER
SEE YOU SOON
GOOD BYE

Figure 8: stego png noisy

The Different between cover image histogram

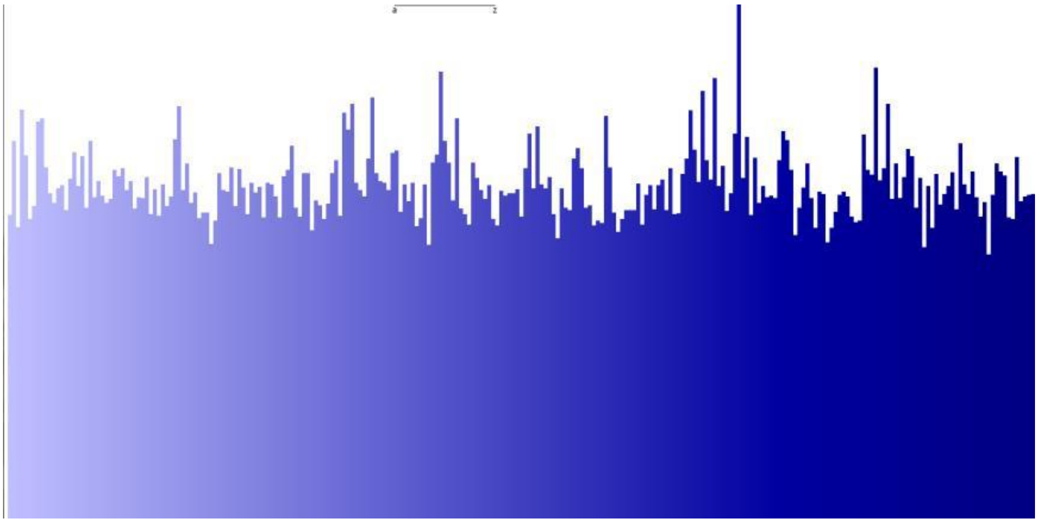


Figure 9: cover histogram

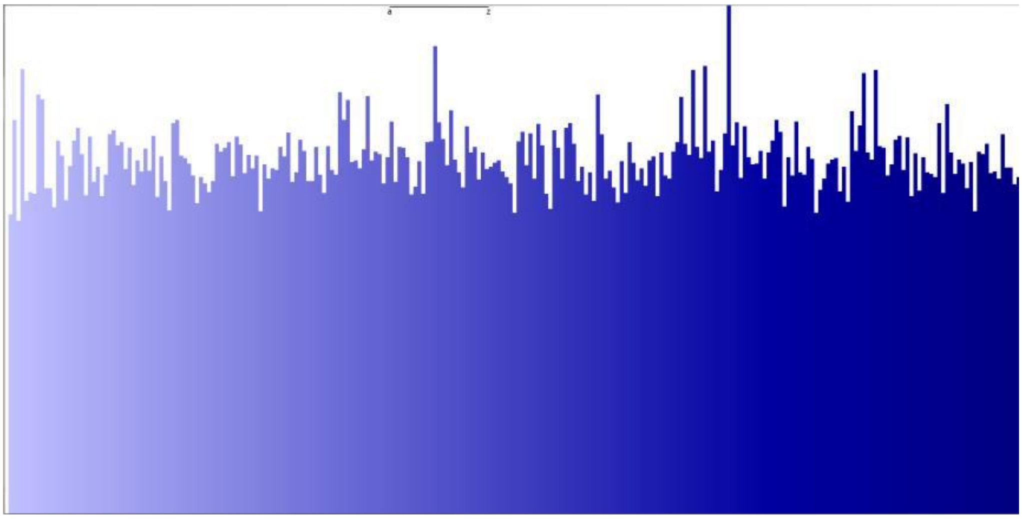


Figure 10: cover png histogram

The Different between stego image histogram

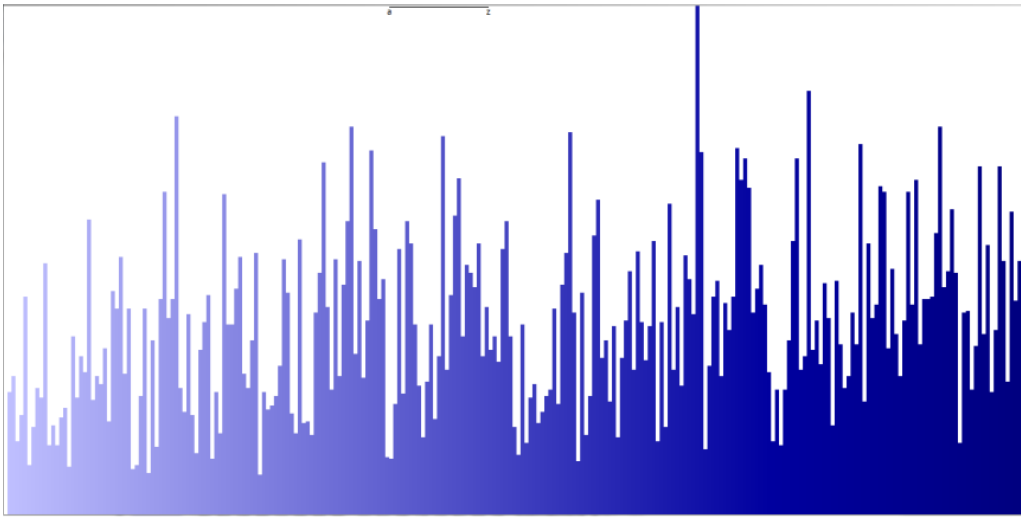


Figure 11: stego histogram

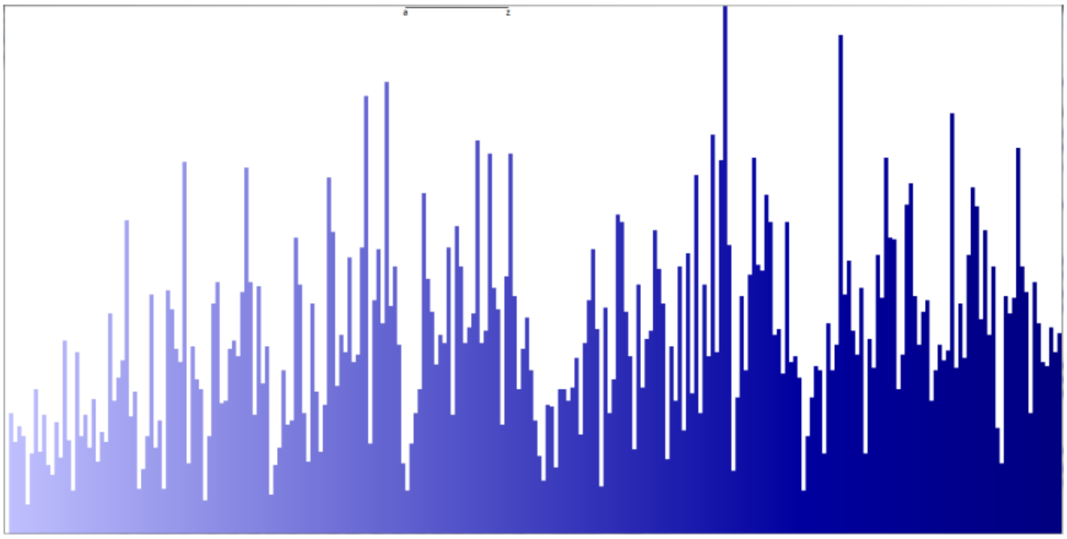


Figure 12: stego png histogram

4. CONCLUSION AND FUTURE WORK

Steganography is an active method to conceal data. In this project scholars employ the LSB technicality numerous layers on image to obtain secure stego- image. Table 4.1 shows that PSNR. The outcome coition than the LSB insert use many hide layers is best than simple LSB insertion in case of lossless compression. The image solution doesn't alteration much and is negligible when comprise the message into the image, the image insert image. and the image is protectorate with private key. So, it is not possible to detriment the data by ulna This research project focuses on the approach like increasing the security of the message and increasing PSNR and reducing the distortion rate . authorized personnel . The algorithm is use for both 8 bit and 24 bit image of the somewhat size of cover and secret image, so it is facilitate to performance in both grayscale and color image.

This research project focus on the approach liking increment the security of the message and increasing PSNR and decreasing the deformity rate. The focus of the search is to apply multilayer masking to text that is hidden in an image cover. The research examines the potential of an elementary estimate of concealment of multilayered steganography images to improvement the sensitivity of short message detection.

REFERENCES

[1] Lin, E.T. and E.J. Delp. A review of data hiding in digital images. in PICS. 1999.

[2] Ibrahim, R. and T.S. Kuan, Steganography algorithm to hide secret message inside an image. arXiv preprint arXiv:1112.2809, 2011.

[3] Bhattacharyya, S., A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier. International Journal of Global Research in Computer Science (UGC Approved Journal), 2011. **2**(4).

[4] Lin, C.-C. and W.-H. Tsai, Secret image sharing with steganography and authentication. Journal of Systems and software, 2004. **73**(3): p. 405-414.

[5] Artz, D., Digital steganography: hiding data within data. IEEE Internet computing, 2001. **5**(3): p. 75-80.

[6] Fridrich, J., M. Goljan, and R. Du, Detecting LSB steganography in color, and gray-scale images. IEEE multimedia, 2001. **8**(4): p. 22-28.

[7] Thangadurai, K. and G.S. Devi. An analysis of LSB based image steganography techniques. in Computer Communication and Informatics (ICCCI), 2014 International Conference on. 2014. IEEE.

[8] Devi, K.J., A secure image steganography using lsb technique and pseudo random encoding technique. no. May, 2013.

[9] Li, B., et al., A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing, 2011. **2**(2): p. 142-172.

[10] Gupta, S., A. Goyal, and B. Bhushan, Information hiding using least significant bit steganography and cryptography. International Journal of Modern Education and Computer Science, 2012. **4**(6): p. 27.

[11] S. Katzenbeisser and F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston, 2000.

[12] B. Barán, S. Gómez, and V. Bogarín, "Steganographic Watermarking for Documents," Proc. 34th Ann. Hawaii Int'l Conf. System Sciences, IEEE CS Press, Los Alamitos, Calif., 2001.

[13] H.K. Pan, Y.Y. Chen, and Y.C. Tseng, "A Secure Data Hiding Scheme for Two-Color Images," Proc. Fifth IEEE Symp. Computers and Comm., IEEE Press, Piscataway, N.J., 2000.

[14] N.F. Johnson and S. Jajodia, "Exploring Steganography:Seeing the Unseen," Computer, vol. 31, no. 2, Feb. 1998,pp. 26-34.

[15] Ravi Kumar, Kavita Choudhary, Nishant Dubey, **"**An Introduction of Image Steganographic Techniques and Comparison", International Journal of Electronics and Computer Science Engineering.

[16] Prashanti .G, Sandhya Rani.K, Deepthi.S " LSB and MSB Based Steganography for Embedding Modified DES Encrypted Text", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 8, August 2013, pp.788-799.

[17] Namita Tiwari, Dr.Madhu Shandilya,"Evaluation of Various LSB based Methods of Image Steganography on GIF File Format",International Journal of Computer Applications, Vol. 6– No.2, September 2010 , pp .1-4.

[18] Dr. Ekta Walia, Payal Jain, Navdeep, "An Analysis of LSB & DCT based Steganography, Global Journal of Computer Science and Technology", Vol.10, Issue 1, April 2010, pp.4-8.

[19] Mr. Rohit Garg, "Comparison Of Lsb & Msb Based Steganography In Gray-Scale Images Vol.1, Issue 8,Oct 2012".,International Journal of Engineering Research and Technology(IJERT).

[20] M. Chen, N. Memon, E.K. Wong, Data hiding in document images, in: H. Nemati (Ed.). Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.

[21] D.C. Lou, J.L. Liu, H.K. Tso, Evolution of information –hiding technology, in H. Nemati (Ed.), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.

[22] Schneider, Secrets & Lies, Indiana:Wiley Publishing, 2000.

[23] E. Cole, Hiding in Plain Sight: Steganography and the Art of Covert ommunication, Indianapolis: Wiley Publishing, 2003.

[24] T. Jahnke, J. Seitz, (2008). An introduction in digital watermarking applications, principles and problems, in: H. Nemati (Ed), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 554-569.

[25] M. Warkentin, M.B. Schmidt, E. Bekkering, Steganography and steganalysis, Premier reference Source–Intellectual Property Protection for Multimedia Information technology, Chapter XIX, 2008, pp. 374-380.

[26] Adelson, E., 1990. Digital signal encoding and decoding apparatus, US Patent no. 4,939,515, 1990.

[27] Bender, W., Gruhl, D., Morimoto, N., Lu, A., 1996. Techniques for data hiding. IBM Systems Journal 35 (3 & 4), 313–336.

[28] Blundo, C., De Santis, A., Naor, M., 2000. Visual cryptography for gray level images. Information Processing Letters 75, 255–259.

[29] Chang, C.C., Lee, H.C., 1993. A new generalized group-oriented cryptoscheme without trusted centers. IEEE Journal on Selected Areas in Communications 11 (5), 725–729.

[30] Hsu, C.T., Wu, J.L., 1999. Hidden digital watermarks in images. IEEE Transactions of Image Processing 8, 58–68.

[31] Kundur, D., Hatzinakos, D., 1999. Digital watermarking for telltale tamper proofing and authentication. Proceedings of the IEEE 87, 1167–1180.

[32] Lin, E.T., Delp, E.J., 1999. A review of fragile image watermarks. Multimedia and Security Workshop in ACM Multimedia ’99, Orlando, FL, USA, 1999.

[33] J. Fridrich, M. Goljan and R. Du, “Distortion-free Data Embedding”, to appear in Lecture Notes in Computer Science, vol.2137, Springer-Verlag, Berlin, 2001.

[34] R.J. Andersen and Petitcolas, F.A.P., "On the limits of steganography," IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and Privacy Protection **16** No.4 (1998) 474-481.

[35] T. Aura, “Practical invisibility in digital communication,” Lecture Notes in Computer Science, vol.1174, Springer-Verlag, 1996, pp. 265-278.

[36] J. Fridrich, M. Goljan, and R. Du, "Steganalysis based on JPEG compatibility," SPIE Multimedia Systems and Applications IV, Denver, CO, August 20-24, 2001.