A Novel Approach for Hiding Encrypted Data in Image, Audio and Video using Steganography

V. Lokeswara Reddy
Associate Professor,
Department of CSE,
K.S.R.M. College of Engg., Kadapa,
Y.S.R. Dist., A.P.(INDIA)

A.Subramanyam
Professor & Head,
Department of CSE,
AITS, Rajampet,
Y.S.R. Dist., A.P. (INDIA)

P. Chenna Reddy
Professor,
Department of CSE,
JNTUCE, Pulivendula,
Y.S.R. Dist., A.P. (INDIA)

ABSTRACT
Today's large demand for internet applications requires data to be transmitted in a safe and secure manner. Data transmission in public communication system insecure because of interception and improper manipulation by eavesdropper. So the solution for this problem is Steganography, Steganography is the art of hiding one medium of information into another medium. There are many approaches for hiding textual information in multimedia file such as image, audio and video. Hiding textual information in multimedia file provides the most effective way to guard privacy. Key aspect of embedding text in multimedia file is that, after embedding text in multimedia file the size of the multimedia file remains same. The existing system can't provide more security and message length is restricted to few characters only. The proposed technique alters the data of lower bit in a cover object to embed textual information. The main goal of this paper is to embed textual information into multimedia file and the text message is encrypted before embedding to get advantage of cryptography.

Keywords Steganography, Data Hiding, Extraction, Cover Object, Stego object

1. INTRODUCTION
The main goal of steganography [1] is to hide a secret message within a cover-media in such a way that others cannot detect the presence of the hidden message. The word steganography originated from Greek and means "concealed writing" from the Greek words 'steganos' meaning "covered or protected", and 'grapheia' meaning "writing". The carrier image in steganography is called the "cover image" and the image which has the embedded data is called the "stego image".

Cryptography conceals about content or meaning of a message, while steganography conceals about the very existence of a message. There exist many steganographic techniques are available for hiding information in different carriers. In early days the secret messages hiding was done in documents [2].The use of Steganography in documents works by simply adding white space and tabs to the ends of the lines of a document. This type of Steganography is extremely effective, because the use white spaces and tabs are not visible to the human eye at all, at least in most text/document editors. White space and tabs occur naturally in documents, so there isn't really any possible way using this method of steganography would cause someone to be suspicious. It is used in initial decade of internet era. But it is not used frequently because documents have a small redundant data.

Later hiding secret message in images becomes more popular technique for Steganography [3] especially on internet. Least Significant Bit (LSB) coding is used to embed secret data in images. The best type of image file to hide information inside of is a 24 Bit Bitmap (BMP) image. The reason being this is the largest type of file and it normally is of the highest quality. When an image is of high quality and resolution of it is a lot easier to hide and mask information inside. But this technique lacks in payload capacity and robustness. At present hiding data in audio files becomes more popular. Audio data hiding [4] method provides most effective way to provide privacy. Embedding the secret messages in digital sounds usually a very difficult process. There are many techniques available for hiding text in audio signal. Many methods have been proposed to protect the security of secret information, such as cryptography and steganography techniques. Cryptography techniques can scramble secret information into an unreadable message. However, the unreadable message can easily attract unauthorized attention. Steganography techniques can provide secure transmission by embedding secret information within cover carriers to avoid observation. The cover carrier can be an image or audio or video. The similarity between cryptography and steganography techniques is that only an authorized person with the right key can recover the secret information. Hence the best approach is to combine steganography and cryptography techniques to protect the security of secret information. In the same way, even if stego carriers are obtained by an unauthorized person, the secret message cannot be exposed. With rapid advancement in technology, steganographic software is becoming effective in hiding information in multimedia files such as image, video, audio or text files[5].

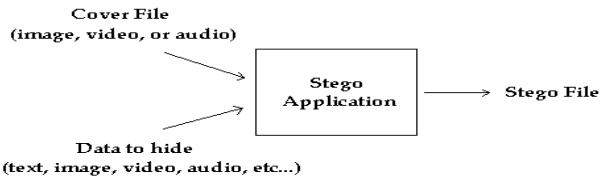


Figure 1: The block diagram of a Steganography Application Scenario

The steganography application hides different types of data within a cover file. The resulting stego file contains hidden information. The Figure 1 shows the block diagram of a steganography application scenario and Figure 2 shows the block diagram of a steganographic system.

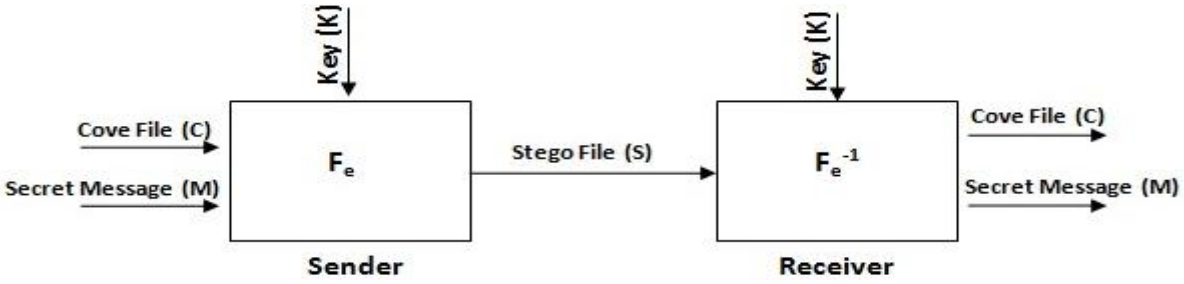


Figure 2: The block diagram of a Steganographic System

The Steganography application hides different types of data within a cover object. The resulting stego object also contains hidden information and it is similar to the cover object. A possible formula of the process may be represented as [6]

Cover Medium + Embedded Message + Stego Key = Stego Medium

Hiding information into a media requires following elements [7]

Cover File: The cover file (C) that will hold the secret data.

Secret Message: The secret message (M), may be plain text, cipher text or any type of data.

Stego File: The Stego file (S) contains the modified version of cover file that contains the secret message.

Key: The Key(K) is additional or optional secret data that is needed for the hiding and unhiding processes and must be known by the sender and receiver.

F_e: A steganographic function that has cover file, secret message and key as parameters and produce stego file as output.

F_e^{-1}: A steganographic function that has stego file and key as parameters and produces secret message as output. $F_e^{-1}$is the inverse function of F_e in the sense that the result of the unhiding process F_e^{-1} is similar to the input M of the hiding process F_e.

2. RELATED WORK

Information can be hidden inside a multimedia object using many suitable techniques. The cover object is image, audio or video file. Depending on the type of the cover object, definite and appropriate technique is followed in order to obtain security. In this section different techniques or methods which are often used in image, audio and video steganography are discussed.

2.1 Image Steganography

The image file is the most widely used cover object in steganography. The images are divided into three types: Binary (Black & White), Grayscale and RGB (Red-Green-Blue). The binary image has only one bit value per pixel, 0 represents black and 1 represents white. While the grayscale image has 8 bits per pixel, 00000000 represents black pixel and 11111111 represents white pixel. The RGB image has 24 bit per pixel, 00000000 (R), 00000000 (G) and 00000000 (B) represents black pixel and 11111111 (R), 11111111 (G), 11111111 (B) represents white pixel. The RGB image is the most suitable image file format for steganography, because it contains a lot of information that help in hiding the secret information with a bit change in the image resolution which does not affect the image quality. Image domain techniques can be divided into two groups: i) Spatial domain ii) Transform domain[8]. Spatial domain also known as Image domain, this technique embed messages in the intensity of the pixels directly, while for Transform domain also known as Frequency domain, this technique embed information in transform coefficients of the cover images. A number of ways exist to hide information in digital media. Common approaches include

- Least Significant Bit (LSB) insertion
- Masking and Filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Algorithms and Transformations

2.2 Audio Steganography

Audio steganography is a method that ensures secured data transfer between parties normally in internet community. In a computer-based audio steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. These methods range form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information. The methods that are commonly used for audio steganography are listed below.

- Least Significant Bit (LSB) Coding
- Parity Coding
- Phase Coding
- Spread Spectrum
- Echo Hiding

2.3 Video Steganography

Video file is generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. So, video steganography is nothing but a combination of image and audio steganography. So, the combined evaluations i.e., the evaluations for image and audio steganography can be taken together for the evaluation of video steganography[9]. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. A video stream consists of collection of frames and the secret data is embedded in these frames as payload[10].

3. LEAST SIGNIFICANT BIT INSERTION METHOD

Least Significant Bit (LSB) insertion method is a common, simple approach for embedding information in a cover media. The fundamental idea here is to insert the secret message in the least significant bits of the multimedia files.LSB algorithm is applicable for all kind of cover medium (Image, Audio, Video). LSB algorithm is used for both embedding and extraction process. A basic algorithm for LSB substitution is to take the first N cover pixels where N is the total length of the secret message that is to be embedded in bits. After that every pixel's last bit will be replaced by one of the message bits.

It is read that one byte at a time from the secret message file, it extracts 8 bits from that byte and then it is read 8 consecutive bytes from the cover file. After that it is checked that the least significant bit of each byte of that 8 byte chunk whether it is different from the bits of secret message or not. If it is different then it is replaced by the bit that obtained from secret message.

Table-1 shows the character and its equivalent ASCII code. Now, it shows how the cover text will be modified after inserting "A" within it.

Table 1. Character & Equivalent ASCII Code

Character	ASCII Code	Bit string
A	65	01000001
B	66	01000010
C	67	01000011
D	68	01000100
E	69	01000101
F	70	01000110
G	71	01000111
H	72	01001000

After embedding the LSB of the cover text by the bits of "A" the modified cover text is shown in Table-2.

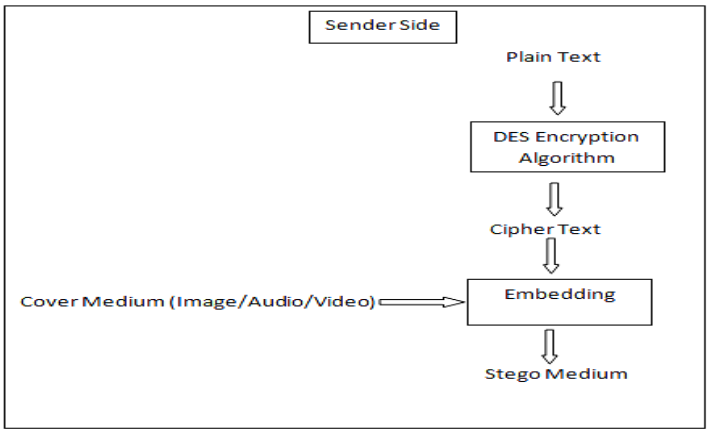
Here out of 64 bits only 4 bits get changed at the LSB position. After embedding "A" in cover text "BCDEFGHI" the cover text converted to "BCDDGFHH". As our eye is not very sensitive so therefore after embedding a secret message in a cover file our eye may not be able to find the difference between the original message and the message after inserting some secret message on to it.

4. PROPOSED SYSTEM

Among different information hiding techniques proposed to embed secret information within multimedia file, Least Significant Bit coding method is the simplest way to embed secret information in a multimedia file by replacing the least significant bit of multimedia file with a binary message. Hence LSB method allows large amount of secret information to be encoded in a multimedia file. The proposed system provides a basic view of multimedia steganographic process at sender and receiver side. At the sender side the text message is encrypted by using Data Encryption Standard (DES) algorithm using a key shared by both sender and receiver. Symmetric encryption is an efficient process for providing security to the secret message. The encrypted message is passed to embedding phase. In embedding phase the encrypted message will embedded into the cover medium which is either image/audio/video format (*.bmp/*.wav/*.avi) resulting a stego medium. The embedded stego medium contains the encrypted text message which is extracted at the receiver side. At the receiver side stego medium is passed to de embedding phase. In extraction process encrypted text will be extracted from embedded multimedia file and encrypted text is decrypted using decryption module. The steganographic system at sender side is shown in Figure 3 and stegangoraphic system at receiver side is shown in Figure 4.

Table2. CHANGING LSB

Original Text	**Bit String**	**Bit to be inserted in LSB**	**Changed Bit string**	**Changed Text**	**Remarks**
B	01000010	0	01000010	B	No Change in Bit Pattern
C	01000011	1	01000011	C	No Change in Bit Pattern
D	01000100	0	01000100	D	No Change in Bit Pattern
E	01000101	0	0100010**0**	D	Change in Bit Pattern
F	01000110	1	0100011**1**	G	Change in Bit Pattern
G	01000111	0	0100011**0**	F	Change in Bit Pattern
H	01001000	0	01001000	H	No Change in Bit Pattern
I	01001001	0	0100100**0**	H	Change in Bit Pattern



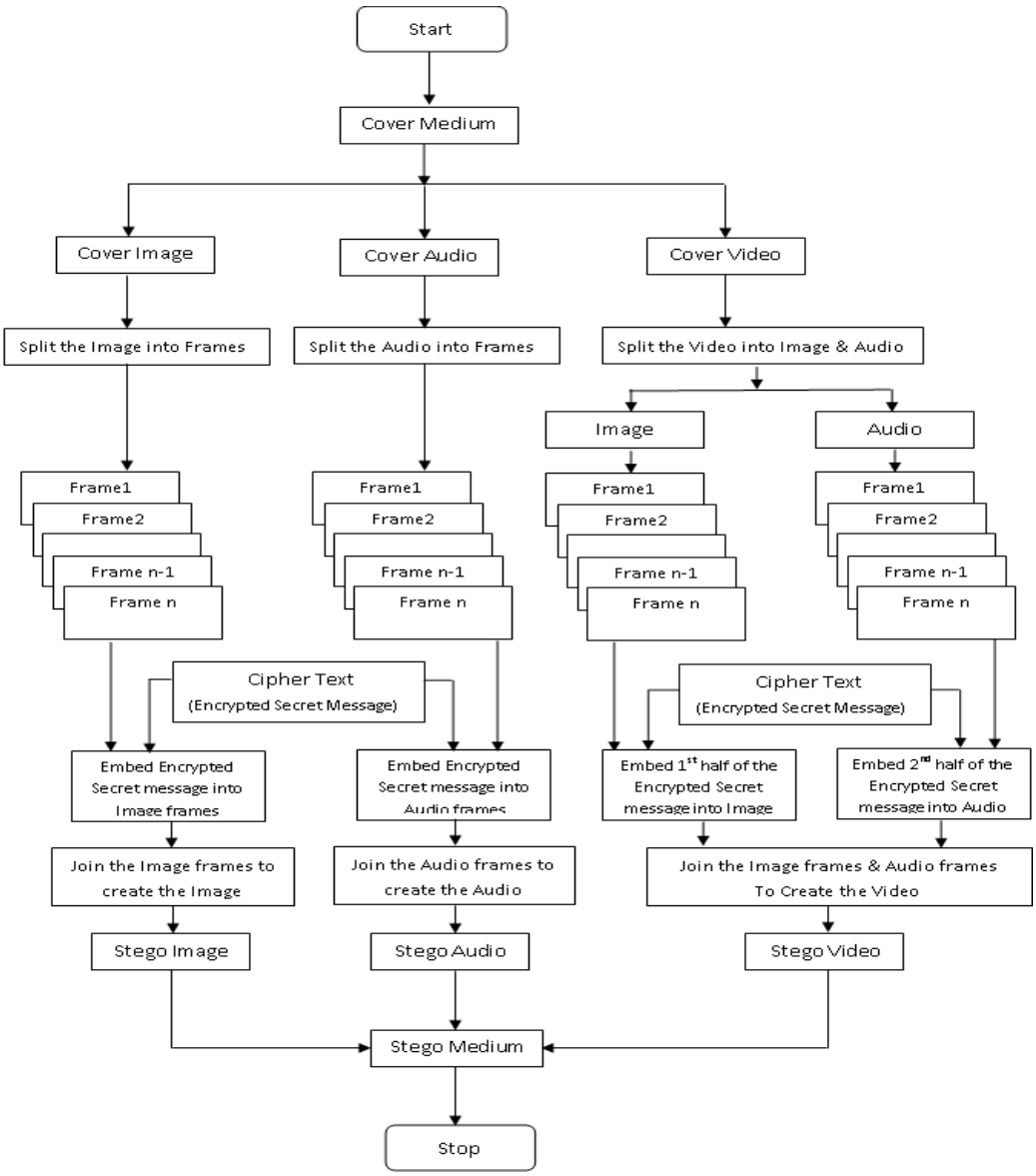
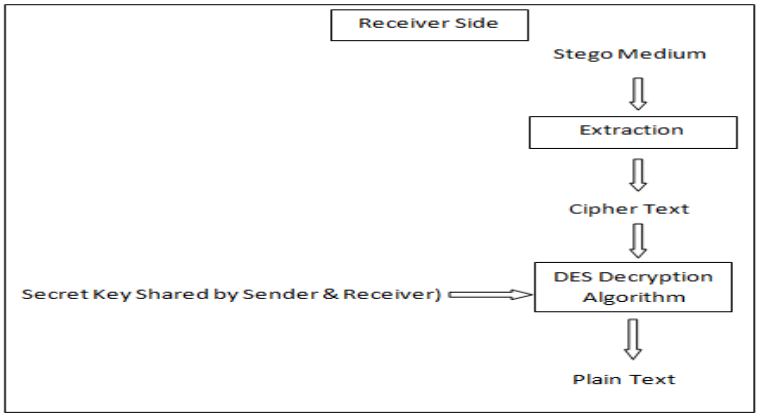


Figure 3: Steganographic System at Sender side



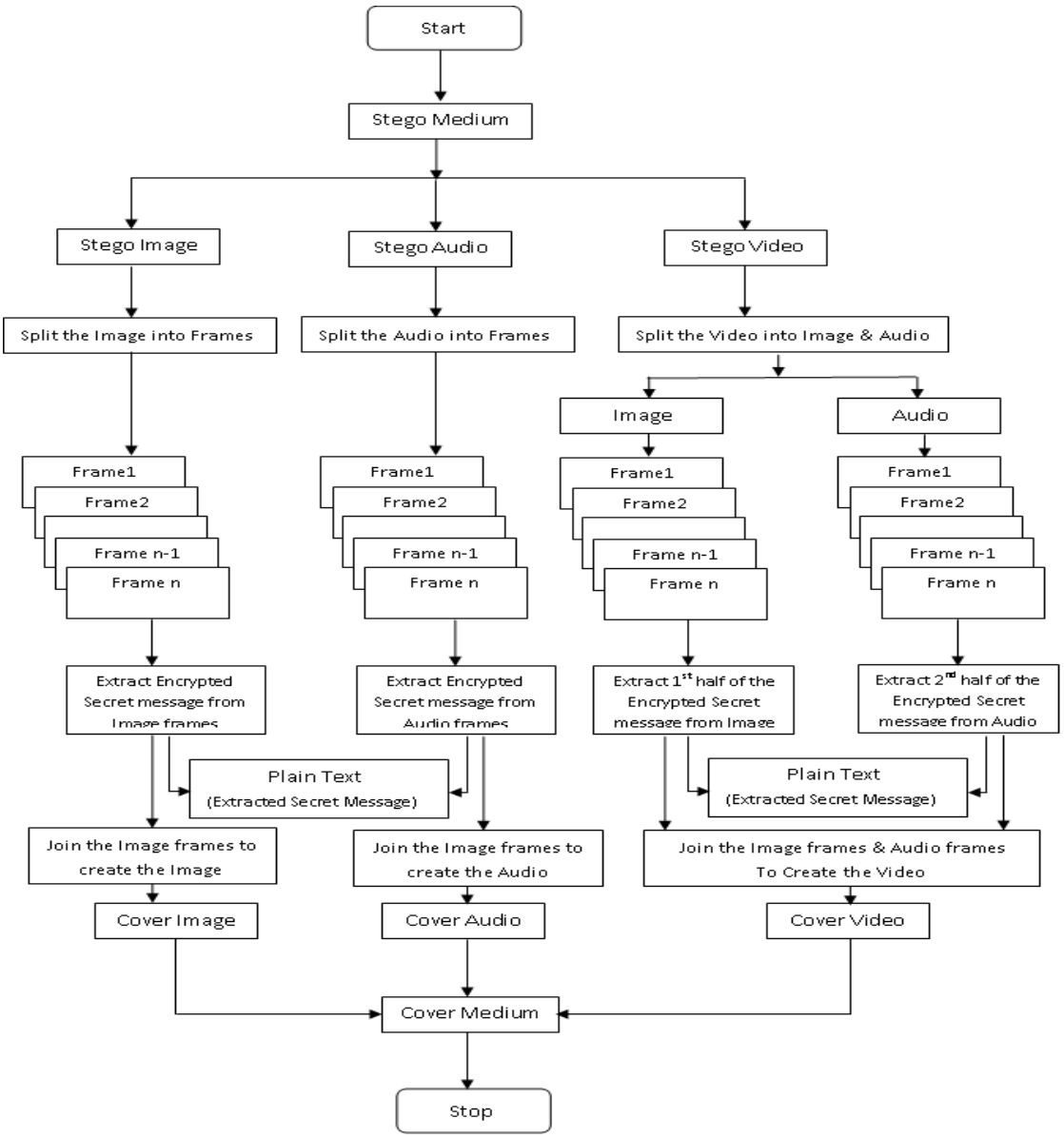


Figure 4: Steganographic System at Receiver side

5. METHODOLOGY

Least significant bit [10, 11]] substitution is the simplest way to embed information in a digital multimedia file. LSB substitution allows for a large amount of data to be encoded. In this paper the encrypted message is embedded into multimedia file and extracted encrypted message from multimedia file. During embedding and extraction process the content of the message is not to be damaged, if any damage occurs problem may arise during decryption process at receiver side.

5.1 Embedding and Extracting

First select a multimedia file and load it into steganographic system. The cover multimedia file is then broken down into frames. Now the least significant technique has been applied to conceal the data in the carrier frames. The proposed technique takes bits of secret data and conceals them in LSB of RGB pixel value of the carrier frames. The process will run until the entire text message will be inserted into multimedia file as shown in Figure 3, Figure 4 shows the extracting procedure at receiver side.

Algorithm for Embedding Secret message in Multimedia file:

Step-1: Input cover Multimedia file, Secret message and Shared Secret key.

Step-2: Break the Multimedia file into frames.

Step-3: Convert the secret message into cipher text by using secrete key shared by sender and receiver.

Step-4: Find Least Significant Bits of each RGB pixels of the cover frame.

Step-5: Convert the encrypted text message into bits.

Step-6: Embed the bits of the secret message into bits of LSB of RGB pixels of the cover frame.

Step-7: Continue the process until the message fully embedded into multimedia file.

Step-8: Regenerate Multimedia file frames.

Algorithm for Extracting Secret message from Multimedia file:

Step-1: Input stego Multimedia file.

Step-2: Break the stego Multimedia file into frames.

Step-3: Find and retrieve the LSB bits of each RGB pixels of the stego frame.

Step-4: Continue the process until the message fully extracted from multimedia file.

Step-5: using shared key decrypt message to get original data.

Step-6: Reconstruct the secret information.

Step-7: Regenerate Multimedia file frame.

6. EXPERIMENTAL WORK & RESULTS

This section presents and discusses the experimental work and results. In this section, here we are going to implement steganography technique on the following images and video files. The images and video files tested in the present experiment are displayed. The cover image is shown in Figure 5 and the resulting stego image is shown in Figure 7. The Figure 9 shows the cover video and Figure 11 shows the stego video.

6.1 Histogram

An histogram is a bar chart that shows the distribution of data values. The histograms are evaluated using MATLAB. The Figure 6 and Figure 8 are the histograms of cover image "Leena_Cover.bmp" and stego image "Leena_Stego.bmp". The Figure 10, Figure 12 shows the evaluated histograms of the cover video "Vipmen_Cover.avi" and stego video "Vipmen_Stego.avi".

Leena_Cover.bmp
Figure 5: Cover Image

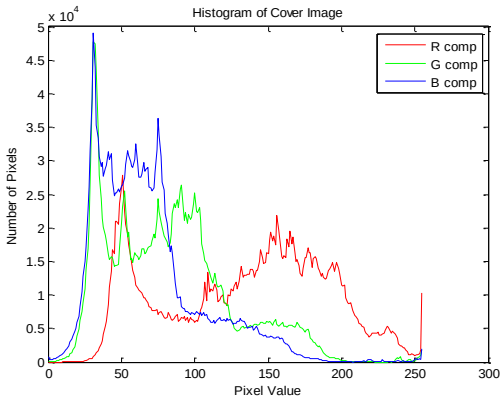


Figure 6: Histogram of Cover Image

Leena_Stego.bmp
Figure 7: Stego Image

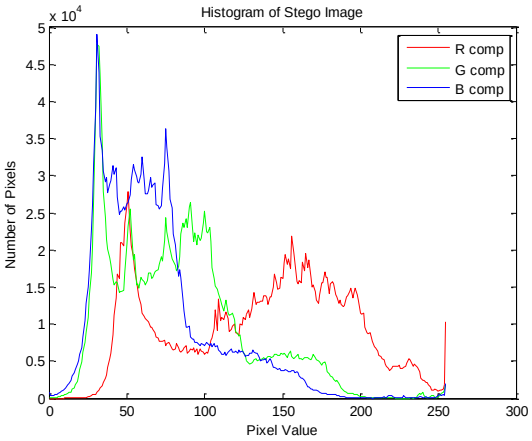


Figure 8: Histogram of Stego Image

Figure 9: Cover Video file

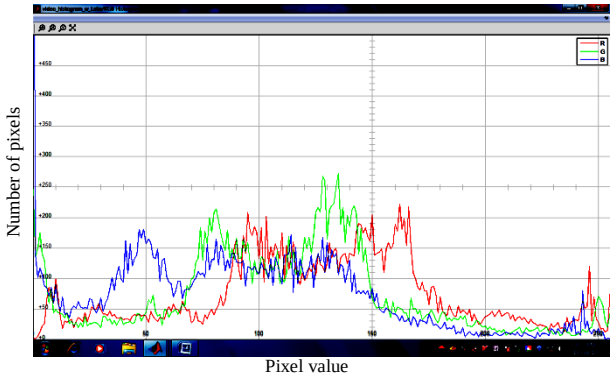


Figure 10: Histogram of Cover Video file

Figure 11: Stego Video file

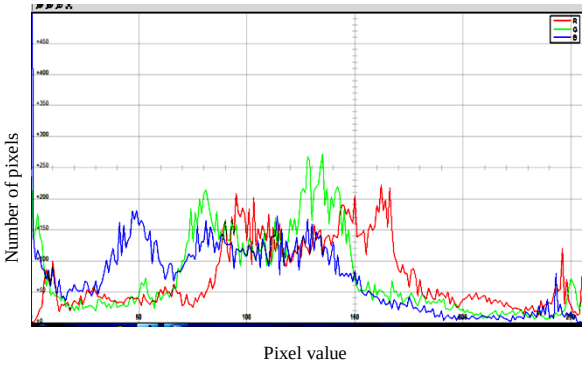


Figure 12: Histogram of Stego Video file

7. CONCLUSION

In this paper an idea to enhance the security of system by combining the cryptography and steganography is given, which provides a secure communication between two parties. The proposed system finds a way to embed secret information in Multimedia file without changing its quality. The encrypted text message is to get the advantage of cryptography. The proposed system embeds the text in multimedia file successfully and retrieves text from stego medium. In this paper the text is encrypted by using available DES encryption algorithm before embedding and at the receiver side text will be decrypted. This paper explores a tiny fraction of the art of steganography. Future scope of the paper is to increase capacity of embedding secret message in the carrier as well as secrecy of the message.

8. REFERENCES

[1] Soum.yendu Das, Bijoy Bandyopadhyay and sugata sanyal, "Steganography and steganalysis: Different Approaches", an article.

[2] Data Hiding in Images Part 1- Fundamental Issues and Solutions, IEEE Transaction on Image Processing, Vol.12, No.6, June 2003.p.p 685-695.

[3] W.Bender, W.Butera, D.Gruhl, F.J.Paiz, S.Pogreb, "Techniques for data hiding", IBM Systems Journal, vol. 39, Issue 3-4, July 2000, pp 547-568.

[4] Pramatha Nath Basu and Tanmay Bhowmik, "On Embedding of Text in Audio-A case of Steganography", International Conference on Recent Trends in Information, Telecommunication and Computing. 2010.p.p 203-206.

[5] Jayaram p, Ranganatha H R, Anupama H S, "Information Hiding using Audio Steganography- A Survey", The International Journal of Multimedia & Its Applications(IJMA), Vol. 03, No. 03, August 2011, p.p 86-96.

[6] Aravind Kumar, Km. Pooja, "International Journal of Computer Applications", Vol.9, No.7, November 2010, p.p 19-23.

[7] Steganographic Techniques and their use in an Open-Systems Environment- Bret Dunbar, The information Security reading Room, SANS Institute.

[8] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001.

[9] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami

Das, "A Tutorial Review on Steganography", International Conference on Comtemporary Computing (IC3'09), June 2009, p.p 105-114.

[10] Kousik Dasgupta, J.K. Mandal, Paramartha Dutta, "Hash Based Least Significant Bit Technique for Video Steganography (HSLB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 01,No 02,April 2012, p.p 1-11.

[11] Asoke Nath, Sankar Das and Amlan Chakrabarthi, " Data Hiding and Retrieval", IEEE International conference on Computational Intelligence and Communication Networks,26-28, Nov 2010 , p.p. 392-397.

[12] K.Geetha and P.Vanitha Muthu, "Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy" International Journal on Computer Science and Engineering Vol.02, No. 04, 2010,p.p 1308-1313.

AUTHOR'S PROFILE

V. Lokeswara Reddy did his M.Tech (CSE) from SRM University, Chennai in the year 2005. He did his M.C.A from S.V. University, Tirupati in the year 2000. He is pursuing his Ph.D from JNTUA, Anantapur. He has a total of 11 years of experience in teaching. Currently he is working as Associate Professor at K.S.R.M College of Engineering, Kadapa. He has presented 5 papers in International, Nationa Conferences and published 3 papers in International journals.

Dr.A.Subramanyam received his Ph.D. degree in Computer Science and Engineering from JNTU College of Engineering, Anantapur. He has obtained his B.E.(ECE) from University of Madras and M.Tech.(CSE) from Visweswaraiah Technological University. He is having 19 Years experience in teaching. He is currently working as Professor & HOD in the Department of Computer Science and Engineering of Annamacharya Institute of Technology & Sciences, Rajampet, Y.S.R. Dist. A.P. He has presented and published number of papers in International and National Conferences, International and National Journals. He is guiding few Ph.D.s. His research areas of interest are parallel processing, network security and data warehousing.

Dr. P. Chenna Reddy did his B.Tech (CSE) from S.V. University College of Engineering, Tirupati in the year 1996. He did his M.Tech from JNTU, Anantapur. He completed his Ph.D from JNTU, Hyderabad. He has a total of 15 years of experience in teaching. Currently he is working as Professor at JNTUA College of Engineering, Pulivendula, Y.S.R. Dist., A.P. He has number of publications to his credit.