A Message Retrieval by Pixel Reading approach on Image Steganography to hide message over Image

Aarti Choudhary, Dr. Arun JB

Abstract— **Steganography refers to the information hiding. The main purpose of steganography is to hide the data behind images. It means that it encrypts the text in the form of image. The steganography is done when the communication takes place between sender and receiver [5]. Now a day's in data transfer over the network, the security is the main issue concerned with this. In order to secure the data while transmission steganography is used. Before the development of the steganography, Security of the data is the main concern of research for the researchers. The number of techniques was developed in order to secure transmission. Steganography use algorithms for hiding the data. In this the data is hiding behind the cover image. The data is hidden character wise behind the pixels of the image. The various algorithms or techniques used for steganography are LSB-Hash, RSA Encryption and Decryption**

Index Terms— **Data hiding; Audio; Video; Text; Security; LSB; Encryption**

I. INTRODUCTION

In this modern era, where technology is developing at fast pace and each day new developments are made, security is of utmost priority. The data needs to be kept secure and safe so that it could be accessed only by the authorized personnel and any unauthorized user cannot have any access of that data. Data sharing is increasing as thousands of messages and data is being transmitted on internet everyday from one place to another. The protection of data is prime concern of the sender. The need is that correct data should be sent but in a secret way that only the receiver should be able to understand the message. At first technique of cryptography was invented to send secret messages over places. In cryptography the message was encoded in another message in a covered way such that only the sender and receiver knew the way to decrypt it [5]. A cryptographic key was used to decode the message that was known only by the authorized persons.
The limitation of cryptography was that other person came to know that the message had a hidden text in it and so the probability of message being decoded by other person increased. To overcome this limitation the technique of steganography was introduced.
The word steganography belongs to Greek language. In Greek the steganography stands for "covered writing".

The first of all steganography was used in Greece. They use to enter the message on a wooden tablet and then apply wax on it to hide the written data. The technique of steganography was far better than cryptography as in it the data was hidden in image.

The image was then sent over internet. It had advantage over cryptography as now the middle person does not come to know whether data is hidden in the image or not. The data could only be decrypted from image by the authorized person as he knows the phenomenon to decode it and had the authorized key with him that was required to decode the data. The security and the reliability of data transmission also improved with invention of steganography as now no other person could change the sent data. The main application fields of steganography are [4]:

- Copyright Protection
- Feature Tagging
- Secret Communication
- Use by terrorists
- Digital Watermarking

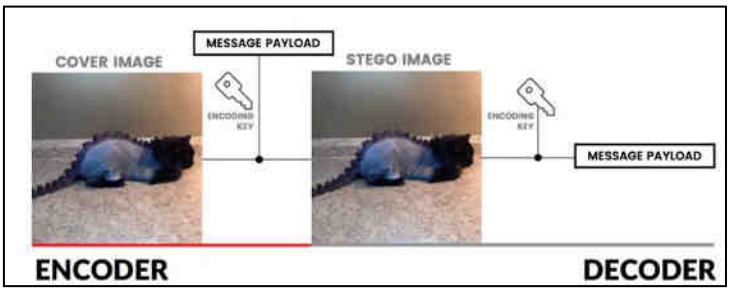


Diagram: Steganography Process

The steganography is done for the purpose of data security. The various techniques are used for steganography. The techniques are LSB, Data Compression, Masking and Filtering, Distortion Technique etc…

II. TECHNIQUES OF STEGANOGRAPHY

The various techniques for steganography is are as follows [4]:

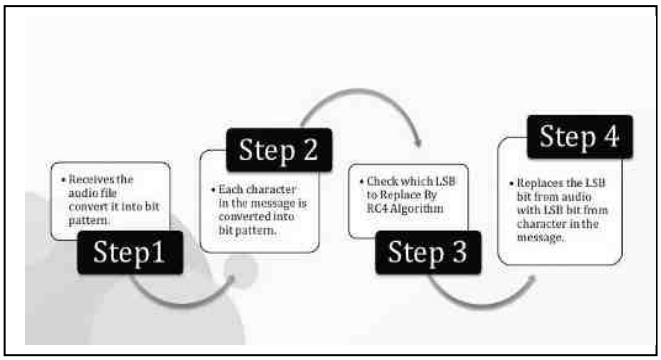
- LSB
- Distortion Technique
- Masking and Filtering
- Transform Domain Technique

A. LSB

LSB stands for Least Significant Bit. This is a technique for image steganography which works on the Least Significant Bit value of the pixels. This technique does not lead to any kind of distortion in the image while embedding data behind it. The value of least significant bit varies but this change is invisible to human eye. The LSB have many advantages such

Manuscript received Feb 26, 2019
Aarti Choudhary, Research Scholar, Bhagwant University, Ajmer, Lecturer, TTC& LRDC, Jodhpur
Dr. Arun JB, Research Scholar, Bhagwant University, Ajmer, Lecturer, TTC& LRDC, Jodhpur

as the image does not depreciated or distorted and by using LSB one can encrypt large amount of data behind an image.[5]



B. Distortion Technique

Distortion technique encrypts the data by decoding it. In this original cover image is decoded into encrypted or distorted cover image. In this technique the receiver applies a function on encrypted or decoded image in order to decrypt it. In this steganography is applied by making distortions in image. This technique perform a sequence of alterations in cover image. Then this sequence is applied for the purpose of comparing the encrypted message with forwarded message. The data is encrypted behind randomly selected pixels. In case when the encrypted image vary from original image then bit "1" is used else bit "0" is used. In this cover image is send to the receiver which is a barrier in the security provided by this technique. It is a rule tat the cover image should always used for once while steganography if any cover image is used more than once in steganography then it will easy for the intruders to attack the image for accessing the enc rypted data behind the image [5].

C. Masking and Filtering

This technique works similarly to the technique of watermarking. In this case data is not hidden behind any image.

Instead of hiding data is appended or inserted on such space which is secure from attackers. In this technique watermarking is used for securing the data. This method facilitate the user with the feature of robustness, compression is done because data is embedded on a secured surface and visible to everyone. The limitation of this system is that it is meant for only gray scale images [5].

D. Transform Domain Technique

This technique posses much complexity as compare to other techniques. It performs steganography by hiding the data behind an image. It uses many algorithms to encrypt the data. Some transformations are also used for steganography. As it is clear from the name of the technique that number of transformation domains are used for embedding the data a nd then further algorithms are used for encryption. The data is embedded in frequency domain. It is much preferable technique of embedding the data in comparison of time domain. This technique hides the data in that images which are safe from attackers and there is no need of data compression in this technique [5].

III. OUR TECHNIQUE OF STEGANOGRAPHY

In order to maintain the first order statistics of the cover image, we have proposed a scheme which inherently preserves the first order properties of the signal. The scheme is outlined below:

Algorithm Pixel Swap:

1. 1.We select a carrier image.
2. 2.We know that an image is nothing but a plane of pixels and each pixel has two properties, its location (x, y) and its color (R,G,B).
3. 3.We use the Blue color property of the pixel's RGB model and hide our message in each of the pixels as ASCII encoded message.
4. 4.As we can see in the above diagram, we use the (0, 0) index to put in the number of digits in the message length integer.
5. 5.Then we insert the message length according to number of digits in it.
6. 6.Once, we store the message length we can store the message character by character (ASCII encoded), pixel by pixel.

Message Retrieval by Pixel Reading (in Image):

1. 1.We read the carrier image.
2. 2.We know, at (0, 0) at B's value, we have the Digits in Message Length.
3. 3.Then, we read the Message length according to the digits it has.
4. 4.Once, we have the message length, all we have to do is read the message character by character and pixel by pixel.
5. 5.Once we've read the message, we now decode it from ASCII to readable text.

Carrier image (without message)

Carrier image (with encrypted message)

As we can see, in an image the difference is unnoticeable, if someone doesn't know the location of the message, he's highly unlikely to decipher it.

CONCLUSION

Steganography is the process to transmit the message over network with secure key and only sender and receiver can know the decryption process to recover the secret message. Steganography increase the security in remote communication to transfer high confidential message to the next party. and also ensures that only authorized personnel can have access to that message. This paper presents a review and implementation of new approach of steganography and techniques that are used for image steganography. Futher addition to be made in this technique for Video Steganography, Password Protection, Blank pixel detection

REFERENCES

[1] Amritpal Singh, "An Improved LSB based Image Steganography Technique for RGB Images", Electrical,Computer and Communication Technologies (ICECCT)
[2] Mehdi Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Scienceand Technology Vol. 54, May, 2013, pp 113-124
[3] R.Poornima, "AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY", (IJCSES) Vol.4, No.1,February 2013, pp 23-31
[4] Shaveta Mahajan, "A Review of Methods and Approach for Secure Stegnography", IJARCSSE, Volume 2, Issue 10, October 2012, pp 67-70
[5] Jasleen Kour, "Steganography Techniques –A Review Paper", International Journal of Emerging Research inManagement &Technology, Volume-3, Issue-5, May 2014, pp 132-135
[6] Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", AppliedMathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915
[7] C.P.Sumathi, "A Study of Various Steganographic Techniques Used for Information Hiding", InternationalJournal of Computer Science & Engineering Surve(IJCSES) Vol.4, No.6, December 2013, pp 9-25
[8] Rashi Singh, "A Review on Image Steganography", IJARCSSE, Volume 4, Issue 5, May 2014, pp 686-689
[9] Gunjan CHUGH, "IMAGE STEGANOGRAPHY TECHNIQUES: A REVIEW ARTICLE", 2013. Fascicule 3 [July–September], pp 97-104
[10] Stuti Goel, "A Review of Comparison Techniques of Image Steganography", Global Journal of ComputerScience and Technology Graphics & Vision Volume 13 Issue 4 Version 1.0 Year 2013, pp 8-14
[11] Rakhi, "A REVIEW ON STEGANOGRAPHY METHODS", IJAREEIE, Vol. 2, Issue 10, October 2013, pp 4635-4638
[12] Anjali Tiwari, "A Review on Different Image Steganography Techniques", IJEIT, Volume 3, Issue 7, January 2014, pp 121-124
[13] Soumyendu Das, "Steganography and Steganalysis: Different Approaches"
[14] Amandeep Kaur, "A Review on Image Steganography Techniques", International Journal of Computer Applications (0975 – 8887) Volume 123 – No.4, August 2015, pp 20-24
[15] Abbas Cheddad, "Digital Image Steganography: Survey and Analysis of Current Methods", Signal Processing,Volume: 20, Issue: 3, March 2010, pp 727-752

AUTHOR PROFILE

Aarti Choudhary Graduated in B.E. [IT] from RCEW , Jaiur. She received Masters degree in M.Tech [CSE] from JNU, Jodhpur. She is pursuing Phd from Bhagwant University, Ajmer. Her Interested areas are Theory of Computation, Computer Organization, Network Security and Cryptography.

Dr. Arun JB completed his M.Tech[EE] and PhD [Soft computing] from JNVU Jodhpur. Presently he is working as an Lecturer instrumentation TTC & LRDC, Jodhpur His research interests include Data computing , Network Security, etc. He has published research papers in various National, International conferences, proceedings and Journals.