Advanced Steganography using Image, Audio and Video as a Cover Media

Mr.Kiran N Somwanshi
Institute of Engineering &Technology
Alwar, Rajasthan.
kn.somwanshi@gmail.com

Prof.Vedant Rastogi
Institute of Engineering &Technology
Alwar, Rajasthan.
vedantnoki@gmail.com

***Abstract*— with the recent surge and rapid growth in digital data usage and transfer in many real life applications, there is a question of new and effective ways to ensure their security. Efficient secrecy can be achieved by using the steganography mechanism. In this system, we have developed steganographic techniques for embedding text data in image, audio and video file. The basic approach behind this system is to provide a good, well-organized method for hiding the data and sent to the destination using secured media in safer manner. Our method is secure in the way that even if the attacker detects and extracts the embedded message from the stego medium (image/audio/video), one would not be able to recover the secret message without the encoded key. The system is also provided with the facility of compression. We have used the efficient technique such as DCT to retain the image quality and file size in image and video steganography. In case of audio steganography, using the method of embedding text in the 4th and 5th layer with same data and different data, data becomes more secure and transparency is minimized. Also, embedding the text file in a video file is done in such a way that the video does not lose its functionality using DCT & LSB Modification method. The proposed video algorithms strive for high security to an eavesdropper's inability to detect hidden information.**

Keywords*— *Steganography, Data Hiding, Image, Audio, Video

I. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message is clear, but the meaning is obscured. Steganography literally means "covered writing" and is the art of hiding the very existence of a message.In today's digital world, invisible ink and paper have been replaced by much more versatile and practical covers for hiding messages – digital documents, images, video, and audio files. As long as an electronic document contains perceptually irrelevant or redundant information, it can be used as a "cover" for hiding secret messages. The possible cover carriers are innocent looking carriers (images, audio, video, text, or some other digitally representative code) which will hold the hidden information. A message is the information to be hidden and it may be plaintext, cipher text, images, or anything that can be embedded into a bit stream. Together the cover carrier and the embedded message create a stego-carrier. Hiding information may require a stego key which is additional secret information, such as a password, required for embedding the information. For example, when a secret message is hidden within a cover image, the resulting product is a stego-image. The basic block diagram representation for steganography mechanism is shown in the below figure.

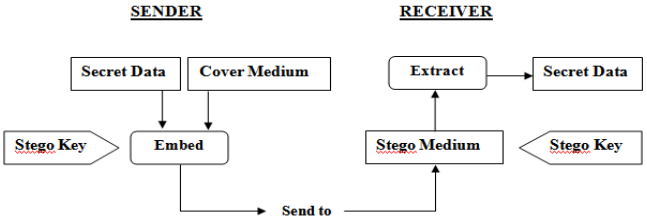


Fig. 1: Steganography Mechanism

The above figure shows a simple representation of the generic embedding and extraction process in steganography. In this example, a secret data is being embedded inside a cover image to produce the stego image/audio/video. A key is often needed in the embedding process. The embedding procedure is done by the sender by using the proper stego key. The recipient can extract the stego cover medium in order to view the secret data by using the same key used by the sender. The stego medium should look almost identical to the cover medium.

The following formula provides a very generic description of the pieces of the steganographic process.

Cover medium + hidden data + stego_key = stego_medium.
Cover medium= is the file in which we will hide the hidden data.
Hidden data=is the secrete data file.
Stego key = is the shared secrete key known to intended recipients
stego_medium=is the resultant file obtained after embedding process.

In proposed work the focus is on image, audio and video file. We are making use of the cover medium and stego_medium & so on. Cover image may be.bmp or.jpeg file, audio, video file. hidden data must be text (.txt) file, stego_key may be text or number and resultant stego_medium can be image/audio/video file as per the respective cover medium. Here we present an algorithm for embedding file in cover medium robust to compression and extracting them efficiently.

Let us see the basics of image, audio and video steganography

1. Image Steganography
   Embedding secret message into images (cover object) is known as image steganography
2. Audio Steganography
   Embedding secret messages into digital sound is known as audio Steganography. It is usually a more difficult process than embedding messages in other media. Audio Steganography methods can embed messages in WAV, AU, and even MP3 sound files.
3. Video Steganography
   Embedding secret message into image and audio or frames is known as video steganography.

II. MOTIVATION

In today's world, the communication is the basic necessity of every growing area. Everyone wants the secrecy and safety of their communicating data. In our daily life, we use many secure pathways like internet or telephone for transferring and sharing information, but it's not safe at a certain level. In order to achieve secure data transmission we used the effective steganographic covers (image, audio and video) to hide the secret data.

III. OBJECTIVES

1) Imperceptibility: The cover data and original data source should be perceptually identical.
2) Robustness: The embedded data should survive any processing operation the host signal goes through and preserve its fidelity.
3) Capacity: To Maximize data embedding payload.
4) Security: Security is in the key for embedding or encryption of data.
5) Privacy: User can achieve privacy while doing data transmission.

IV. DETAIL PROBLEM DEFINITION

The system works in two modules:
1. To hide the secret message the process of embedding is performed on the secret message.
2. To get the secret message from the stego medium (image/audio/video) the extraction algorithm is executed

-- Embedding Algorithm

1. Input : Secret Message and Cover Medium (image/audio/video)
2. Output : Stego Medium(image/audio/video)

-- Extraction Algorithm

1. Input : Stego Medium(image/audio/video)
2. Output : Secret/Confidential Message

-- System Input:

It includes following parameters of embedding phase …

1. Cover medium(image/audio/video)
2. Embedded medium that will be created
3. Shared secret password(text or number or combination of both)
4. Quality factor Q of cover medium(one out of integers provided)
5. Actual secrete data (text or image)to be embedded(any formats)

-- System Output:

It includes following parameters of extraction phase

1. Embedded medium that will be created
2. Shared secret password(text or number or combination of both)
3. Extracted message file that will be created (contains secrete data).

V. NEED OF THE PROPOSED SYSTEM

An effective image, audio and video steganography is needed to provide a good and efficient way for hiding the data from hackers and sent to the destination in a safe manner. The proposed system will not change the size of the file even after encoding and also suitable for any type of file format.

VI. APPLICATIONS

In the business world, audio data hiding, video data hiding and text data hiding can be used as a secret chemical formula or plans for a new invention. Audio data hiding can also be used incorporate world. Terrorists can also use audio data hiding to keep their communications secret and to co-ordinate attacks.

Data hiding in video and audio is of interest for the protection of copyrighted digital media and to the government for information system security and for covert communication. It can also be used in forensic application for inserting hidden data in to audio files for the authentication of spoken words and other sounds and in the music business for the monitoring of the songs over broadcast radio.

Image hiding is to secure in the way that even if the attacker detects (i.e., statistical attacks) and extracts the embedded message from the stego-image, he/she would not be able to recover the secret message without the encoded key.

So, the key areas for the use of steganography are:

- Confidential Communication and Secret Data Storing
- Protection of Data Alteration
- Access Control System for Digital Content Distribution
- E-Commerce
- Media
- Database Systems
- Digital watermarking

VII. STUDY OF EXISTING TECHNIQUES

Title	Drawbacks	Description
Image : 1. LSB [1], [2], [3]	Intruder can easily guess and change the LSB's of the image pixels, thus original message gets destroyed.	Message is hidden in the least significant bits of image pixels
2. Parity checker method [4]	In some situations when odd or even parity not present, then it can be made by both +1 or -1. So, it creates confusion, which one to choose.	In this, concept of even and odd parity is used.
Audio :		

1. Echo hiding **[**12**]**, [13]	Low security and capacity	Embeds secret information in a sound file by introducing an echo into the discrete signal.
2. Spread Spectrum[11]	Vulnerable to time scale modification	The basic spread spectrum (SS) method attempts to spread secret information across the frequency spectrum of the audio signal.
Video : "Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error" [16]	May lead to quality distortion	Deals with data hiding in compressed video

Table 1: Analysis of existing systems

A. Comparison of Existing System with proposed:

In Existing systems there are chances of poor stego medium (image/audio/video) quality, whereas the proposed system has good stego medium quality. As compare to existing vulnerable techniques, our work is secure in the way that even if the attacker detects (i.e., statistical attacks) and extracts the embedded message from the stego-medium, he/she would not be able to recover the secret message without the encoded key. The message bits are embedded randomly into the cover image pixels instead of sequentially (existing).

Finally, we have shown that steganography that uses a key has a better security than existing non-key steganography. This is so because without the knowledge of the valid key, it is difficult for a third party or malicious people to recover the embedded message.

This system will not change the size of the file even after encoding and also suitable for any type of file format. Encryption and decryption techniques have been used to make the system security robust.

VIII.SYSTEM SCOPE

Steganography is necessary for the protection of copyright. Currently, hundreds of thousands of images, audio and video are being distributed on the internet without any proper protection against piracy. Due to the lack of security online many of the pictures & visual artworks were discourage from being circulated on the internet, Digital image ,Steganographic image is out there to change all that & allow for a more safe online experience. Steganography will clear up ambiguities that occur during other ship copyright-related confrontations & so forth.

The scope of the system includes following aspects.

1) The steganographic medium (image/audio/video) should remain as closely as possible to the quality of the original medium.
2) The embedded data recovery process should be able to prove to such a high degree of certainty that if the image/audio/video is steganographic then the extracted data is matching only with the original data and not with any other randomly generated data.

IX. SYSTEM DESIGN

A. System Architecture:

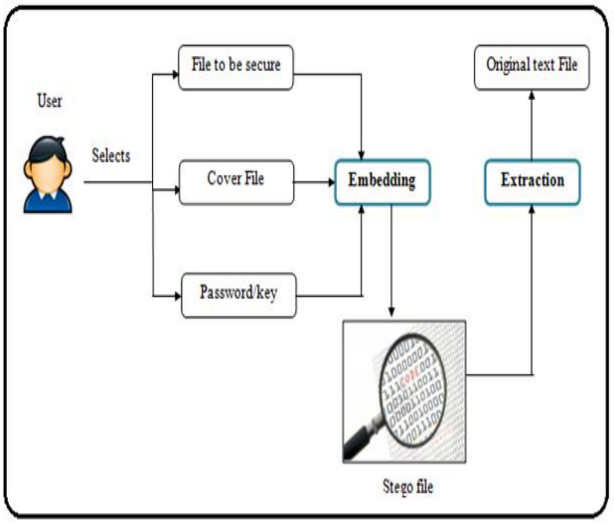


Fig.3. System Architecture

B.Methodology

There are two phases in which system works

Phase 1: Embedding

Data embedding is the process of embedding information in a data source without changing its perceptual quality. It includes following steps.

1. Select the message file to be kept secret.
2. Using respective embedding algorithm(image/audio/video) and key hide secret file in cover medium
3. Get the stego image/audio/video

Data embedding requirements include the following: 1) Imperceptibility: The video with data and original data source should be perceptually identical. 2) Robustness: The embedded data should survive any processing operation the host signal goes through and preserve its fidelity. 3) Capacity: Maximize data embedding payload. 4) Security: Security is in the key for embedding or encryption of data.

Phase 2: Extraction

Extraction is the process of extracting a secrete message from stego image using password. It includes following steps.

4. Take the embedded (stego) image/audio/video.
5. Accept the shared secret password
6. Using password as stego_key apply respective decoding algorithm(image/audio/video) to stego medium
7. Get the original text message file.

C.Algorithm

**** ALGORITHM 1:** For image as a cover/carrier file

-- Embedding Algorithm

Input: secret file, cover image file
Procedure:
Start
Step 1: Encode the message using the T-Codes
Step 2: Divide the cover image into 8x8 Blocks
Step 3: Calculate DCT coefficients for each block
Step 4: Quantize the coefficients
Step 5: while complete message not embedded
Do
Step 5.1 get next DCT coefficient
Step 5.2 if DCT 0, DCT 1 and DCT = -1 then
Step 5.2.1 get next bit from Message
Step 5.2.2 replaces DCT LSB with message bit
End {if}
End While}
Step 6: De-quantize and take inverse DCT to obtain the stego-image
End
Output: Stego- image

-- Extracting algorithm

Input: Stego image
Procedure:
Start
Step 1: Divide the stego image into 8x8 blocks
Step 2: Calculate DCT coefficients for each block
Step 3: Quantize the coefficients
Step 4: while secret message not completed
Do
Step 4.1 get next DCT coefficient
Step 4.2 if DCT 0, DCT l and DCT = -1 then
Concatenate DCT LSB to secret message
End {if}
End {while}
Step 5: Decode secret message bits using the T-codes
End
Output: Extracted secret file

Description of an algorithm:

Jpeg – Jsteg image which embeds secret message into LSB (Least Significant Bit) of the quantized DCT (Discrete Cosine Transform) coefficients. Only few messages can be embedded in the cover image.

Steganographic system that change LSBs (Least Significant Bits) sequentially cause distortion detectable by steg-analysis methods. The embedding of high entropy data changed the histogram of color frequencies in a predictable way. The secret message can be embedded in the middle frequency part of the quantized DCT coefficients. Another method is to embed message bits using a pseudo random number generator to select DCT (Discrete Cosine Transform) coefficients at random. This is done in the first pass. After embedding, the image is processed again using a second pass. Corrections are made to the coefficients to make the stego - image histogram matches the cover image histogram.

T-CODES

We know that the best Variable-Length Codes (VLC) are the Huffman codes. They are easy to construct for optimum efficiency if source statistics are known. But if they are used in serial communication, a loss of synchronization often results in a complex resynchronization process whose length and outcome are difficult to predict T –codes provide the solution to this problem. T-codes are families of variable-length codes (VLC) that BVICAM'S International Journal of Information Technology exhibit extraordinarily strong tendency towards self -synchronization. The concept of simple T-codes proposed a novel recursive construction of
T -codes known as the Generalized T -codes that retain the properties of self-synchronization. In situation where code word synchronization is important, the T -codes can be used instead of Huffman codes, giving excellent self-synchronizing properties without sacrificing coding efficiency.

The main advantage of the T -Code is that they are self-synchronizing, so if some bits are lost or modified in a T-code encoded stream, the decoder will regain synchronization automatically. The best T-codes achieve self-synchronization within l.5 characters following a lock loss. Thus, we can use T -codes in place of Huffman codes in the algorithms such as Jpeg-Jsteg. The advantage of this approach is the ability to send steganographic messages in lossy environment that are robust against detection or attack.

Using of T-codes as source encoding in place of Huffman codes result into better PSNR values. In this paper we propose T -codes for the encoding of original message and for the entropy encoding of compressed stego-image in place of Huffman codes. The proposed scheme takes advantage of the synchronizing ability of T-codes to increase the robustness of popularly. Following figures shows the difference between the cover image/test image and stego image after applying an embedding algorithm.

Fig.4 Test Image

Fig.5 Stego Image

**** ALGORITHM 2:** For audio as a cover/carrier file

-- Embedding Algorithm

Input: secret file, cover audio file
Procedure:
Start
Step1: Select the audio file for embedding the secret message.

Step2: Play the audio file so that it sounds clear to the end user.

Step3: Select the text file containing the secret message.

Step4: Encrypt the text file contents.

Step5: Compare text file and audio file size.

If text file size > audio file contents then

Error message displayed indicating cannot embed secret message.

Else

Embed secret message in the audio file in the 4th and 5th LSB bit of every sample.
Step6: Display message to user of the new audio file created after embedding secret message.
End
Output: Stego audio

-- Extracting algorithm

Input: Stego audio
Procedure:
Start
Step 1: Select the new audio file for extracting the secret message.

Step 2: Extract the secret message from the audio file from the 4th and 5th LSB bit of every sample.
Step 3: If secret message present in audio file Then

Display message to end user after extracting message.

Else

Display that no hidden data is present in the text.

Step 4: Decrypt the secret message.

Step 5: Display message to end user after decrypting the message.
End
Output: Extracted Secret file

Description of an algorithm:

Least Significant Bit (LSB) coding method is the simplest way to embed secret information in a digital audio file by replacing the least significant bit of audio file with a binary message. Hence LSB method allows large amount of secret information to be encoded in an audio file. Algorithm shows the complete working of the audio stegnography process of embedding the encrypted secret message using public key cryptographic algorithm, RSA into the 4th and 5th layers of the audio file. In the sender side, the text file which has to be embedded into an audio file is encrypted using public key cryptographic algorithm, RSA. The cipher text obtained is then embedded in the 4th AND 5th LSB bit using one of the Steganographic algorithms, LSB algorithm. The resultant audio file contains the secret message embedded into it. On the receiver side, the embedded audio file is selected to extract the secret message. The secret message is decrypted using RSA decryption method and the secret messages are compared before embedding and after embedding. Also, comparisons are made based on PSNR of both original audio file and embedded audio file, to indicate that less noise intrusion even after changing the 4th and 5th LSB bit of the original wave.

**** ALGORITHM 3:** For video as a cover/carrier file

There are two algorithms :

-- DCT Algorithm

1. Algorithm to embed text message:

Input: secret file
Procedure:
Start
Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8×8 block of pixels.
Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.
Step 8: Write stego image.
End
Output: Stego Image

2. Algorithm to retrieve text message:

Input: Stego Image
Procedure
Start
Step 1: Read stego image.
Step 2: Stego image is broken into 8×8 block of pixels.
Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is applied to each block.
Step 5: Each block is compressed through quantization table.
Step 6: Calculate LSB of each DC coefficient.
Step 7: Retrieve and convert each 8 bit into character.
End
Output: Text Message

-- LSB Algorithm

1. **Algorithm to embed text message:**
   Input: Cover image and text message
   Procedure:
   Start
   Step 1: Read the cover image and text message which is to be hidden in the cover image. **Step 2:** Convert text message in binary.
   Step 3: Calculate LSB of each pixels of cover image.
   Step 4: Replace LSB of cover image with each bit of secret message one by one.
   Step 5: Write stego image
   End
   Output: Stego Image

2. **Algorithm to retrieve text message:**
   Input: Stego image
   Procedure:
   Start
   Step 1: Read the stego image.
   Step 2: Calculate LSB of each pixels of stego image.
   Step 3: Retrieve bits and convert each 8 bit into character
   End
   Output: Text Message

Description DCT and LSB:

1. **Discrete Cosine Transform (DCT):**

DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

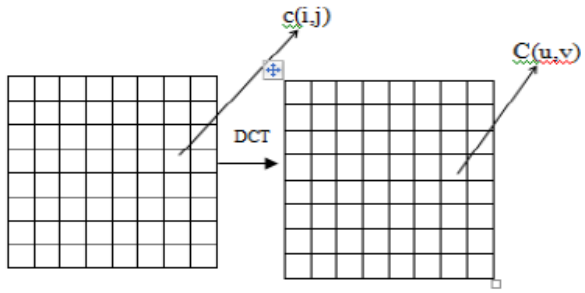


Fig.6: Discrete Cosine Transform of an Image

The general equation for a 1D (N data items) DCT is defined by the following equation:

$$C(u) = \alpha(u)\sum_{x=0}^{N-1} f(x)\cos\left[\frac{(2x+1)u\pi}{2N}\right]$$

for u = 0, 1, 2, . . . , N-1.

***** Formula 1: Equation for 1D DCT*

The general equation for a 2D (N by M image) DCT is defined by the following equation:

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (2)$$

For u,v = 0, 1, 2, . . . , N-1

***** Formula 2: Equation for 2D DCT*

Here, the input image is of size N X M. c(i, j) is the intensity of the pixel in row i and column j; C(u,v) is the DCT coefficient in row u and column v of the DCT matrix. Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT. Compression can be achieved since the lower right values represent higher frequencies, and generally small enough to be neglected with little visible distortion. DCT is used in steganography as: Image is broken into 8×8 blocks of pixels. Working from left to right, top to bottom, the DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

2. **Least Significant Bit (LSB):**

LSB is the lowest bit in a series of numbers in binary. E.g. in the binary number: 10110001, the least significant bit is far right. The LSB based Steganography is one of the steganographic methods, used to embed the secret data in to the least significant bits of the pixel values in a cover image. e.g. 240 can be hidden in the first eight bytes of three pixels in a 24 bit image.

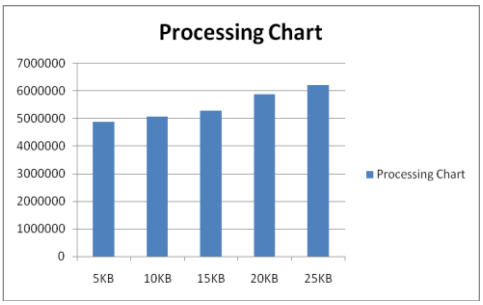
PIXELS: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
240: 011110000
RESULT: (00100110 11101001 11001001)
(00100111 11001001 11101000)
(11001000 00100110 11101000)

Here number 240 is embedded into first eight bytes of the grid and only 6 bits are changed.

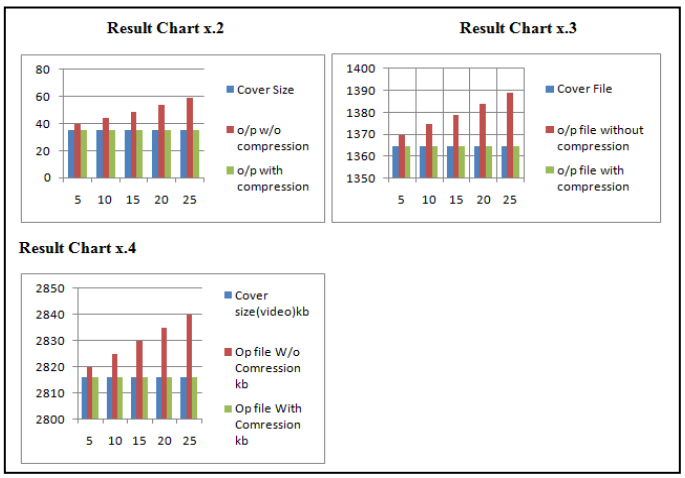
X .Result & Discussion

This proposed system which supports the image, audio and video (as a carrier file) to provide a good efficient method for hiding the data from hackers and sent to the destination in a safe manner. In this system main important factor is that time required to hide the data are very crucial .when the secret data size are more it take more time(microsecond) to embed it. Also when we hide the data file into cover file then resultant steno file with compression & without compression get increased according size of secret data file.

(1)

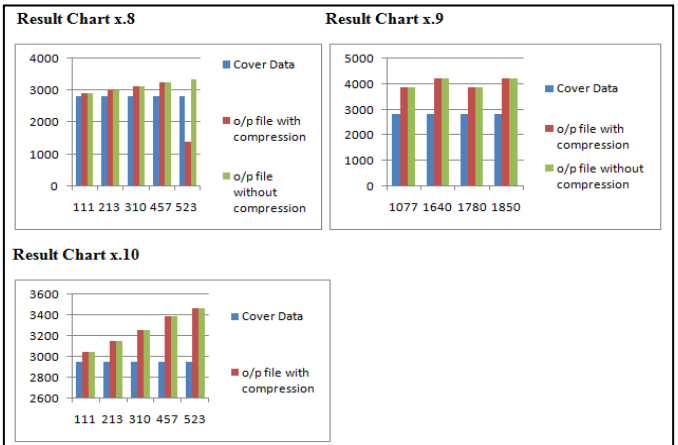


Above fig. shows the processing chart. It shows the time required to cover or hide the data under image.



In above representation, Result Chart x.2 shows that text data is covered under the image whereas, Result Chart x.3 and Result Chart x.4 shows that text data is covered under the audio and video respectively. X and Y axis represents file size in kb.

Result Chart x.5, Result Chart x.6, Result Chart x.7 represents the covering of the image file under the image, audio and video file respectively. X and Y axis represents file size in kb.



As per the above discussion, same methodology is applicable for video and audio file covering or hiding. It is represented in the Result Chart x.8 represents audio covered under video, Result Chart x.9 represents video covered under video and Result Chart x.10 represents audio covered under audio. X and Y axis represents file size in kb.

It is the best way to achieve the security for huge data efficiently.

XI. CONCLUSION

We proposed a system which supports the image, audio and video (as a carrier file) to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. We observe that PSNR values of the proposed Jpeg-Jsteg algorithm based on T-codes for the different images are almost same as that of original algorithm based on Huffman codes, i.e., there is no change in the stego-image quality. Our method is secure in the way that even if the attacker detects and extracts the embedded message from the stego-image, one would not be able to recover the secret message without the encoded key. Moreover due to the inherent property of self-synchronizing of T -codes, our method is more robust as after the extraction process the recovered secret message is decoded and found to be without being much destroyed. Steganography can be used for hidden communication. We pointed out the enhancement of the image steganographic system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover-image. In our proposed approach, the message bits are embedded randomly into the cover-image pixels instead of sequentially. Finally, we have shown that steganography that uses a key has a better security than non-key steganography. This is so because without the knowledge of the valid key, it is difficult for a third party or malicious people to recover the embedded message. In further research our focus will be on using an efficient, reliable and secure techniques for embedding other media such as image, audio and video inside a cover medium.

REFERENCES

[1] Adel Almohammad "Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility" A thesis submitted for the

degree of Doctor of Philosophy, Department of Information Systems and Computing , Brunel University, August,2010.

[2] Neil F Johnson, Sushil Jajodia, "Exploring Stenography: Seeing the Unseen", IEEE Computer, Feb 1998, pp 26-34.

[3] Rajkumar Yadav "Analysis of Incremental Growth in Image Steganography Techniques for Various Parameters" Int. J. Comp. Tech. Appl., Vol 2 (6),1867-1870, NOV-DEC 2011.

[4] Rajkumar , Rahul Rishi , Sudhir Batra " A New Steganography Method for Gray Level Images using Parity Checker" International Journal of Computer Applications (0975 – 8887) Volume 11– No.11, December 2010.

[5] Ahmad T. Al-Taani and Abdullah M. AL-Issa "A Novel Steganographic Method for Gray- Level Images" International Journal of Computer and Information Engineering 3:1 2009.

[6] Chung-Ming Wang , Nan-I Wu , Chwei-Shyong Tsai , Min-Shiang Hwang, "A high quality steganographic method with pixel-value differencing and modulus function" J. Syst. Software (2007), doi:10.1016/j.jss.2007.01.049.

[7] G.Rupesh Kumar "Steganography", Seminar Report, Balaji Institute of technology and Sciences, Deptt. of Computer Science and Engg. Narsampet, Warangal, March 2011.

[8] Jayaram P, Ranganatha H R, Anupama H S "INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.

[9] Nedeljko Cvejic, Tapio Seppben "Increasing the capacity of LSB-based audio steganography " FIN-90014 University of Oulu, Finland ,2002.

[10] Yin-cheng qi, liang ye, chong liu "Wavelet domain audio steganalysis for multiplicative embedding model" Proceedings of the 2009 International Conference on Wavelet Analysis and Pattern Recognition, Baoding, 12-15 July 2009.

[11] Mengyu Qiao, Andrew H. Sung , Qingzhong Liu "Feature Mining and Intelligent Computing for MP3 Steganalysis" International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing 2009.

[12] Sajad Shirali-Shahreza M.T. Manzuri-Shalmani "High capacity error free wavelet domain speech steganography" ICASSP 2008

[13] V. Vapnik, "Statistical Learning Theory", John Wiley, 2008.

[14] Mozo AJ., and Obien M.E., C.J. Rigor, "Video Steganography using Flash Video (FLV)" I2MTC 2009 - International Instrumentation and Measurement Technology Conference Singapore, 5-7 May 2009.

[15] Qin c., Ying-Hsuan Huang, "An Inpainting-Assisted Reversible Steganographic Scheme Using a Histogram Shifting Mechanism" IEEE transactions on circuits and systems for video technology, vol. 23, no. 7, July 2013.

[16] Hussein A. Aly ", Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error" IEEE transactions on information forensics and security, vol. 6, no. 1, march 2011.

[17] Bodhak V. and Gunjal L., "Improved protection in video Steganography using DCT & LSB" international journal of engineering and innovative technology (IJEIT) vol. 1, issue 4, April 2012.

[18] Tasdemir K. and Kurugollu F., "Video steganalysis of LSB based motion vector steganography" International Conference on Communication Systems and Network Technologies 2010.

[19] Sunil. K. Moon, "Analysis of secured video Steganography using computer forensics techniques for enhances data security" IEEE second international conference on image information processing (ICIIP-2013).