Image Steganalysis of Improvised Algorithms Based on Pixel Difference Pattern and Random Embedding

Prashant Rawat[1], Bhupesh Kumar Dewangan[2], Anurag Jain[3], Nitin Arora[4]

[1] *Systematics Department, School of Computer Science, University of Petroleum & Energy Studies, Dehradun, India*
[2] *Informatics Department, School of Computer Science, University of Petroleum & Energy Studies, Dehradun, India*
[3] *Virtualization Department, School of Computer Science, University of Petroleum & Energy Studies, Dehradun, India*
[4] *Informatics Department, School of Computer Science, University of Petroleum & Energy Studies, Dehradun, India*

Abstract

In Today's Modern World, We all know that Communication is the necessity of everyone's life. However, the important thing is that, Are all Data Communications are secure. Because, we all know that the security of Data is very important in this evolutionary world because of some illicit hackers. That is why not only Communication but Covert Communication is also major necessity of life. It will help to make sure that the Data Communications are securely processed. Therefore, Covert Communication can hide the secret data with steganography. We will introduce fuzzy edge identification technique to use the Adaptive Steganography method. In this project, we are using fuzzy logics because this technique is very efficient for determining the edge areas after concealing the secret data. We are concealing our Data in the edges because edge areas of an image are not properly visible to Human systems as compare to the center part of an image. An Adaptive steganography method with edge identification technique is proposed. This technique will perfectly reveals the part of edges in cover image and shows the accurate position of the secret data to be hide. Experiment has been perform on the above methods, which attains a better imperceptibility, rather than other methods.

Keywords: *Steganography, Cryptography, Data Hiding, Steganography algorithms.*

1. Introduction

The prime concern for any of the organization is security of their information, which actually introduced to further data security research. We have promoted Cryptography for secure data transmission and its reliability. An encrypted data raise to be suspicion for unethical attackers. In the rapid growth of networking, steganography is brought to overcome this weakness by intangible by putting secret data into stago image without brings any attention to be suspicion [1]. This feature of interment of steganography makes itself different from cryptography. Now a days hidden conveyance are revealed for the protection of information from close observation by using these kind of steganography approach. Fingerprinting and digital signature could be the

major application of proposed technique [2]. The Volume, Intangibility and Robustness are three major factor to take care while using steganography methods observed by Johnson et al [3]. The volume signifies the amount of information that can hide behind the cover image. Robustness concern with the security of information from unethical attackers whereas, intangibility calcite the quality of an image via calculating the PSNR (Peak-signal-to-noise).

Figure 1. Scheme for data hiding.

Image steganography can be categorized in basic components: spatial domain and frequency domain. In spatial domain technique, data can hide directly into pixels intensity of an image, whereas frequency domain techniques, confidential data is inserted directly into transform coefficients. LSB (Least Significant Bit) is a conventional spatial domain technique which supply high capacity and minimal computational complexity. This type of method does not resist attack from adversary. DWT (Domain Wavelet Transform) and DCT (Discrete Cosine Transform) of transform domain techniques that are used to provide higher robustness against attacks. Adaptive steganography gives better result and known as "Satistics embedding". This method obtain statistical global attributes of the stego image that tells where to make changes before inserting confidential data into LSB/DCT coefficients.

The Edge areas of an image can be utilized for concealing secret data so that it won't affect the visual quality of stago image. Humans Visual systems are comparatively less sensitive to focus on edge location of an image compare to uniform colors or smooth surface. Hence, hiding confidential data onto the edge on an image give better imperceptibility of stego images.

Steganography has come up with more efficient techniques that people would like to join World Wide Web revolution. As the growth in Information and Communications Technology, Mostly the information been kept in gadgets. We all know that Technologies are developing very faster day by day. Hence, huge amount of data or information passing from one place to another on a large scale. Therefore, which raises the questions on the security of Data communications. In this project for the shake of protection of our Data or any information, we are using Adaptive Steganography Method through Fuzzy logic edge identification technique. This technique is used for determining the edge areas in image pixels. As a result, it improves the visual quality, capability, robustness of an image and keep it safe from illicit hackers. The main purpose of using adaptive steganography with fuzzy logic is to hide the secret information in the edges because edges areas of any image are less reactive or delicate to any other third party. The pixels which have "high" edge strength called as edge pixels and those pixels which have low or medium edge strength are called non edge pixels of an image. Hence, we can conceal the secret message in the edges without any distortion in an image using fuzzy logics.

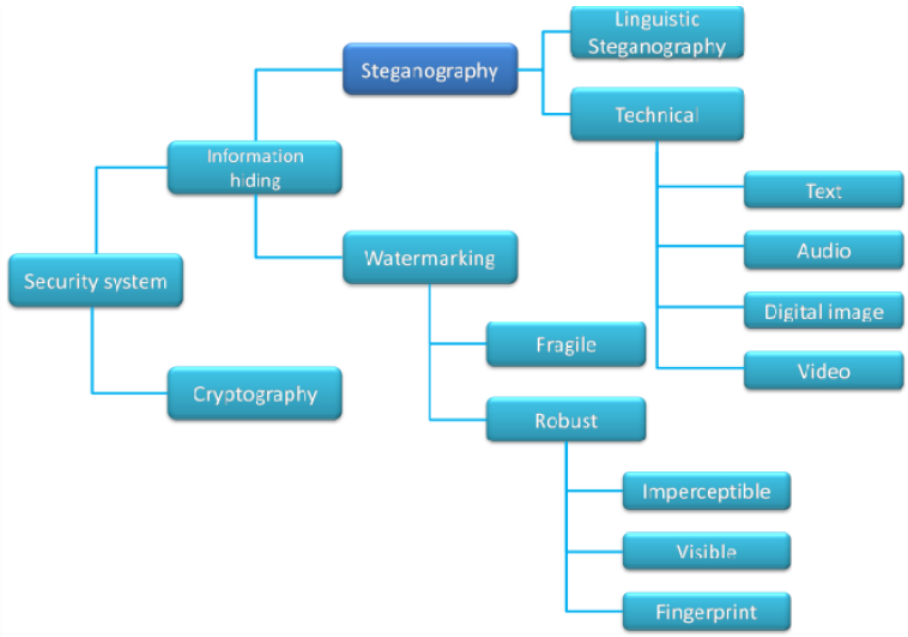

Figure 2. Domain specific categorized Steganography.

2. Related Work

Hiding data onto the edge plays a vital role in image steganography that means edge location can be utilized for hiding confidential information while maintaining good perceptibility. The pixel values of an image at edges has inconstancy. There is diverse classical edge detectors encounters through the literature, i.e., Laplacian, Canny, Robert, Sobel, Prewitt operators. In academic sector, canny edge and fuzzy logic edge majorly used [10] in spatial domain. The edge identification in case of Sobel edge operator are only performed on only one of the channel of R, G or B of any image. This method does not guarantee for high capacity of secrete data to hide.

There were many other techniques which was based on edge detection like Sobel, Canny, Hybrid, Bassil ,etc. Sobel[1] operator was used for color images steganography based on sobel operator in which edge identification was based on R,G,B Channel and we insert our any information or data on the basis of their intensity gradients,the major drawback of this technique that it may insecure the transferred data i.e, third party can easily access it.

Canny[2] operators were also introduced for edge detection method ,the method was able to hide the secret information from the illicit third parties but the major drawback of this technique that when the normal image was converted to stego image ,an image leads to distortion and sensitive to noise also. Hybrid[3] technique was introduced to embed multiple image process. It was possible by generate a secret key and that key was shared only between the sender and the receiver .Therefore, there was a no chance of involvement of third party to access that particular information .Hence, the capability of a image improved.

Bassil technique [4]which was based on the parameterized canny edge detection technique estimates the different output of a particular image .The three parameters was

- High threshold value
- Low threshold value
- Gaussian Filters

3. Problem Statement

The main problems in the Steganography are: The size of the data hidden as larger quantity of data embedded in the file can introduce suspect changes to the image which can be viewed by human eyes. The quality of the image can be compromised which can lead to distortion.

This project is developed for hiding information in any image file. The main objective of the project is implement different steganography tools for hiding information and compare the result and find out which algorithm is best in terms of t.

To design a User communication interface which uses the concept of data hiding in an image with edge detection method i.e. Steganography for securing confidential information through communication channel without any involvement of third party.

It is possible that visible encrypted data may arise suspicion of any other person so, he will try to decrypt that data. This will arise the situation of message being viewed by any other person (other than sender and receiver). However, by hiding a text file or an image file besides an image no one will came to know that something is hidden, as the processed image looks similar to the original one and it could not be seen with naked eye. This ensures the security of our data and hence only the sender and receiver knows the reality.

4. Methodology

People had been using Steganography from ancient times to hide data. The secret message will be visible only to sender and receiver and not any third party. Let us consider one sentence "Where real interesting technical changes can overcome dull environment." From the first letter of every word we will get a message "write code." This can be easily visible. More efficient hiding techniques use second or third letter of every word or it can be like first letter from the first word, second letter from the second word and so on. The result of Stagenography is something which looks as if there is nothing hidden and which prying eyes can't even see.

Hiding of information is the title for two techniques, the first one is used to protect the data from different attackers, which is Steganography which is the topic of our interest and the second method is basically used to demonstrate the personal rights, or ensuring reliability of our data is Digital Watermarking. There is a major difference between Steganography and other hiding techniques which enables transferring of secret information., for example, in cryptography, one can notice the information by seeing the coded data but it is not possible to mentally grasp it. However, if we are using Steganography the results of hiding are not visible to the naked eye.

Stagenography had been widely used from the ancient times by these ways.

- Confidential messages on paper were written using secret inks, or underneath other messages or on the blank spaces existing in messages.
- Messages were written on yarn by the use of Morse code and then were knitted in a clothing which were worn by couriers.
- During the times of World War two, photosensitive glass was used as a medium by armies to send secret information.
- Messages were written in the areas which were covered by postage stamps in an envelope.

4.1.Module – I (LSB Adjustment Method)

In this method, we break the storing process into two steps,

- Storing structural part, and
- Storing data part in different positions.

Since structural part of an image takes less space comparing to the data part, the structural part of the sink image may be stored in the data part of the container image by using the most common least significant bit technique. Consequently, we can say a number of bits corresponding to a sink image. That means if M bits represents the original structured part of the sink image, we need only N(M) bits by the use of LSB techniques. It may be mentioned here that when one wants to store an adequate number, k, of sink images one can effectively save $\sum Mi -$ bits (where$1 \leq i \leq K$) or which may be quite large in size. Further, for security point of view, as we are inserting the stego-key before and after the structural part of each sink image it gives an additional layer of protection.

Proposed Techniques (Algo) & Implementation-Module-I(LSB)

Step 1: Ask User for either Encryption or Decryption.
Step 2: IF Encryption THEN go to Step 3.
ELSE go to Step 8.
Step 3: Ask the user for the image and the text file which contains the data.
Step 4: Open the image and the text file in rb (Read Binary) mode.
Step 5: First copy the Image header to a new file (.BMP Format) opened in wb (Write Binary) mode.
Step 6: Since each pixel contains 24 bits so we can replace every 8^{th} bit with a bit of the text file because it is the Least Significant Bit in each RGB i.e. Red Green Blue color bits and copy it to the new file.
Step 7: After that close the new file and all the other files.
Step 8: Ask the user for the image.
Step 9: Open the image in the rb (Read Binary) mode and open a new text file in wb (Write Binary) mode.
Step 10: Now read every 8^{th} bit from the image file after the header and copy it to the text file.
Step 11: Close all the file and now the new text file can be opened to read the Decrypted text.

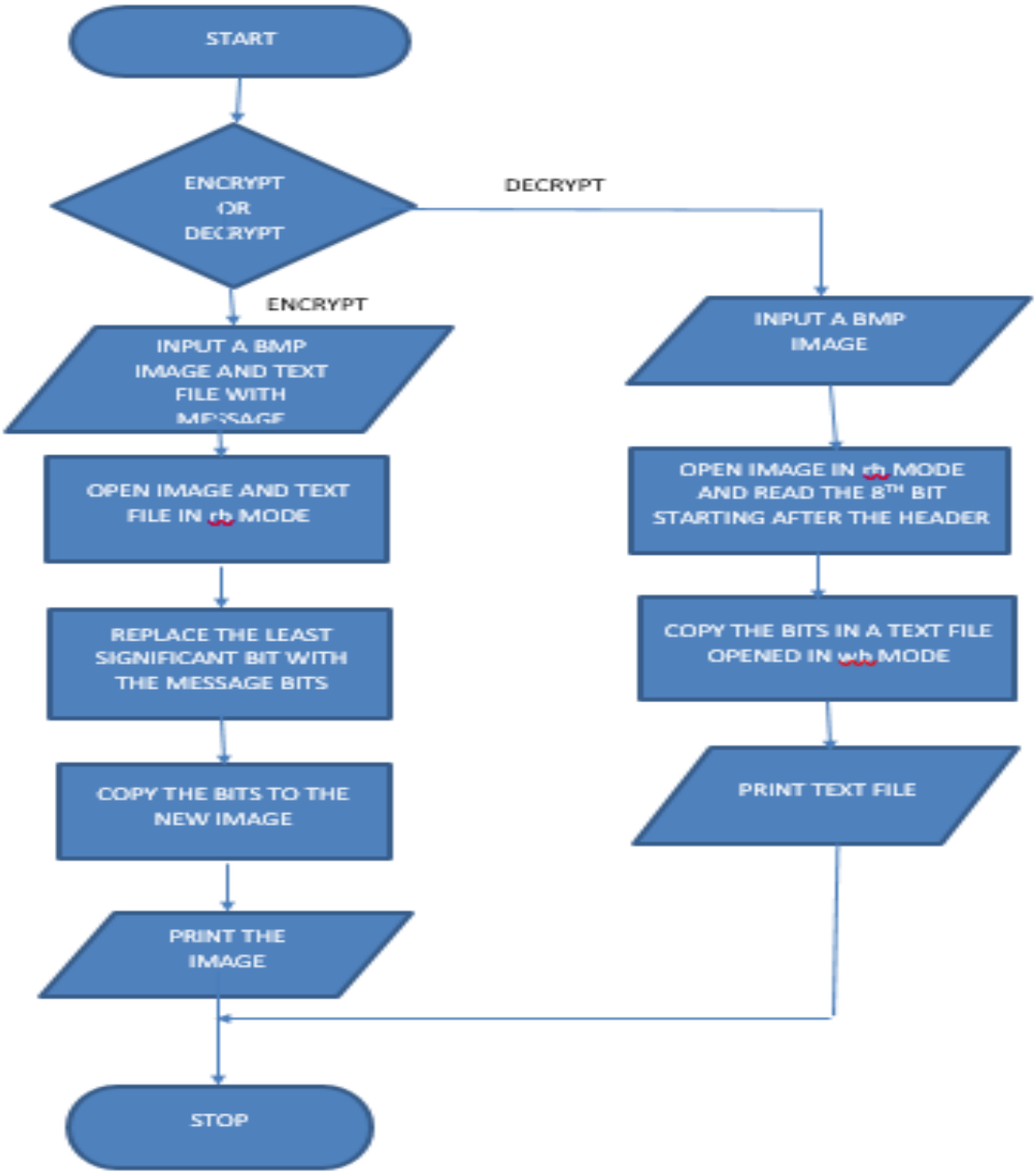

Figure 3. Flow chart for LSB (Least Significant Bit) to hide confidential data behind an image.

4.2. Module – II (DE algorithm)

Differential Evolution method proposed by Tian (2002). Differential Evolution technique mainly used to hide confidential data in pixel part. It employs higher interconnection of cover image, therefore high-interconnected cover image proposed for minimizing the deformation and improvising embedded volume. Assume that the couple of integral elements of high interconnected cover image as x & y used for embedding confidential data be D. Let the difference be z, integer mean be k and its inverse transform of x & y be given by z,

$$z = x - y$$

$$k = \text{floor}(|(x+y)/2|)$$

$$x = k + \text{floor}(|(z+1)/2|)$$

$$y = k - \text{floor}(|z/2|)$$

For embedding the confidential data D, the new difference be z' is obtained by,

$$z' = 2 * z + D$$

Therefore, the stego image pair (x' and y') is obtained by,

$$x' = k + \text{floor}(|(z'+1)/2|)$$

$$y' = k = \text{floor}(|z'/2|)$$

Proposed Techniques (Algo) & Implementation-Module-II(DE)

Step 1: Ask User for either Encryption or Decryption.
Step 2: IF Encryption THEN go to Step 3.
ELSE go to Step 8.
Step 3: Ask the user for the image and the text file which contains the data.
Step 4: Open the image and convert into grayscale image.
Step 5: First copy the Image header to a new file (.BMP Format) opened in wb (Write Binary) mode.
Step 6: Assume that the couple of integral elements of high interconnected cover image as x & y used for embedding confidential data be D. for embedding the confidential data D, the new difference value z′, the stego image pair (x' and y') is obtained.
Step 7: After that close the new file and all the other files.
Step 8: Ask the user for the image.
Step 9: Convert the image into grayscale format and open a new text file in wb (Write Binary) mode.
Step 10: Read every bit inserted by the help of stego image pair and the difference d.
Step 11: Close all the file and now the new text file can be opened to read the Decrypted text.

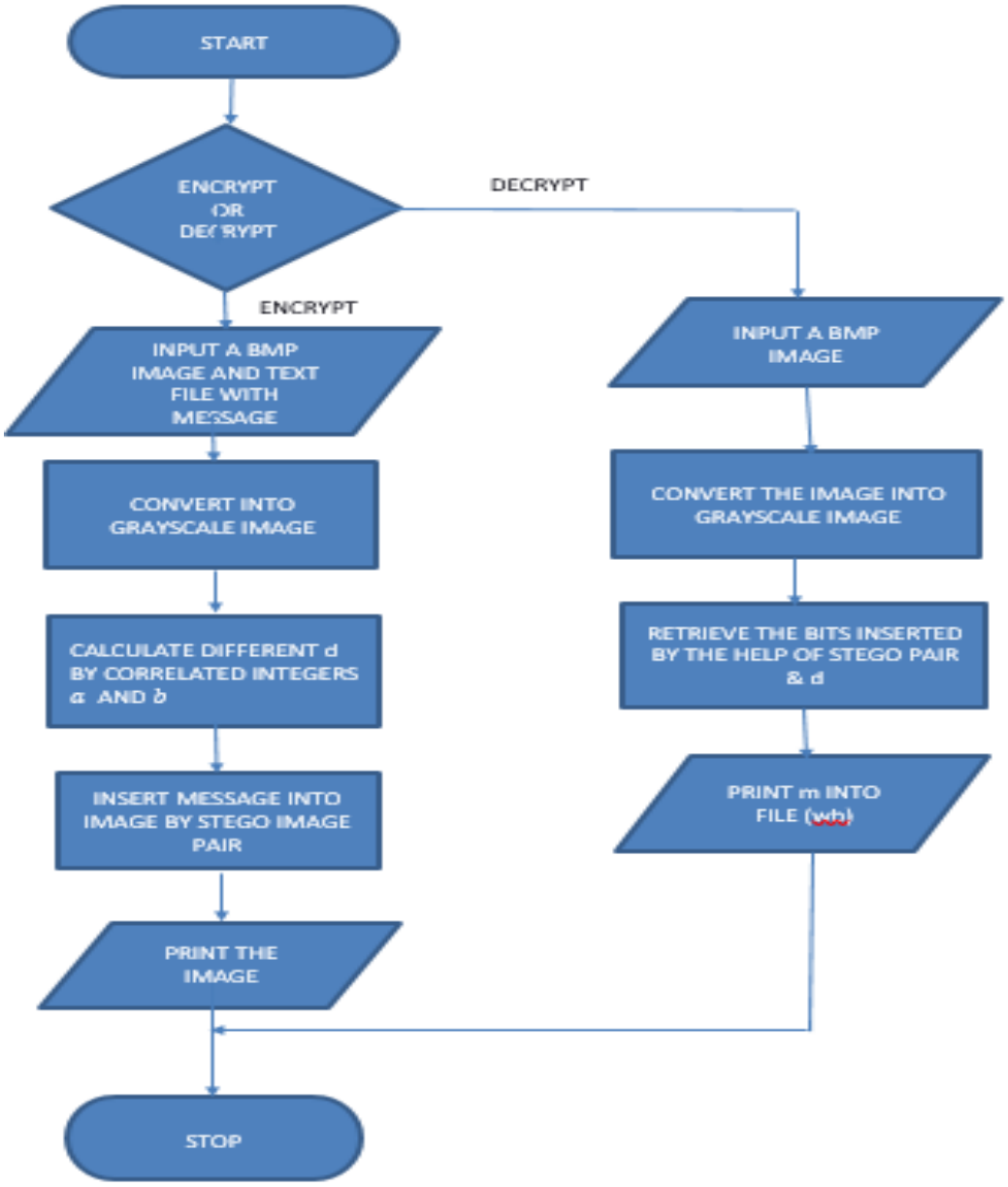

Figure 4. Flow chart for DE (Differential Evolution) to hide confidential data behind an image.

4.3.Module – III (Hide and Seek algorithm)

This algorithm randomly dispense the message or information all over the image. It is named after "Hide and Seek" - a Windows 95 steganography is little bit similar to that [5]. Let us say, it used single password for generating single random seed, and then need to pick the first position

to hide our confidential data into it. It continuously generating the position with the help of seed until the whole message is been hide. The way its hide the secrete message reveals the smarter way because every combination of pixels has to be repeated again & again for each and every order to try and "crack" the algorithm – until and unless we got password.

Proposed Techniques (Algo) & Implementation-Module-III(Hide and Seek)

Step 1: Ask User for either Encryption or Decryption.

Step 2: IF Encryption THEN go to Step 3.

ELSE go to Step 11.

Step 3: Ask the user for the image, the text file which contains the data and a password.

Step 4: Open the image and the text file in r (Read) mode.

Step 5: Read the first character of the password and convert it into its equivalent ASCII code.

Step 6: Traverse the same amount of bits obtained in our code after the header of the image and write the image to a new file at the same time of the traversal of the bits.

Step 7: After moving for one character of our password, we encrypt one character of our message in the succeeding bit.

Step 8: Now, we convert the second character of our password to its equivalent ASCII code and traverse the amount of bits in our image and copy it at the same time after the encrypted bit.

Step 9: Repeat Steps 7-8 for as long as the message needs to be encrypted. If our password is used and encryption still needs to be done, then go back to the first character of the password.

Step 10: After that close the new file and all the other files.

Step 11: Ask the user for the image and password.

Step 12: Open the image in the r (Read) mode and open a new text file in w (Write) mode.

Step 13: Convert the first character of the password to its equivalent ASCII code.

Step 14: Now read the equivalent bits from the image file after the header and copy the least significant bit from the next 8 bytes and then convert it into character and then copy it to the text file.

Step 15: Repeat for every other character of the password.

Step 16: Close all the file and now the new text file can be opened to read the Decrypted text

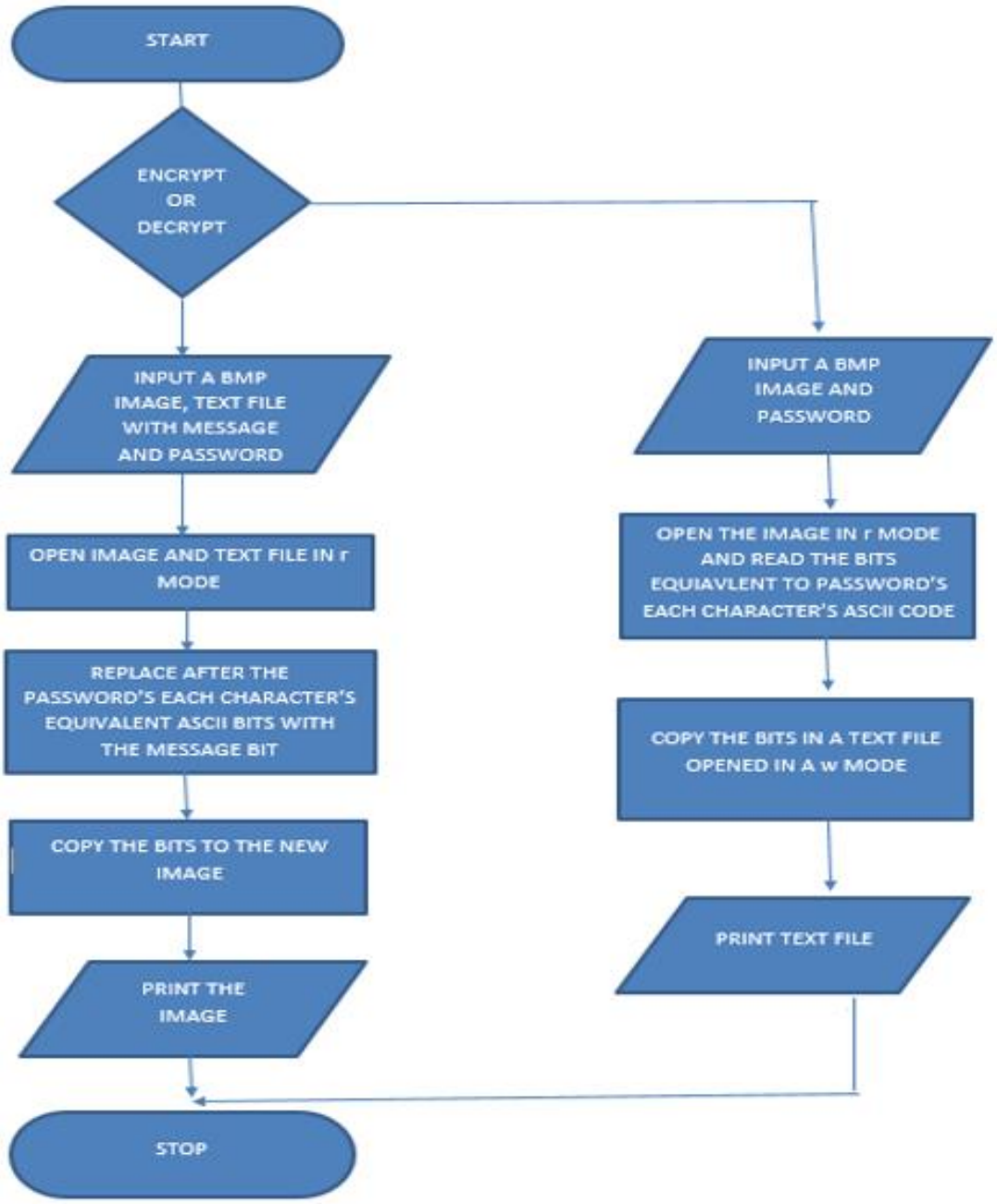

Figure 5. Flow chart for H & S (Hide and Seek) to hide confidential data behind an image.

5. Results

There is not much difference between the two algorithms as we can see from Figure 10. However, if we compare on the minute imagery, the Hide and Seek algorithm is better as our

data is scattered in our image compared to Least Significant Bit algorithm. In the future we will be more into adding filters to the image who sizes is too big to encrypt and try to implement it on other formats.

For LSB(Least Significant Bit)

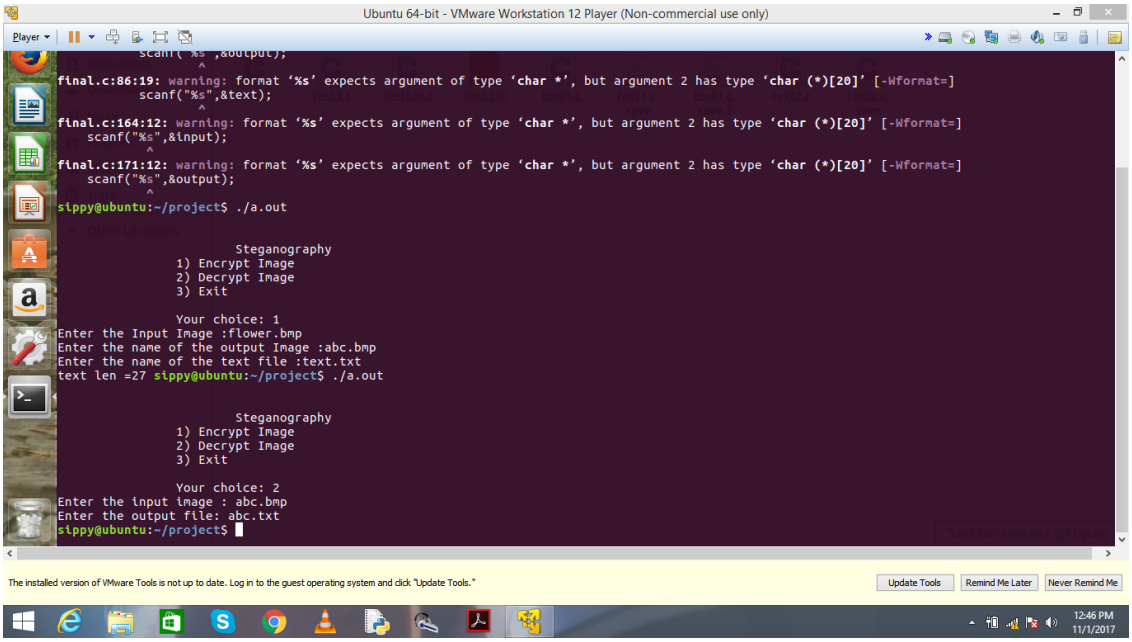

Figure 6. Demonstration for LSB implementation.

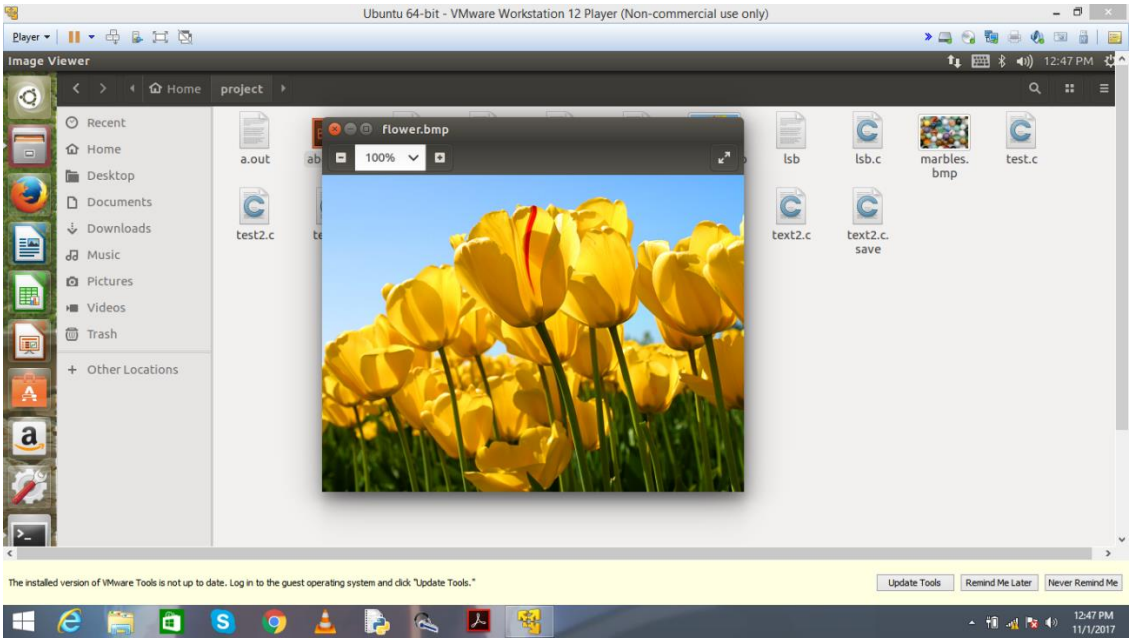

Figure 7. Cover image for LSB Implementation

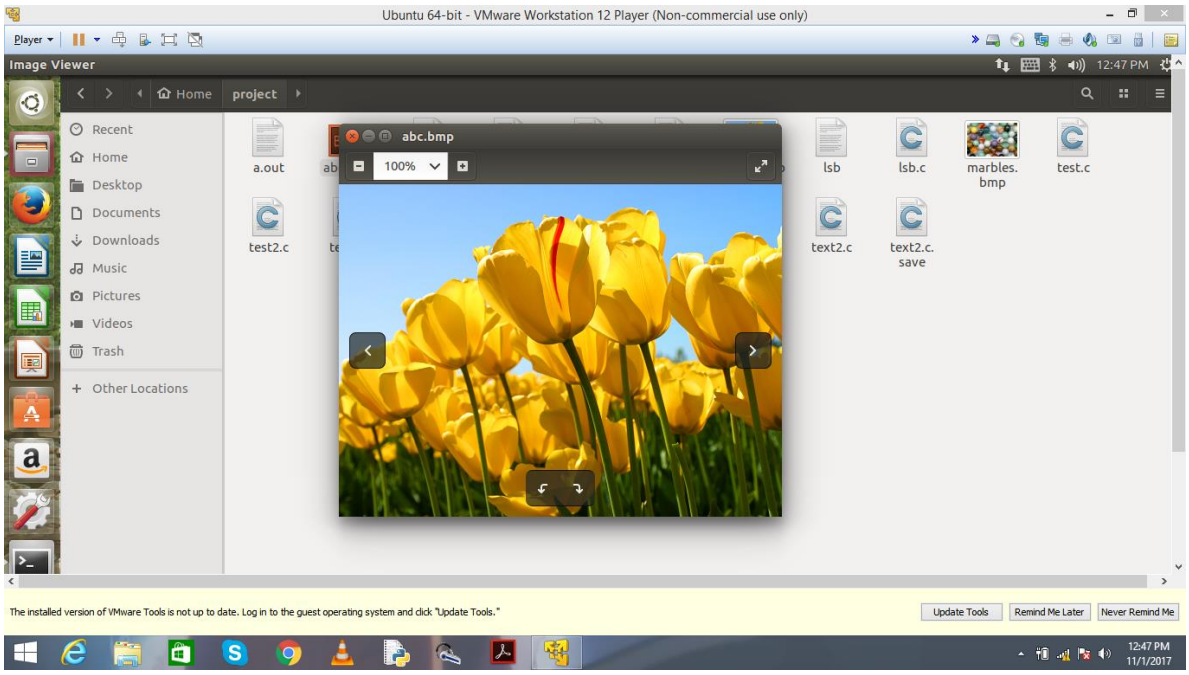

Figure 8. Stego Image for LSB Implementation

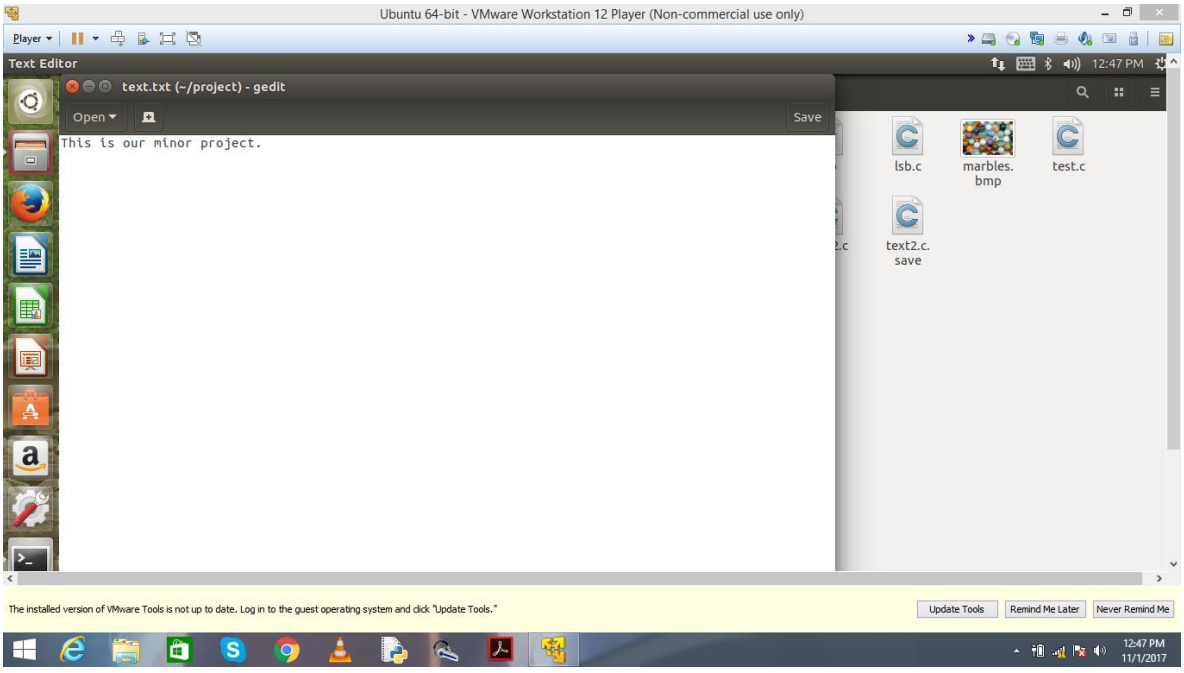

Figure 9. Text Hidden Behind the stego image

For Hide and Seek

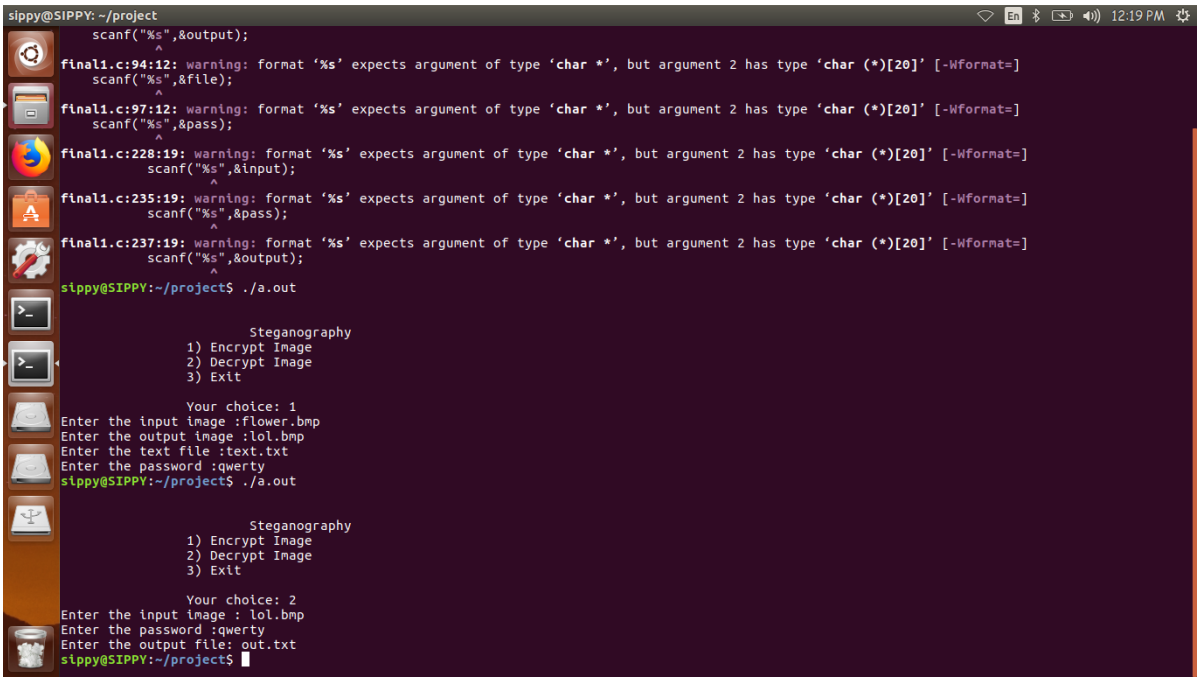

Figure 10. Demonstration of H & S(Hide and Seek) Algorithm for hiding text.

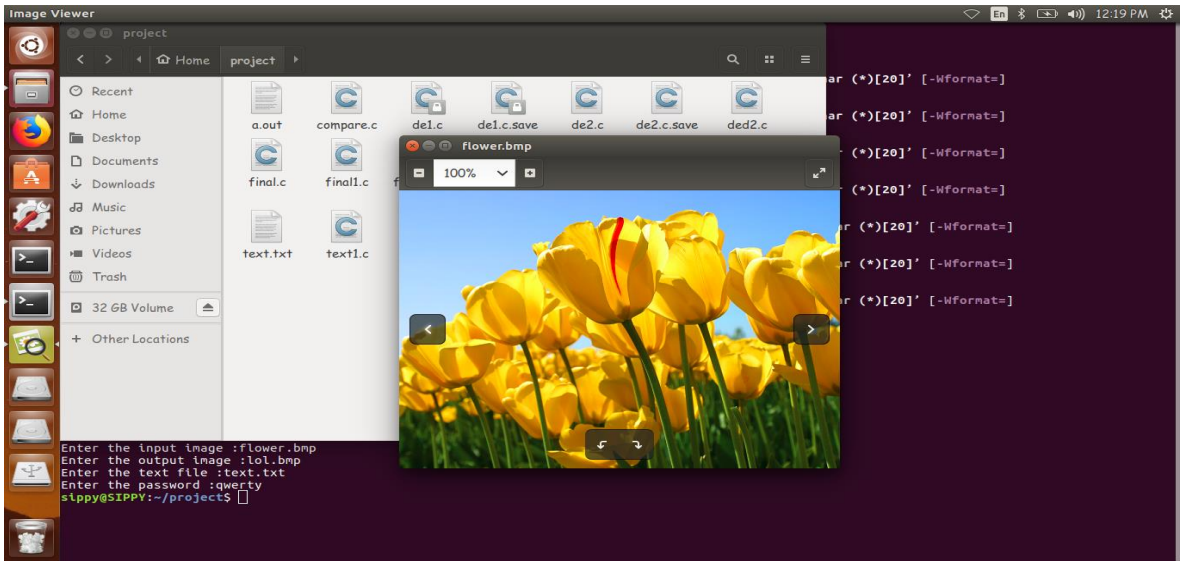

Figure 11. Cover Image for H & S(Hide and Seek) Algorithm for hiding text.

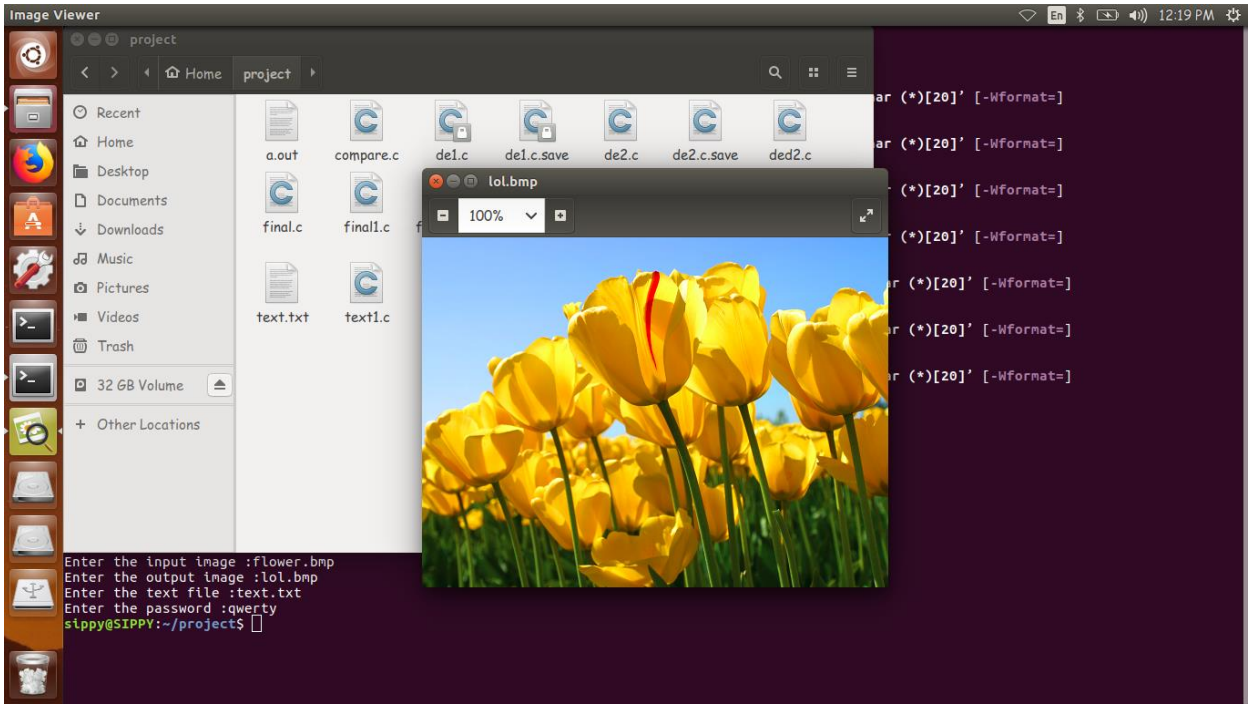

Figure 12. Stego image for H & S(Hide and Seek) Algorithm for hiding text.

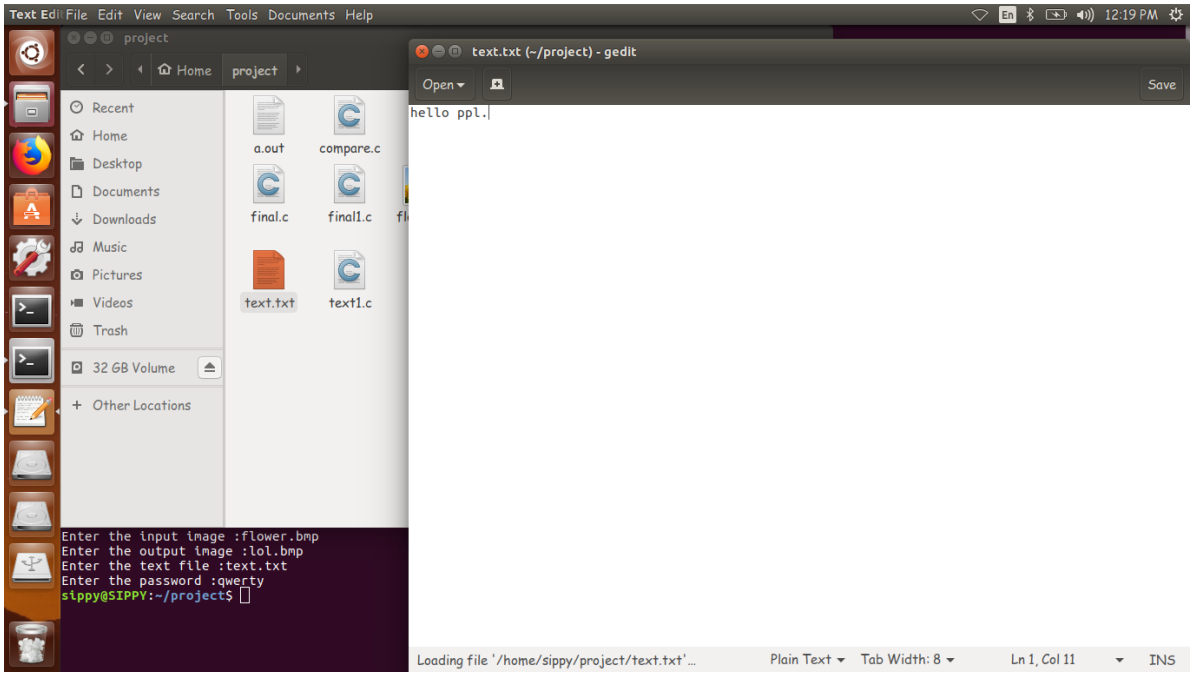

Figure 13. Text Hidden Behind the stego image.

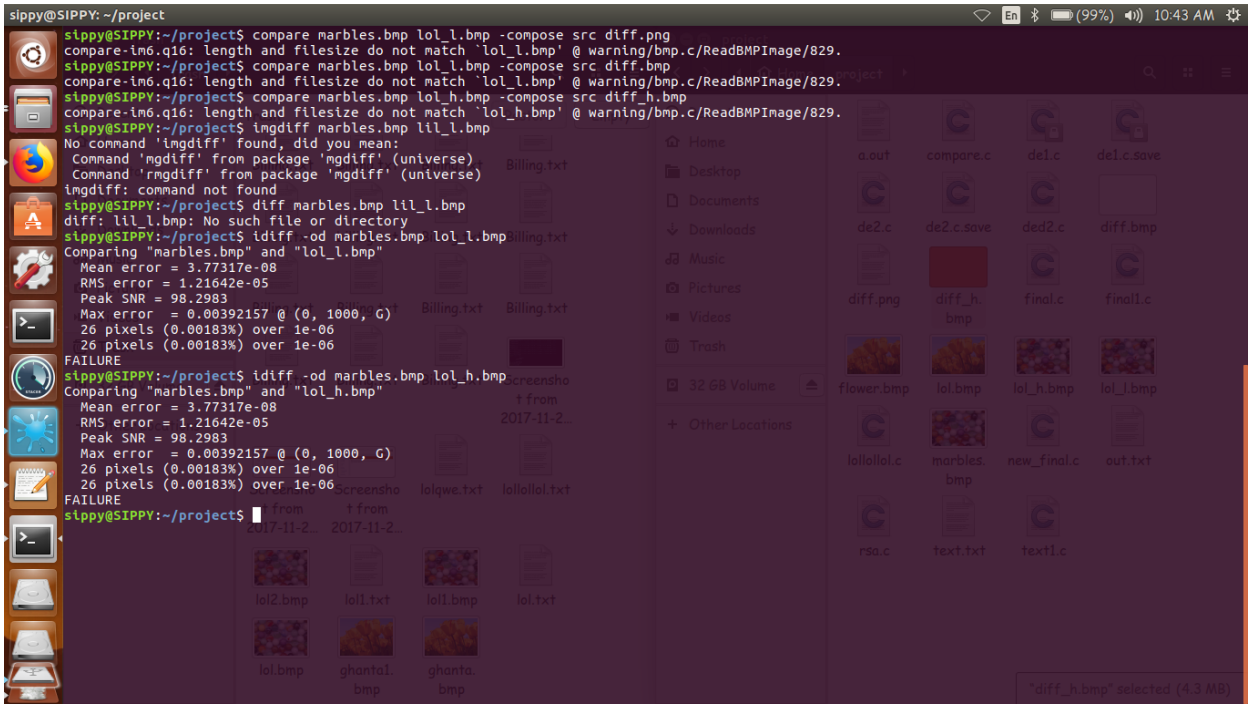

Figure 15. Demonstration of result of the paper.

6. Conclusion

In the rapid growth of networking, steganography is brought to overcome this weakness by intangible by putting secret data into stago image without brings any attention to be suspicion. LSB (Least Significant Bit) is a conventional spatial domain technique, which supply high capacity and minimal computational complexity. This type of method does not resist attack from adversary. DWT (Domain Wavelet Transform) and DCT (Discrete Cosine Transform) of transform domain techniques that are used to provide higher robustness against attacks. It was possible by generate a secret key and that key was shared only between the sender and the receiver .Therefore, there was a no chance of involvement of third party to access that particular information .Hence, the capability of a image improved. There is not much difference between the two algorithms. However, if we compare on the minute imagery, the Hide and Seek algorithm is better as our data is scattered in our image compared to Least Significant Bit algorithm. In the future we will be more into adding filters to the image who sizes is too big to encrypt and try to implement it on other formats.

References

[1] *Tang W., Li H., Luo W., Huang J. Adaptive steganalysis based on embedding probabilities of pixels IEEE Transactions on Information Forensics and Security, 11 (4) (2016), pp. 734-744.*

[2] *Harsh Prayagi, Tushar Srivastava, Gyanendra Ojha, Sunil Chaurasia "Information Hiding in an Image File: Steganography" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3), 2012, 4216-4217.*

[3] *C. Qin, X. Zhang Effective reversible data hiding in encrypted image with privacy protection for image content J Vis Commun Image Represent, 31 (2015), pp. 154-164.*

[4] *T. Filler, J. Fridrich, Design of adaptive steganographic schemes for digital im- ages, in: Proc. SPIE - Electronic Imaging, Media Watermarking, Security and Forensics of Multimedia XIII, 7880, 2011, pp. 1–14.*

[5] *P. Bas, T. Filler, T. Pevný Break our steganographic system the ins and outs of organizing boss ACM workshop on information hiding and multimedia security (2011), pp. 59-70.*

[6] *S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R.H. Deng, "Dynamic Secure Cloud Storage with Provenance", Cryptography and Security, pp. 442–464, Springer, 2012.*

[7] *J. Fridrich, J. Kodovsky Rich models for steganalysis of digital images IEEE Transactions on Information Forensics and Security, 7 (3) (2012), pp. 868-882.*

[8] *R.J. Anderson, F.A. Petitcolas On the limits of steganography Selected Areas in Communications, IEEE Journal on, 16 (4) (1998), pp. 474-481.*

[9] *C. Munuera Steganography from a coding theory point of view Algebraic Geometry Modeling in Information Theory, 8 (2013), p. 83.*

[10] *J. Anderson, F. Petitcolas On the limits of steganography IEEE J Selected Areas Commun, 16 (1998), pp. 474-481.*

[11] *N. Provos, P. Honeyman Hide and seek: an introduction to steganography IEEE Security & Privacy Magazine, 1 (2003), pp. 32-44.*

[12] *R.Z. Wang, C.F. Lin, J.C. Lin Image hiding by optimal LSB substitution and genetic algorithm Pattern Recognition, 34 (3) (2000), pp. 671-683.*

[13] Xiaoxia Li, Jianjun Wang A steganographic method based upon JPEG and particle swarm optimization algorithm Information Sciences, 177 (2007), pp. 3099-3109.