iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Information Security through Steganography Technique

Vijay Prakash[1], Aakash Gupta[2]
[1,2] Department of Computer Science, Gateway Institute of Engineering & Technology (GIET), Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat

Abstract: ***The encrypted messages will often attract the concentration of unauthorized users. They try to crack the encrypted message and get access to the actual contents of the message. To conceal the subsistence of message steganography is introduced by hiding a secret message inside another credulous message. Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. Since nobody except the sender and the receiver knows the existence of the message, it does not attract unwanted attention. There are different methods for steganography such as text, image, audio & video. Out of above methods, image steganography is most popular due to vast amount of images on the Internet. There are different techniques for hiding information in cover object. One of the oldest & popular methods is least significant digit method. It hides data in the lowest bit of any image. In this paper we use different medium for hiding secret information using LSB technique.***

Keywords: ***Steganography, Steganalysis, DCT, LSB***

I. INTRODUCTION

Cryptography and steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence. These two techniques share the common goals and services of protecting the confidentiality, integrity and availability of information from unauthorized access. Cryptography is the process of changing information which are need to be transferred on insure transmission medium (e.g., Internet) so that no one except sender or receiver can understand the meaning of information. The cryptographic technique uses various types of algorithms which are generally impossible for unauthorized users to break. Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. Since nobody except the sender and the receiver knows the existence of the message, it does not attract unwanted attention.
This method of secret communication is also prevalent in ancient time where messages are written with some special ink etc. The modern Steganography uses different mediums for hiding secret information such as image, text, audio and video. Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content. By combining Steganography and Cryptography one can achieve better security [2]. Figure 1 below shows the one of mechanism of steganography for hiding secret information.

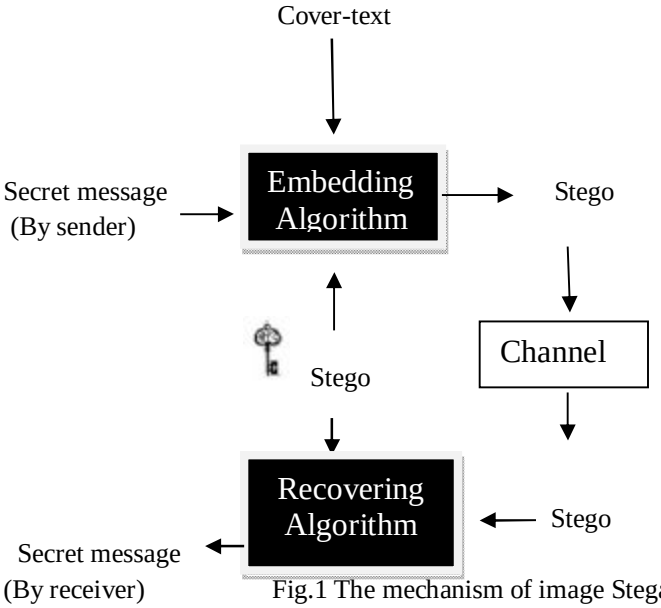


Fig.1 The mechanism of image Steganography

When a user detects the hidden information of steganography then it is referred as Steganalysis. Steganalysis is the process of extracting secret information by using multiple parameters of stego media. The first step for steganalysis is to find the stego image i.e., an image containing some secret data hidden in it. After that steganalysis process determines whether that media contains hidden message or not and then try to recover the message from it. With cryptanalysis, encrypted message is easily examined & conclude that message contains some secret information. But in the case of steganalysis this may not be true. The suspected media may or may not be with hidden data or information [3].

In this paper we provide steganography technique using all the three popular medium – image, audio and video. We also provide compression of stegano object.

II. TYPES OF STEGANOGRAPHY

Secrets can be hidden inside all sorts of cover information. The following formula provides a very generic description of the pieces of the steganographic process:

Cover_ medium + hidden_ data + stego_key
= stego_medium

In this context, the cover_medium is the file in which we will hide the hidden_data, which may also be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course be the same type of file as the cover_medium). There are four ways to implement steganography [4][5]:

A. Text Steganography

Text steganography can be classified in three basic categories - format-based, random and statistical generation and linguistic method. Format-based methods used physical text formatting of text as a place in which to hide information. Generally, this method modifies existing text in order to hide the steganographic text. Insertion of spaces, deliberate misspellings distributed throughout the text, resizing the fonts are some of the many format-based methods being used in text steganography. However, Bennett has stated that those format-based methods managed to trick most of the human eyes but it cannot trick once computer systems have been used. Random and statistical generation is generating cover text according to the statistical properties. This method is based on character sequences and words sequences.

The hiding of information within character sequences is embedding the information to be appeared in random sequence of characters. This sequence must appear to be random to anyone who intercepts the message. A second approach for character generation is to take the statistical properties of word-length and letter frequency in order to create “words” (without lexical value) which will appear to have the same statistical properties as actual words in a given language. The hiding of information within word sequences, the actual dictionary items can be used to encode one or more bits of information per word using a codebook of mappings between lexical items and bit sequences, or words themselves can encode the hidden information.

The final category is linguistic method which specifically considers the linguistic properties of generated and modified text, frequently uses linguistic structure as a place for hidden messages. In fact, steganographic data can be hidden within the syntactic structure itself. Example: Sender sends a series of integer number (Key) to the recipient with a prior agreement that the secret message is hidden within the respective position of subsequent words of the cover text. For example the series is „1, 1, 2, 3, 4, 2, 4“and the cover text is “A team of five men joined today”.

So the hidden message is “Atfvoa”. A “0” in the number series will indicate a blank space in the recovered message. The word in the received cover text will be skipped if the number of characters in that word is less than the respective number in the series (Key) which shall also be skipped during the process of message unhide.

B. Image Steganography

The most widely used technique today is hiding of secret messages into a digital image. This steganography technique exploits the weakness of the human visual system (HVS). HVS cannot detect the variation in luminance of color vectors at collection of color pixels. The individual pixels can be represented by their optical higher frequency side of the visual spectrum. A picture can be represented by a characteristics like 'brightness', 'chroma' etc. Each of these characteristics can be digitally expressed in terms of 1s and 0s. For example: a 24-bit bitmap will have 8 bits, representing each of the three color values (red, green, and blue) at each pixel. If we consider just the blue there will be 2 different values of blue. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Hence, if the terminal recipient of the data is nothing but human visual system (HVS) then the Least Significant Bit (LSB) can be used for something else other than color information [6].

1) *LSB Coding:* The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In this method, we can take the binary representation of the hidden_data and overwrite the LSB of each byte within the cover_image. If we are using 24-bit color, the amount of change will be minimal and indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

10010101	00001101	11001001
10010110	00001111	11001010
10011111	00010000	11001011

Now suppose we want to "hide" the following 9 bits of data : 101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in **bold** have been changed):

10010101	00001100	11001001
10010111	00001110	11001011
10011111	00010000	11001011

Note that we have successfully hidden 9 bits but at a cost of only changing 4, or roughly 50%, of the LSBs.

Fig.2 Original Image

Fig.3 Embedded Image

Left hand side image is the original cover image, whereas right hand side does embedding a text file into the cover image make the stego image. LSB is one of the most popular technique which is used for hiding the secret message. LSB hiding technique works as it hides the secret message directly in the least two significant bits in the image pixels, which affects the image resolution, due to this it reduces the image quality and make the image easy to attack. This method works quite well when both the host and secret images are given equal numbers of bits. When one has significantly more room than another, quality is sacrificed.

2) *Masking and Filtering:* Masking and filtering techniques are mostly used on 24 bit and grey scale images. They hide information in a way similar to watermarks on actual paper and are sometimes used as digital watermarks. Masking images entails changing the luminance of the masked area. The smaller the luminance change, the less of a chance that it can be detected. Masking is more robust than LSB insertion with respect to compression, cropping, and some image processing. Masking techniques embed information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the “noise” level. This makes it more suitable than LSB with, for instance, lossy JPEG images [7].

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

C. Audio Steganography

Steganography, in general, relies on the imperfection of the human auditory and visual systems. Audio steganography takes advantage of the psychoacoustical masking phenomenon of the human auditory system [HAS]. Psychoacoustical or auditory masking property renders a weak tone imperceptible in the presence of a strong tone in its temporal or spectral neighborhood. This property arises because of the low differential range of the HAS even though the dynamic range covers 80 dB below ambient level. Frequency masking occurs when human ear cannot perceive frequencies at lower power level if these frequencies are present in the vicinity of tone- or noise-like frequencies at higher level. Additionally, a weak pure tone is masked by wide-band noise if the tone occurs within a critical band. This property of inaudibility of weaker sounds is used in different ways for embedding information. Embedding of data by inserting inaudible tones in cover audio signal has been presented recently.

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file [8].

The list of methods that are commonly used for audio steganography are listed and discussed below.

1) *Parity Coding:* Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion.
2) *Phase coding:* Human Auditory System (HAS) can't recognize the phase change in audio signal as easy it can recognize noise in the signal. The phase coding method exploits this fact. This technique encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to- noise ratio.

D. Video Steganography

Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. When information is hidden inside video the program or person hiding the information will usually use the DCT (Discrete Cosine Transform) method. DCT works by slightly changing each of the images in the video, only so much that it is not noticeable by the human eye. To be more precise about how DCT works, DCT alters values of certain parts of the images, it usually rounds them up. For example, if part of an image has a value of 6.667 it will round it up to 7. 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. Therefore, any small but otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information.

III. IMPLEMENTATION

In our implementation work Steganography can be used to hide data using different mediums such as image, audio and video. The implementation is performed in Java programming language. The implementation is divided into two parts-embedding of secret data by the sender and then extraction of hidden data by the receiver.

Figure 3 below shows the embedding screen.

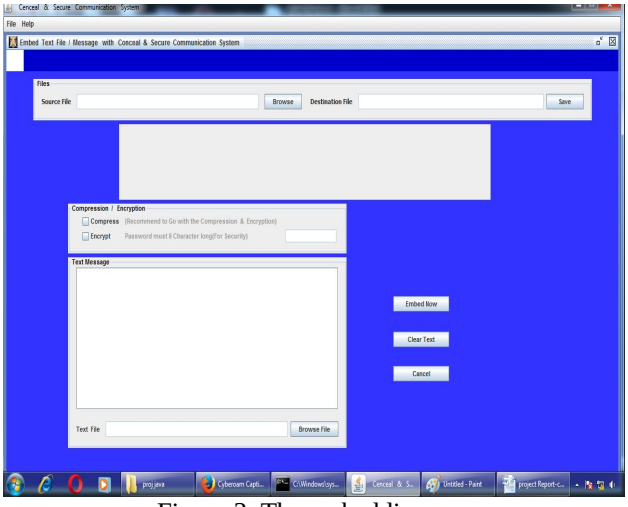


Figure 3: The embedding screen.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

User can select the steganography medium as source file, destination file and type the secret information in the text area. Next press the embed button for hiding the secret data. The figure 4 below shows these values.

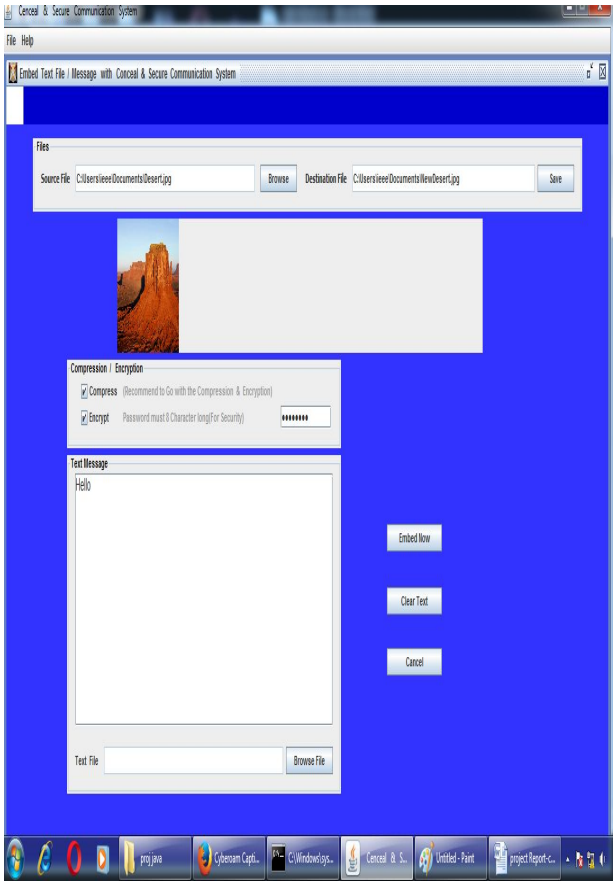


Figure 4: Embedding of secret data in image file.

Figure 5 shows the de-embedding screen.

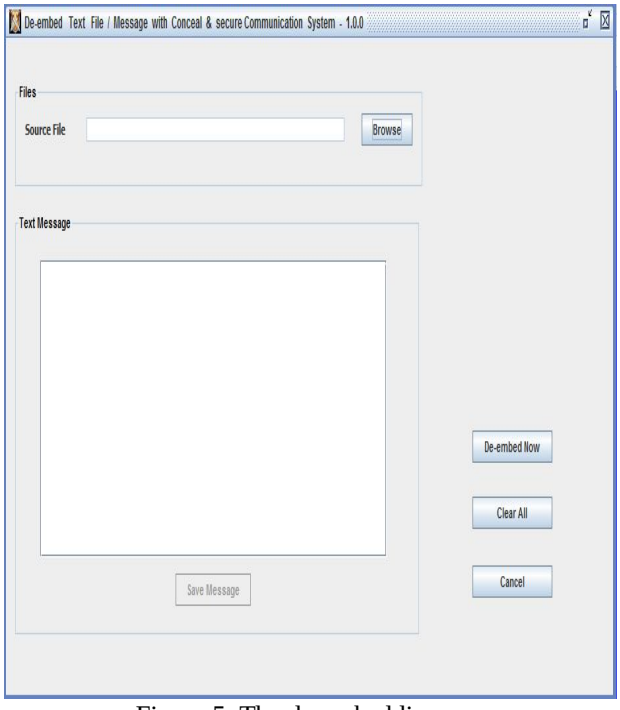


Figure 5: The de-embedding screen.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

User need to select the file containing secret information, specify the key (password) & press the de-embed button as shown in figure 6 below.

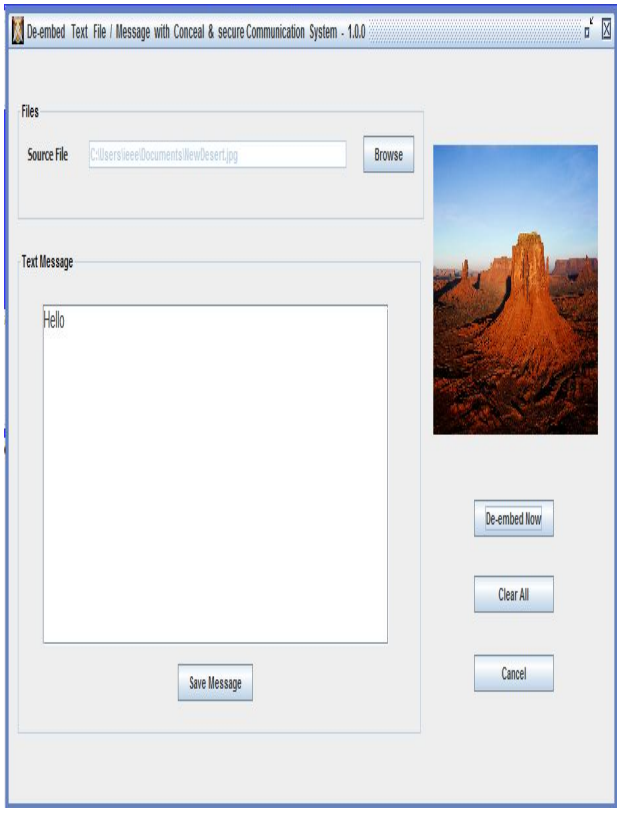


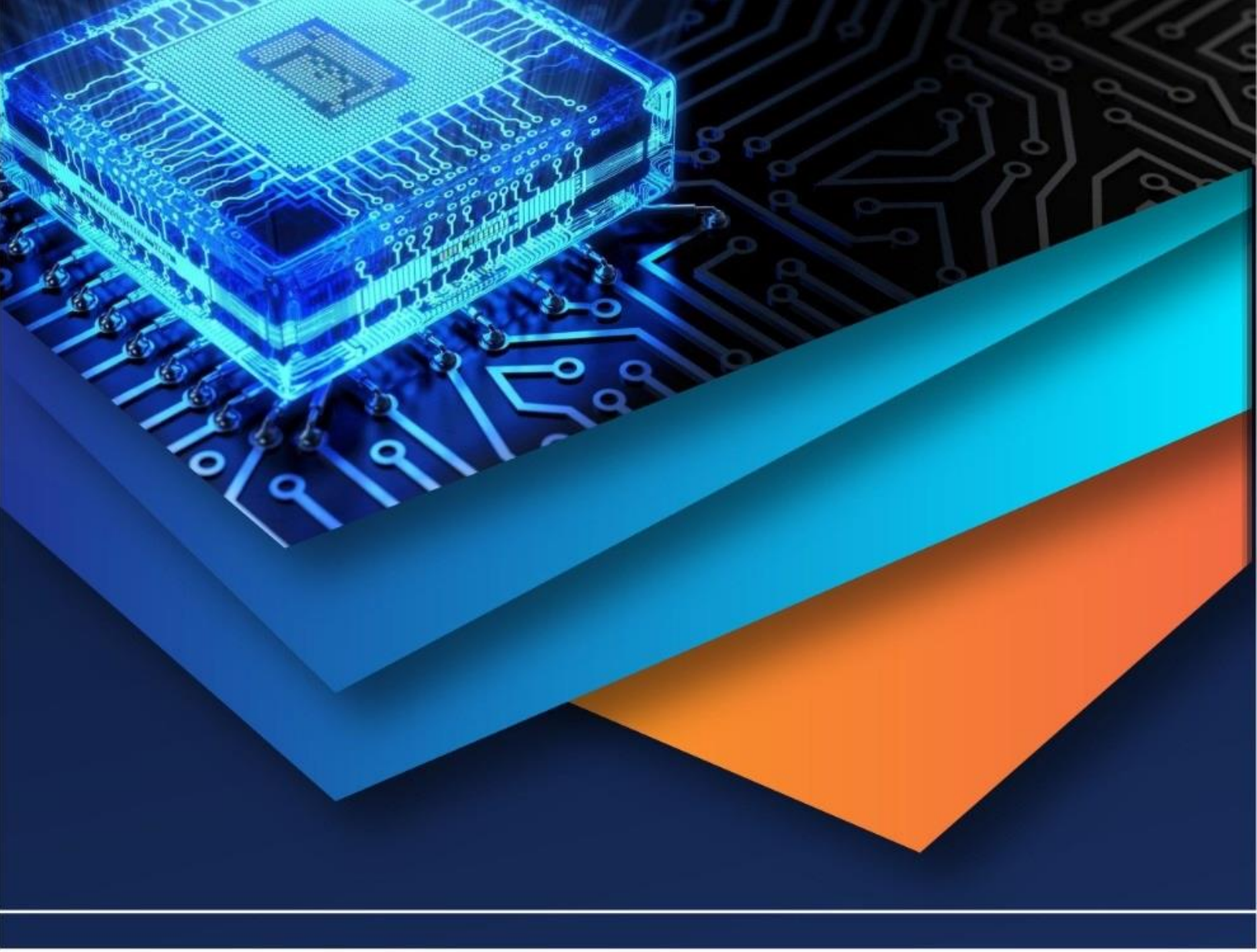
Figure 6: Extracting the hidden information

V. CONCLUSION

It is the process of hiding information which are need to be transferred on insure transmission medium (e.g., Internet) so that no one except sender or receiver can know the very existence of information. As the message is not visible so it does not get any attention of unauthorized users which safeguard the secret message. There are many good reasons as well to use this type of data hiding, including watermarking or a more secure central storage method for such things as passwords, or key processes. In this paper, we used different techniques for hiding/embedding secret data in text, image, and audio/video signals as cover media.

REFERENCES

[1] Stefan Katzenbeisser, Fabien A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking (Boston, Artech House, 2003)
[2] M.Grace Vennice, Prof. Tv. Rao, M. Swapna, Prof. J. Sasi kiran , "Hiding the Text Information using Steganography", International Journal of Engineering Research and Applications (IJERA) ,Vol. 2, Issue. 1, ISSN: 2248-9622, pp. 126-131, Jan-Feb. 2012.
[3] Abikoye Oluwakemi C., Adewole Kayode S., Oladipupo Ayotunde J. , "Efficient Data Hiding System using Cryptography and Steganography", International Journal of Applied Information Systems (IJAIS), Vol.4, Issue 11, ISSN:2249-0868, Dec. 2012.
[4] Kunal Hossain, Ranjan Parekh, "An Approach towards Image, Audio and Video Steganography", Second International Conference on Research in Computational Intelligent and Communication Networks (ICRCICN), IEEE 2016.
[5] Navneet Kaur, Sunny Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques", International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014.
[6] Vikas Tyagi, Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh, "Steganography Using Least Significant Bit with Cryptography", Journal of Global Research in Computer Science, Vol.3, Issue 3, ISSN: 2229-371X, March. 2012.
[7] Youngran Park, Hyunho Kang, Kazuhiko Yamaguchi and Kingo Kobayashi, "Integrity Verification of Secret Information in Image Steganography, Symposium on Information Theory and its Applications, 2006.
[8] Budda Lavanya, Yangala Smruthi, Srinivasa Rao Elisala, "Data hiding in audio by using image steganography technique", International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 6, November – December 201
[9] Pooyan, M. Delforouzi A., "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", IISSPIT 2007. IEEE
[10] Sukrati Jain, Dr. Ashendra K Saxena, "A Comparative Study of Various Security and Issues in Steganography Techniques", International Conference on Advanced Computing (ICAC-2016).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY