IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 12, December. 2019, ||Series -I || PP 24-27

Steganography For Hiding Data By Using Reversible Texture Synthesis(Audio & Video)

D. Mohini, Mr.Lalitkumar.P Bhaiya, Neelam Sharma
Chhattisgarh Swami Vivekanand Technical University
Name of organization: Bharti College of Engineering & Technology, Durg, India
Received 28 November 2019; Accepted 13 December 2019

Abstract–Hiding a data in cover stego file by using different techniques and method of steganography. As steganography defines concealing of a data as a secret information in cover stego file, the file may be in text or audio but message at text format and transferred from sender to receiver side. Receiver can able to retrieve/extract the message through reversible texture synthesis. In digital world, data transmission from one to another place by internet with its security is not an easy task. Few decades the data transmission is not secure because it's a public communication and attackers are ready to attack by proxies, intruder etc. which makes many issues. By video and audio steganography approaches, data can easily transmit its destination in a secure manner. It allows to extract messages from source texture through a stego synthetic in video and audio steganography, message is concealed in another medium such as audio file. So we are dealing with different steganography techniques, methods, algorithms, its pros and cons.
Keywords- Steganography technique, Digital Steganography, Texture Synthesis, LSB, DCT

I. INTRODUCTION

In this era of digital world of networking security becomes a critical issue to secure our data from intruders. More information is needed to transmitted for communication which should be faster, simpler and easier through the internet. But internet fails to keep secret from unauthorized party. So that for data security we are using steganography methods which deals with a conceal of data i.e. hiding a data inside digital content, it may be audio file or image file. The data is in the text format which is hidden in image or audio file. Steganography is a data hiding technique where information is embedded in a digital media i.e. sharing hidden information by putting data in audio & video file, finally it sends the secret information confidentially [1]. In this research paper, two different steganography techniques are used firstly image steganography, where data is hidden in a image so we can easily embed and extract the data using a sharing secret key between sender and receiver [2]. Secondly audio steganography which is same as like image steganography but the medium of transferring file is audio file, which is in the format of .au file.

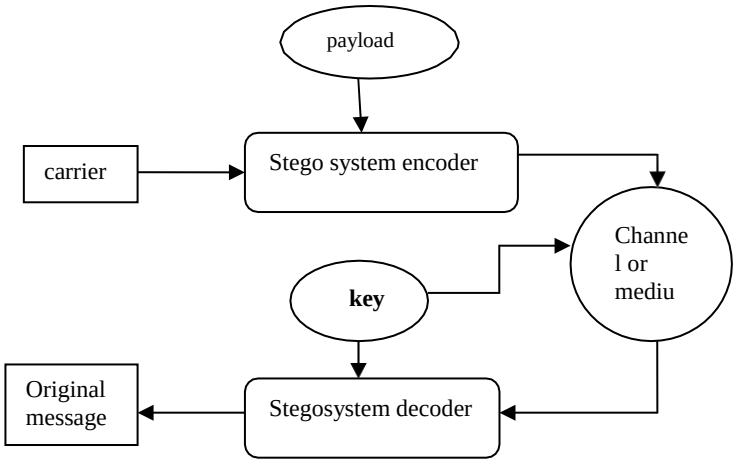

Figure 1: The flow chart of stegosystem

In this figure 1: defines the flow process of Steganography process. Encoder and decoder helps the system to extract the output which is needed, such as to make unique id or to decode for investing purpose. Channel or medium defines the source as in the form of text, image, audio or video and convert it into the needy output. This system is capable of handling hidden data inside digital content. There are two parties who makes secure communication by depending existence communication detection. We use the texture synthesis process

in steganography to seal a message which embeds the source texture image of secret messages through the reversible texture synthesis that allows source and secret to extract from stego synthetic structure [3]. Stego synthetic structure is a frame work synthesis of cover data applicable whenever it generated. The structured stegofiles are composed of source texture, our proposed system is not vulnerable to any kind of hazards generated in steganalytic algorithm. Advantage of this audio and video steganograpy by using reversible texture synthesis is a "simple and easiest security system". Steganographic message is invisibly integrated and covered inside the medium of harmless source, it is difficult to detect and extract without knowing key and its scheme of encoding.[4].

II. RELEATEDWORK

1. LEAST SIGNIFICANT BIT (LSB)

LSB had a property to hide a data in image or audio, where signifies least significant bit of audio or image is replaced with data bit i.e. it replaces the last bit of each pixel values to reflect the message that needs to be hidden [5]. By LSB we can able to encode a large amount of data. In this paper, a lossless data is hidden by using the technique of LSB in stego file, which does not affect on any properties of file. In recent days this LSB algorithm is implemented and taking as challenging to transfer the embedded information to destination without any defect [6]. In audio steganography, LSB coding the last bit of carrier file is replaced by bytes of secret message. Mainly right most bit is chosen for replacement because it makes impact on the quality of file [7]. In video steganography, LSB using substitution using different polynomial equations and it operates on LSB bit from media files to embed in a carrier file. We can able to hide text information in a video visual file, which LSB (Least Significant Bit) of each byte of the carrier file is changed to embed at confidential data[8]. So here the secret text data is embedded in cover medium using a secret key and same key is used for decoding the hidden data

2. DISCRETE COSINE TRANSFORM(DCT)

In audio steganography, a good steganographic technique is not only intends at embedding data that changes made in cover audio but also at efficient extraction of data. LSB is popular algorithm in steganographic. The main aim and purpose of this paper is creating audio steganography technique by changing LSBs of DCT coefficients of cover audio [9]. The data which is proposed embedding by spreading all over layers LSBs of the DCT coefficient. It has proven to be robust than conventional LSB technique and channel induced noise as well, in terms of evaluation

DCT packs the energy of signal into the low frequency regions which provides an option of reducing the size of the signal without reducing the quality of the signal. Since we are working on audio signals here, we focus on the DCT of a 1-D sequence, especially DCT-II and its respective inverse, IDCT-II.Following are the definitions of the DCT-IIand IDCT-II [10]

IDCT-II

$$x\,k = w\,k \sum_{k=1}^{N} y(k)\cos\frac{\pi(2n-1)}{2N}$$

$$k=1,2\ldots N$$

where*w(k)* used both in DCT and IDCT is defined as

$$w\,k = \begin{cases} \frac{1}{N} & k = 1 \\ \frac{2}{N}, & 2 \le k \le N \end{cases}$$

In video steganography we are using 32*32 quantization vector, by this all videos are sliced in number of images differently. Firstly, text messages are converted to ASCII and encode as bit form compatible according to vector of video. It fills the bits to occupy low intensity, if still lefts then pinned into high intensity bits. Finally embedding scheme is done by DCT. The proposed algorithm is enhanced further by making confidential imagery [11].

III. PROPOSEDMETHODOLOGY

We approached some methods for audio and video steganography which has a bit of hiding process. The secret key helps to hide information from unauthorized person.

For Audio, the methods and steps are as follows: -

Input:
Cover Audio + Secret Information (text document) + Key = Stego Audio (Embedded with Data)

Decryption:
Stego Audio + key = Secret Information (Extracted)

A. Steps of AudioEmbedding
1. An audio is selected as stega file oraudio.
2. A text document as an information is embedded withfile
3. LSB and DCT algorithm follows and secret key is given to embeddeddata
4. After reading the secret data, key is given as a form ofpassword.
5. Convert audio into binary format by Least SignificantBit
6. Embed secret data in identical location and produces a stegoaudio

B. Steps for message extraction process from audiofile
1. Stego audio as input init.
2. Identifies the location of hide the secret data in bits ofindex
3. Give the password as a key which is shared between receiver andsender
4. Extract the secret message which is in document form

For video steganography we are using developed technique is based on LSB steganography, a substitution steganography that replaces the least significant bit of the DCT coefficients of the cover video. The whole process is mainly of two stages: The sender‟s side and the receiver‟s side.

A. Sender'sSide:

***a)* Compression of the secretmessage:**

HerethesecretmessageistakenasaninputfromtheuserandthecorrespondingHuffmanDictionaryiscalculateddynamically,using which the message is compressed using HuffmanCoding

***b)* Finding the DCT coefficients of the CoverAudio:**

InthisstepttheCoverAudioisfirstmappedontotheDCTdomain,usingtheformulaforDCTinSectionItisthenconverted to itscorrespondingbinaryform,aftermultiplyingitwithasuitablescalingfactor.

***c)* Embedding of thedata:**

The spread factor and bit position are taken as inputs from the user in this step. The compressed and encoded secret message is then spread along layers of the LSBs of the DCT coefficients in a sine wave. message (See Figure.2). In the end a parity-bit is added to facilitate the integrity check on the message.

***d)* Keysequence:**

The spread factor and the bit position is XORed with a predefined sequence and is transmitted to the receiver through a covert channel as a „key sequence‟. Refer Figure.3 for the process on the sender‟s side.

B. Receiver'sSide:

a) **Extraction of the data:**

The DCT-II of the stego file received at the receiver‟s end is taken. It is again scaled and converted to binary in the same way as in the sender‟s side. Using both the covertly received key sequence and majority logic decoding the Huffman dictionary and compressed message is extracted. The message is then decoded to its original form using the Huffman dictionary[12].

IV. ONCLUSION & FUTURE SCOPE

In these paper we introduced two robust methods of data hiding in video or in audio,which is known as video steganography and audio steganography respectively. In video steganography, the carrier medium is video file which is in the form of .mp4 where hiding text file equal to size of video same as in audio steganography but the carrier medium is audio file in form of .au. The secret keys have to be known from both receiver and sender side. Keys are not shared in cover images but distributed separately.

ACKNOWLEDGEMENT

Its highly immense pleasure to express my deep gratitude towards my project guide Prof. Neelam Sharma and Project Director Mr.Lalitkumar.P Bhaiya of Computer Department for valuable co-operation and guidance that had gave me throughout my research
.All work done in the paper will surely help to research for future work.

REFERENCES

[1]. D. Singla and M.Juneja," Hybrid Edge Detection- based Image Steganography technique for Color Images," in Intelligent Computing and Devices Services Advances in Intelligent Systems aaaand computing 2015277-280

[2]. A.A. Efros and W.T.Freeman," Image Quilting for Texture Synthesis and Transfer", in Proc. 28th Annu. Conf. Comput.Graph. Interact.Tech., 2001 pp341-346

[3]. Lou D.C., Liu J.L. &Tso H.K. (2008). Evolution of Information – Hiding Technology. . In Nemati H. (Ed.). *Premier Reference Source – Information Security and Ethics: Concepts, Methodologies, Tools and Applications*, Volume 1, Chapter 1.32. New York: Information Science Reference. pp 438 –450.

[4]. E.Cole , Hiding in Plain Sight: Steganography and the Art of Convert Communication, Wiley publishing,2003.

[5]. Arun Kumar Singh, Juhi Singh, Dr Harsh Vikram Singh," Steganography in ImagesUsing LSB Technique", International Journalsof Latest Trends in Engineering and Technology(IJLTET) vol 5 Issue 1 January 2015Kuo-Chen Wu and Chung-Ming, Member, "Steganography Using Reversible Texture Synthesis",IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 24, NO. 1, JANUARY2015

[6]. M.Jayachandran and J.Manikandan, "SAR Image Compression using Steganography", 2010 International Conference on Advances in Computer Engineering,pp.203-206.

[7]. Prashnat Jhori, Amba Mishra, sanjoy Das, Arun Kumar," Survey on Steganography methods (Text, Image, Audio, Video, Protocol, and Network Steganography", 2016 International Conference on Computing for Sustaiable GlobalDevelopers.

[8]. MrithaRamalingamandNorAshidiMatIsa,"AsteganographyApproachforSequentialdataencodinganddecodinginVideo Images", IEEE International Conference on Computer Control Information and its application(IC 3 INA), 2014,100-125

[9]. Jayaram, Ranganatha and Anupama, "INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August2011.

[10]. ChhayaVarade,DanishShaikh,GirishGund,VishalKumar,ShahrukhQureshi,"ATechniqueforDataHidingusingAudioand Video Steganography',International Journal of Advanced Research in Computer Science and Software Engineering,Volume6,
Issue 2, February 2016

[11]. Khan Muhammad, Jamil Ahmad, Haleem Farman, Muhammad Zubair, "A Novel Image Steganographic Approach for Hiding Text in Color Images using HSI Color Model", pg.1-11

[12]. Shreyank N Gowda, "Advanced Dual Layered Encryption for Block BasedApproach to Image Steganography",2016 International Conference on Computing, Analytics and Security Trends (CAST)College of Engineering Pune, India. Dec 19- 21, 2016

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

D. Mohini." Steganography For Hiding Data By Using Reversible Texture Synthesis(Audio & Video)." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 12, 2019, pp. 24-27.