ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

Hybrid Steganography Using Multimedia (Image, audio, video) Concepts Based on Invariant Substitution Techniques

[1]M.Vara Lakshmi, [2]Sundaradasu Suresh
[1]Final M Tech Student, [2]Associate professor
[1,2]Dept of Computer Science and Engineering, Nimra Institute of Science & Technology, Ibrahimpatnam, Vijayawada

Abstract: Communication is the main aspect in present days. In communication secret message sharing is the main problem for confidential data transferring. Previously more number of methods or algorithms and techniques were introduced for providing security in confidential data sharing. Traditional techniques i.e. MLSB Embedding, LSB Varying Mode Embedding, Fusion Embedding, Thresholding Embedding comparing these algorithm results with every technique present in the steganography process. The method is designed in such a way that the modification is never out of the range interval. Above traditional algorithms present only image steganography in network data sharing. In this paper we will introduce audio steganography algorithms like Substitution methods. By using these methods we will provide more security using cryptographic methods developed in substitution techniques.

Index Terms: *audio steganography, substitution techniques, Image Steganography, Data Hiding, Cryptographic Systems.*

I. INTRODUCTION

Steganography is of Greek origin means "concealed writing ", from the Greek words staganos meaning " covered or protected " and graphei means "writing". Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. Steganography establishes a covered information channel in point-to-point connections, whereas watermarking does not necessarily hide the fact of secret transmission of information from third persons.

The Main Objective of Steganography is that the Data Hidden in it should not be detected if taken in to consideration in Cryptography though the data Is hidden even other than the receiver and sender can understand that there is some data in it because it occurs in scrambled form whereas in steganography apart from the receiver and sender no one can understand that some data is existed in the image and steganography mainly concentrates on how to avoid detection of data.

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

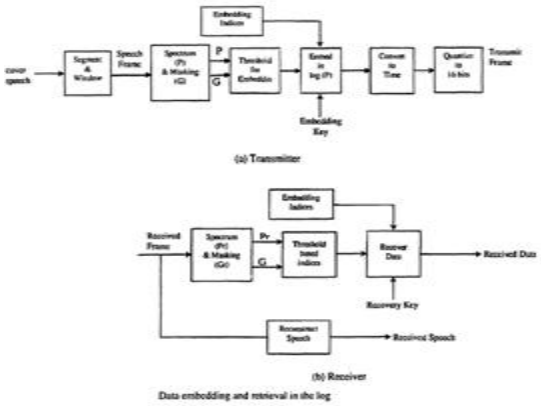

Figure 1: Data hiding process with audio.

Traditional steganography techniques are image data hiding process with LSB cryptographic systems. The previous Steganographic methods have the Falling of Boundary Problem. My Proposed Methods can overcome this problem. A Falling of Boundary Problem is that a Pixel Value may greatly differ from its surrounding Eight Pixels when the data is embedded in it as I know the Pixel value must be between (0-255). In this region we will provide security using encryption and decryption techniques.

Steganography is not actually for encrypting messages but hiding them within something else to enable them to pass undetected. Traditionally it was achieved with invisible ink, microfilm or taking the first letter from each word of a message. This is now achieved by hiding the message within a image file or audio file. In our proposed work also used Pixel Value Differencing for the representation of Image data hiding.

In the process of embedding a secret message, a cover image is partitioned into non-overlapping blocks of two consecutive pixels. A difference value is calculated from the values of the two pixels in each block. All possible difference values are classified into a number of ranges. The selection of the range intervals is based on the characteristics of human vision's sensitivity to gray value variations from smoothness to contrast. The difference value then is replaced by a new value to embed the value of a sub-stream of the secret message. The number of bits which can be embedded in a pixel pair is decided by the width of the range that the difference value belongs to. The method is designed in such a way that the modification is never out of the range interval. This method provides an easy way to produce a more imperceptible result than those yielded by simple least-significant-bit replacement methods. The embedded secret message can be extracted from the resulting Stego-image without referencing the original cover image. Moreover, a pseudo-random mechanism may be used to achieve secrecy protection.

II. RELATED WORK

In today's dynamic and information rich environment, information systems aware become vital for any organization to survive. With the increase in the dependence of the organization on the information system, there exists an opportunity for the competitive organizations and disruptive forces to gain access to other organizations information system. This hostile environment makes information systems security issues critical to an organization. This hostile environment makes information systems security issues critical to an organization. Current information security literature either focuses on anecdotal information by describing the information security attacks taking place in the world or it comprises of the technical literature describing the types of security threats and the possible security systems. In order to secure the transmission of data,

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

Steganography has to be implemented. Steganography is the science of devising methods that allow information to be sent in a secure form in such a way that the only person able to retrieve this information is intended recipient. Traditional techniques i.e. LSB was used image transformation with bit of information. There are several ways of hiding information. Simple techniques include hiding data in unused portion of the file such as the header of the Microsoft word.

III. BACK GROUND WORK

Traditionally we using different data hiding techniques using image were introduced. In that firstly we introduce MSLB embedding message algorithm. Next we are using LSB Varying Mode Embedding using 8 bit gray level cover image was used providing security. Fusion Embedding was used for cover image data hiding. Thresholding Embedding used for random key distribution events in data transfer. By performing these entire algorithm in data then we describe different image security events. But all these algorithms are worked in only image data hiding process.

IV. PROPOSED WORK

Due to the Falling of Boundary Problem in existing data hiding techniques. We will introduce substitution technique for information hiding.

for $i = 1 \ldots, \ell(c)$ do
  $s_i \leftarrow c_i$
end for
generate random sequence k_i using seed k
$n \leftarrow k_1$
for $i = 1, \ldots, \ell(m)$ do
  $s_n \leftarrow c_n \leftrightharpoons m_i$
  $n \leftarrow n + k_i$
end for

Figure 2: Generating code for security in both audio video hiding.

By using encryption and decryption processes present in substitution techniques were developed in audio data hiding.

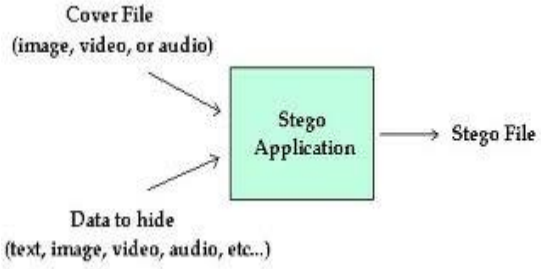

Figure 3: Procedure for data hiding using different techniques.

We will provide efficient data protection in transfer of data from one network to another network. As shown in above figure we are using different methods for providing security in image, audio, video.

V. EMPIRICAL RESULTS

In this section we describe the results obtained by performing security considerations to data. As shown in figure 3, description as follows select image or audio for storing information then we will perform substitution techniques for data security. In that select entire text present information that can be stored

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

default. Then we will perform encryption technique on that file then file can be changed with smile migrations present audio or image. We will calculate following things Transparency evaluates the audible distortion due to signal modifications like message embedding or attacking. In order to meet fidelity constraint of the embedded information, the perceptual distortion introduced due to embedding should be below the masking threshold estimated based on the HAS/HVS and the host media. Capacity of an information hiding scheme refers to the amount of information that a data hiding scheme can successfully embed without introducing perceptual distortion in the marked media. Robustness measures the ability of embedded data or watermark to withstand against intentional and unintentional attacks. Unintentional attacks generally include common data manipulations such as lossy compression, digital-to-analog conversion, re-sampling, re-quantization, etc. whereas intentional attacks cover a broad range of media degradations which include addition white and colored noise, rescaling, rotation (for image and video steganography schemes), resizing, cropping, random chopping, and filtering attacks.

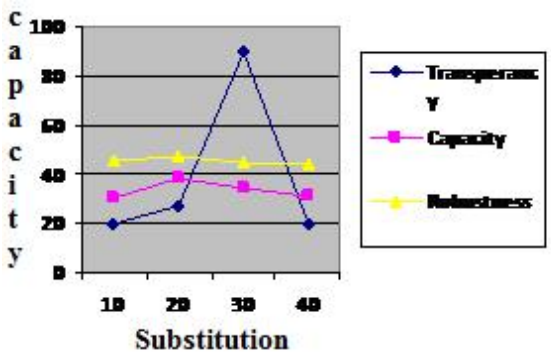

Figure 4: Efficient results for data hiding techniques.

As shown in above diagram we will increase the data transfer rate in network data sharing using steganography techniques.

Analysis for Image Hiding:

I/P	Cover Image	LSB	Bits	Embedded	O/P
.png	12.6kb	Y	1 to 1	Red bar	.png
.png	204kb	N	1 to 7	Png	.png

Table 1: Image hiding results.

According to the image hiding results shown in above table we are providing efficient security religious.

Analysis for Audio Hiding

I/P	Cover Audio	LSB	Bits	O/P
.mp3	112kb	No	1 to 1	.mp3
.mp3	50kb	No	1 to 7	.mp3

Table 2: Audio hiding results.

According to the audio hiding results shown in above table we are providing efficient security religious.

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

Analysis for Video Hiding

I/P	Cover Video	LSB	Bits	O/P
.mpg	112kb	No	1 to 1	.mp4
.mpg	50kb	No	1 to 7	.mp4

Table 2: Audio hiding results.

According to the video hiding results shown in above table we are providing efficient security religious.

VI. CONCLUSION

In this paper we observe the hiding techniques for image hiding and audio hiding. Audio hiding can be developed in single event substitution technique. In our proposed work we are providing efficient security than image security considerations. As a further improvement of our proposed steganography, is it was developed in different encryption and decryption techniques in symmetric block cipher process with pixel value differences

VII. REFERENCES

[1] C Chang. A steganographic method based upon JPEG and quantization table modification. Information Sciences, 141(1-2):123 -138, March 2002.

[2] Mazdak Zamani , Azizah A. Manaf , and Rabiah B. Ahmad," Knots of Substitution Techniques of Audio Steganography", 2009 International Conference on Computer Engineering and Applications IPCSIT vol.2 (2011) © (2011) IACSIT Press, Singapore.

[3] Swati Malviya1, Manish Saxena2, Dr. Anubhuti Khare3," Audio Steganography by Different Methods", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 7, July 2012).

[4] Preeti Singh, Charu Pujara," Comparative study of various Techniques Employ in Image Steganography", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[5] Sushil Kumar1, S.K.Muttoo2," A Comparative Study Of Image Steganography In Wavelet Domain", IJCSMC, Vol. 2, Issue. 2, February 2013, pg.91 – 101.