Data Security with combination of Cryptography and Audio Steganography

MSc Internship
MSCCYB

Kapil Kapoor
x18109128

School of Computing
National College of Ireland

Supervisor: Mr Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Kapil Kapoor		
Student ID:	X18109128		
Programme:	MSc Cyber Security	**Year:**	2019
Module:	MSc Internship		
Supervisor:	Mr Vikas Sahni		
Submission Due Date:	12/12/2019		
Project Title:	Data Security with combination of Cryptography and Audio Steganography		
Word Count:	**6453**	**Page Count: 20**	

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: ………

Date: ………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Data Security with combination of Cryptography and Audio Steganography

Kapil Kapoor
X18109128

Abstract

In this age of technology, digital information such as image, text, audio, etc are exchanged over the network. Confidential text messages can easily be intercepted and misused if not send properly. So, data security has been a major area of research. Much of the research has been done to find the optimal solution for confidentiality, integrity and reliability of text. Combination of cryptography and steganography have proved to be useful, but every method has its own pros and cons. This paper implements a hybrid combination of the cryptography and steganography technique echo hiding for secret transfer of text data in an audio file. The metrices like PSNR, MSE and SNR have been used for evaluation of approach.

Keywords: Cryptography, Audio Steganography, LWT-DCT, Echo Hiding, Bipolar Forward-Backward Kernel, Test Security, AES algorithm, PSNR, MSE, SNR.

1 Introduction

Text shared over internet is very vulnerable if not sent securely. Cryptography aims to provide the confidentiality to the data and steganography provides the imperceptibility. Through the combination of these, confidential data can be sent in an imperceptible way maintaining the integrity and reliability. In steganography data to be send is embedded into cover media to make its existence unknown. This cover media may be image, audio or video file. A lot of research has been done for secure exchange of data but still the intruder can come up with different techniques to get confidential information. A good technique should have imperceptible, robust, high payload capacity and immunity to noise (Lahiri, 2016).

How efficiently can a combination of Cryptography and Audio Steganography technique be used to provide secure means of communication.
The main objective of the proposed model is to provide confidentially, integrity, imperceptibility, reliability and robustness by using combination of the cryptography and steganography in transform domain. The steganography provides the required imperceptibility and confidentiality of the data but once the algorithm is known to intruder it is possible to break and get the embedded text. So, to strengthen the approach of the steganography a hybrid model is proposed which makes use of the cryptographic algorithm to encrypt the text before embedding. This encryption provides an extra layer of robustness against intruders. It is 3-layer model for the data security. A combination of the LWT-DCT techniques for getting the embedding area for better compression and space. The combination

is resilient to many attacks. The bipolar forward-backward echo hiding technique which is better among other echo hiding for providing robustness against noise. The secret text to be send is encrypted using cryptographic algorithm which can only be decrypted by the key. Even if intruder bypass all and get the text, still it will cipher text and needs key with cryptographic algorithm to get plain text.

The audio steganography provides more payload capacity and has more randomness as a greater number of bits are present. The proposed approach should embed in such a way that there are minimal changes on the cover audio signal.

2 Background

Audio steganography uses signal as cover media. Echo hiding is one of the methods that exploits the characteristics of audio signal. In echo hiding the cover signal is divided into the number of segments equal to number of bits to be embedded. Echo is produced to embed the data such that size of echo produced should not be greater than length of signal. Echo signal is embedded with each block. After embedding these blocks are joined together to get signal with text. The hiding is dependent on three parameters decay rate, offset and initial amplitude. Off set provides the distance between data points of echo and cover signal. Initial amplitude helps in determining the amplitude of the cover audio. Echo function is prepared by keeping decay rate in mind. Figure 1 represents the parameters discussed.

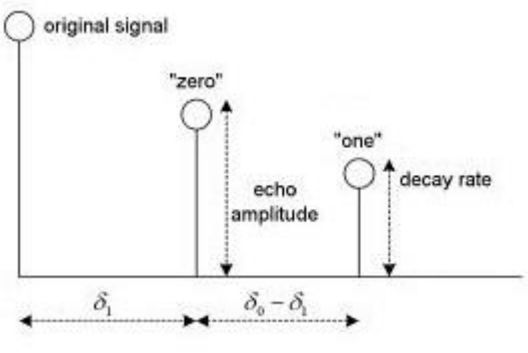


Figure 1Echo hiding parameters (Lahiri, 2016)

The extraction is done by using the cepstrum analysis. The echo introduced should not cause much distortion in the original signal. There are some limitation of the human auditory system, these limitations are exploited in the echo hiding to get good results.

Much of the research has been done but with advancement of technology intruders find new ways to get the data.

The transform domain techniques like DWT an DCT have different advantages and disadvantages. The DWT is more robust when retrieving the data on the other hand DCT provides better compression that’s minimum distortion and good quality of cover media (“(PDF) Review of Transform Domain Techniques for Image Steganography,” n.d.). Many researches have been done on the combination of the DWT-DCT to provide better robustness and compression which are discussed in next section.

The encryption using the cryptographic algorithm helps in keeping the data safe from unauthorized access. Only authorized user who have key can decrypt and view the data. Based on key used for encryption and decryption they are classified as symmetric and asymmetric. Algorithms which use same key for encryption and decryption are classified as symmetric and algorithms using two different keys as asymmetric. The key length also plays an important role in providing security and resilience against attacks(“What is Cryptography?,” 2018) . The cryptographic approach used in this paper aims to improve text security using the robust algorithm available.

3 Related Work

3.1 Steganography

Steganography is continuous field of research and various researches have been carried out taking different cover files. Time and Frequency are two major domains according to embedding process. Methods like least significant bit, Spread Spectrum, Parity coding, Phase coding and echo hiding are used for embedding in audio cover file (Macit, Hüseyin & Koyun, Arif & Güngör, Orhan. (2018)” n.d.).

a) Least Significant bit hides data in the least significant bits that is the last bit of the cover. Since LSB are not used so change in them do not affect the cover. The cover data is converted into to the bit string and last bit are used to embed the data. LSB is classified on the basis of number of bit to be changed such as 1-LSB,2-LSB,3LSB and 4-LSB.

b) Spread Spectrum uses the wide frequency bandwidth for the data embedding as data to be embedded is spread over it. The SNR is kept low so that imperceptibility is maintained. Also, if fragments of the data get removed from a few frequency bands still we have enough bands for data recovery.

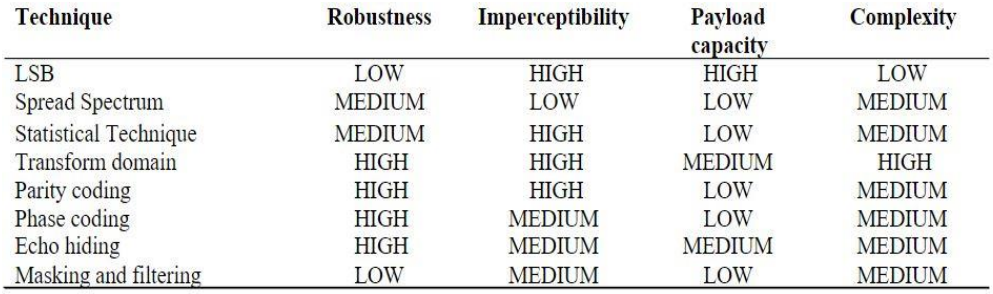
c) Parity coding is bit based method, where parity bits are added to sequence of bits based on the fact that sum is 0 or 1. If the wrong sequence is used for extraction the whole data can be corrupted.

d) Phase coding used the phases to embed the data. The data is embedded onto the first phase spectrum of the divided blocks of the cover signal, it has low capacity to embed data.

e) Echo hiding hides the data by adding an echo. It has high transmission rate and robustness if only one echo is generated. Cepstrum analysis is used to get the hidden data embedded using echo.

So, a technique must have good robustness, imperceptibility and payload capacity but low complexity. In comparison shown in Table 1 (Macit, Hüseyin & Koyun, Arif & Güngör, Orhan. (2018)” n.d.). LSB technique seems to be ideal but the due to slight change in the LSB would result in loss of data and provides low robustness. Spread spectrum and parity has low payload capacity and imperceptibility. Phase coding and echo hiding have all the required components but echo hiding has a better payload capacity form phase coding which makes it one of the best available technique based on the parameters taken.

Table 1: Comparison of Steganography (Macit, Hüseyin & Koyun, Arif & Güngör, Orhan. (2018)" n.d.)



Technique	Robustness	Imperceptibility	Payload capacity	Complexity
LSB	LOW	HIGH	HIGH	LOW
Spread Spectrum	MEDIUM	LOW	LOW	MEDIUM
Statistical Technique	MEDIUM	HIGH	LOW	MEDIUM
Transform domain	HIGH	HIGH	MEDIUM	HIGH
Parity coding	HIGH	HIGH	LOW	MEDIUM
Phase coding	HIGH	MEDIUM	LOW	MEDIUM
Echo hiding	HIGH	MEDIUM	MEDIUM	MEDIUM
Masking and filtering	LOW	MEDIUM	LOW	MEDIUM

Echo hiding hides the data in audio signal as an echo. Major drawbacks of the methods are its low data security and low capacity (Almarabeh, 2016). The paper by (Matsumoto and Sonoda, 2015) makes use of audio signal as key sequence instead of pseudo random noise sequence combined with time spread echo hiding. It showed great resilience to variety of attacks like MP3 compression, noise addition, bandpass filtering, echo addition and time stretching. The echo hiding with key sequence provided robustness which was less in previous approaches. The security of embedded data is in dilemma if the steganography is known.

(Lahiri, 2016) introduced a model which embeds the binary data in the transform coefficients by using 2D DWT. Also, a pseudorandom sequence is used to encode data to provide security. The use of echo hiding here provides more robustness to channel disturbance and Nosie. The results show better secrecy and robustness provided by the method with the use of DWT, echo hiding and pseudorandom sequence, but text was left vulnerable.

Author in (K.P. and S., 2009) uses the bipolar kernel for audio watermarking. The choice of echo kernel plays an important role in defining the fidelity. An extended bipolar kernel is used to provide fidelity without any much compromise on detection. The traditional bipolar kernel causes noticeable distortion which was decreased by the extended approach. (Delforouzi and Pooyan, 2007) proposed a new echo hiding technique based on the dual backward and forward echo kernel which shows better robustness and detection rate. By increasing the kernel change in the payload capacity and robustness is noticeable drawback is that embedded text will be exposed to intruders if the steganography is known. (Tabara et al., 2017) presented a data hiding method with use of the echo hiding and correlation. On the decoding side to improve its efficiency voicing correlations used. The approach proved to be even more robust against noise attacks. Once the procedure is known the embedded data can be retrieved. The selection of the echo kernel and echo depending parameter selection helps in providing the security and the improves the payload capacity and imperceptibility.

(Tekeli and Aşlıyan, 2017) showed a comparison of various echo hiding methods like Single echo hiding, bipolar echo hiding, backward-forward echo hiding, bipolar backward and forward echo hiding and time-spread echo hiding. Parameters like robustness, imperceptibility and SNR were considered against MP3 compression at 64, 96 and 126 Kbits/s. Bit error rate and Normalized correlation were calculated. Results showed robustness increases when the length of segment is increased. Bipolar backward and forward echo hiding is considered more robust than others which is combination of the bipolar and backward-forward echo kernel. With the valuable research study bipolar backward-forward echo hiding proved to be most robust among other echo hidings so it is used in proposed research.

3.2 Transformation Techniques

The transform domain techniques make use of the mathematical operation to convert the data into frequency domain. Most common techniques used are Fast Fourier Transform (FTT), DCT (Discrete Cosine Transform), Dual Tree Complex Wavelet Transform (DTCWT), DWT (Discrete Wavelet Transform), Lifting wavelet transform (LWT) etc. In (Priyanka and Sathyanarayana, 2014) transform domain techniques are used to embed the text which was encrypted by the AES algorithm. Reasonable PSNR values with high correlation coefficient is observed by researcher.(Jain, 2013) proposed a DCT(Discrete Cosine Transform) coefficient comparison method. The cover is segmented and DCT is applied on each one of it to get two outputs; one DC signal which has high power and low frequency, other is AC signal with low power and higher frequency. The showed higher embedding capacity and signal quality than regular approach but the secret data is vulnerable if steganography is identified.

(Tewari et al., 2014) proposed work on audio watermarking with modification of DCT coefficients middle frequency band for embedding. The DCT provided good compression ratio and payload capacity but the compression was lossy.

LSB (Least significant Bit) substitution and replacement are most common techniques in time domain. The author (Meligy et al., 2015) showed a new method b using LWT and LSB embedding with use of the random keys. A good compression along with improved security was introduced with LSB but still little change in LSB will destroy the whole data hidden. (Kanhe et al., 2018) presented new method based on voiced and unvoiced speck characteristics with DCT coefficients for audio steganography higher robustness against different kind of signal processing attacks but embedded data is vulnerable. No security measure is applied to data individually.

A combination of DWT-DCT is proposed (Gupta and Khunteta, 2017) to embed the text. DWT is applied on the image first and to calibrate the text as per the sub-band it is also processed through the DCT. Embedding is done in three different bands with different equations resulting in more security. The hybrid model has provided more embedding, high insusceptibility and resistance to signal processing attacks.

LWT is based on the DWT but is betters as consumption of memory and time for computation reduces significantly.(Preet and Aggarwal, 2017) A combination for LWT-DCT is implemented by with Arnold transformation. The approach showed high PSNR and payload capacity with combination

(Lalitha et al., 2016) did an analysis of the DWT, LWT and DCT combined with SVD. It was seen that with change of the quantization level the SNR (Signal to Noise Ratio) decreases exponentially. The robustness was increased to a variety of the signal processing attacks like resampling, re-quantization, echo addition, cropping, additive white gaussian noise, signal addition and signal subtraction. In LWT-DCT model DWT is applied first to the signal to compute approximation and detailed coefficient vectors. On the resultant coefficients DCT is applied to get respective coefficients. DCT is like DFT (Discrete Fourier Transform) but uses real numbers. Clearly better SNR values between 0.01 and 1.0 with good imperceptibility. The techniques LWT-DCT-SVD was found robust to attacks.

A combination of the LWT and hyper chaotic encryption is used by author to provide security to the data in (Saleem et al., 2017). The reversibility of the cover and recover data with high payload capacity was proposed. The Reserve Room Before Encryption approach was used for embedding data. The approach provided complete reversibility of the cover with minimal data loss and high payload capacity with LWT.

(Panyavaraporn and Horkaew, 2018) paper presents the DWT-DCT hybrid watermarking for better robustness and extraction even after HEVC compression. DWT was used to get sub-bands and on those sub-bands DCT is applied to get the embedding area. The hybrid model proves to be more robust and secure.

In (Kabra and Agrawal, 2016) a robust LWT- SVD based watermarking is introduced. The use of LWT provided the lossless compression and low computational memory usage. The approach was found imperceptible and robustness against variety of geometric attacks. The use of LWT instead of DWT improved computational efficiency over other discussed approaches. DCT provides better compression and LWT offer low computational memory and scalability in watermarking techniques. The combination provides the fast compression and scalability. Proposed paper will use the combination of LWT-DCT for better robustness, compression and capacity.

3.3 Encryption

Encryption plays an important role in the proposed methodology, process of converting the normal text into the cipher text using encryption key is referred as encryption. For getting original plain text back decryption key is required and process is known as decryption. It provides the confidentiality to the data.

(Torvi et al., 2016) uses a unique for text steganography method for securing the data transmission. It encrypts the payload with XOR encryption before using steganography. The simple yet effective approach is used here. But text doesn’t have much randomness which can be provided by the audio steganography. Multiple encryption algorithms are available for providing the confidentiality to the data. Based on the requirements they are chosen. A comparison of various algorithm based on key size, block size, number of rounds, structure, flexibility and features is shown by (Abood and Guirguis, 2018) to determine the most suitable for encryption. The chosen algorithms were DES, DH, E-DES, RSA, T-DES, ECC, RC4, RC2, BLOWFISH, SEAL, DSA, RC6 and AES. After performing the analysis on various attributes, author states the selection of algorithm is based on the requirements. AES, Blowfish, RC4, E-DES and TDES are fastest in speed, encryption time, security and flexibility. The result shows that the AES is best in flexibility, encryption performance and security. Table 2

Algorithm	Created By	Year	Key Size	Block Size	Round	Structure	Flexible	Features
DES	IBM	1975	64 bits	64bits	16	Festial	No	Not Strong Enough
DH	Whitfield Diffie and Martin Hellman	1976	Variable	-	-	Public key Algorithm	Yes	Good Security and

								Low Speed
E-DES	IBM	1977	1024 bits	128 bits	16	Festial	-	Good Security and fast Speed
RSA	Rivest Shamir Adleman	1977	1024 to 4096	128 bits	1	Public Key Algorithm	No	Excellent Security and Low Speed
T-DES	IBM	1978	112 or 168	64 bits	48	Festial	Yes	Adequate Security and fast
ECC	Neal Koblitz and Victor Miller	1985	More than symmetric and variable	Variable	1	Public Key Algorithm	Yes	Excellent Security and fast Speed
EEE	Taher Elgamal	1985	1024 bits	-	-	Public Key Algorithm	Yes	Enough secured and fast Speed
RC4	Ron Rivest	1987	Variable	40-2048	256	Festiel Stream	Yes	fast Cipher
RC2	Ron Rivest	1987	8,128,64 by	64 bits	16	Festiel	-	Good and fast Security
BLOWFISH	Bruce Schneier	1993	32-448	64 bits	16	Festiel	Yes	Fast Cipher in SSL
SEAL	Phillip Rogaway and Don Coppersmith	1994	160 bits	32 bits	2	Public Key Algorithm	Yes	Not Strong and fast Speed
DSA	NIST	1997	variable	-	-	Public Key Algorithm	Yes	Good Security and fast Speed
RC6	Ron Rivest et.al	1998	128 bits to 256 bits	128 bits	20	Festial	Yes	Good Security
AES	Joan Daeman & Incent Rijmen	1998	128,192,256 bits	128 bits	10,12, 14	Substitution Permutation	Yes	Security is excellent. It is best in security and Encryption performance

Table 2 Comparison of cryptographic algorithms (Abood and Guirguis, 2018)

AES algorithm has excellent security level, least vulnerable to attacks and has most avalanche effect making it ideal to use for text encryption where are high concern privacy and integrity as shown by (Semwal and Sharma, 2017) A unique combination of the LSB embedding and AES encryption of text is shown by(Hashim et al., 2018). Using the MSB

(Most significant bits) for choosing the LSB bit for substitution with payload bits. The security of the text is enhanced by the encryption it with AES before embedding alone is vulnerable, so text is encrypted with AES to provide robustness. Based on the artifacts AES will be used for encryption.

The literature review conducted shows that audio watermarking technique must have high robustness, payload capacity, imperceptibility and maintains confidentiality and integrity. The techniques discussed have their merits and demerits, so we need to use a combination for getting the optimal result. Here in this a novel LWT-DCT based embedding using the bipolar forward-backward echo hiding techniques with the AES encryption for text is proposed.

4 Research Methodology

Integrity and confidentiality of the data is the issue faced with evolution of technology. In order to provide confidentiality of data and maintain the integrity, much of research has been done as discussed in the previous section. The discussed approaches have their strengths and the weaknesses, hence there is need for new approach to overcome all the short comings in existing methodology. A novel model of the audio steganography is proposed to provide the required confidentiality and integrity to secret data. The proposed method uses a hybrid combination of cryptography and steganography for successful transmission of data with least compromise on the quality of the carrier and high security of the secret text from intruders. Cryptographic algorithm is used to encrypt the secret text which provides the confidentiality and audio steganography algorithm is used to hide the text for better imperceptibility.

The approach aims to provide the better imperceptibility and enhanced secret data security with no noticeable change in cover file. For the development of application MATLAB is required which is a tool used for signal processing and wavelet analysis.

Text is encrypted with the help of the AES algorithm which is fast and reliable encryption algorithm (Abood and Guirguis, 2018). Through the literature survey done in previous section we came across conclusion of using the AES due to its feature, flexibility and block size which provide excellent security level. Two different codebases for the AES encryption are available on the GitHub by (Jonna, 2019) Jonna and Nicholas Lau (Lau, 2017). These are studied and downloaded. After deep study and modifications, a single AES text encryption code was obtained which encrypts the normal text to cipher text and vice-versa. A hybrid combination of the LWT-DCT transformation is used in which LWT is primary and DCT is secondary transformation the audio file. The effectiveness and advantages of the LWT-DCT over other techniques is found in the literature survey. For embedding the cipher text, the text must be converted into the ASCII values which then are converted to binary. For embedding the echo hiding technique is used. Different kinds of echo hiding techniques code repositories are available on GitHub by author Kadir Tekeli. The code is downloaded(Tekeli, 2019) and studied in detail. For embedding a process with resistance to various signal processing attacks echo hiding is good option. It can be differentiated based on the types of kernel used. Here in this paper a novel bipolar forward and backward kernel is used. The embedding takes places with the help of bipolar forward-backward echo hiding (BBFEH) technique which is combination of bipolar and forward-backward echo hiding technique provides the robustness for embedded data against noise attacks and good detection rate. The code for the forward-backward kernel and negative positive kernel was downloaded(Tekeli, 2019). The code was referred to generate code for the Bipolar Backward-Forward Echo hiding. Now the important part was the integration of the all the three modules, author (Lahiri, 2016)was contacted on social media and LinkedIn for gaining knowledge on the integration. Unfortunately, was unable to reach him. By trial and error method, and after numerous combinations the

integration was made possible. A hybrid combination of the techniques was used to get the confidentiality, integrity, robustness, imperceptibility and detection of kernel data.
For the evaluation matrices (Lahiri, 2016) used are

a) **PSNR (Pixel to noise Ratio)**

It is the ratio of the maximum power of a signal to noise which influences its representation.

$$PSNR = 10log_{10}\left[\frac{I^2}{MSE}\right]$$

Here ‘I ‘is maximum intensity.

b) **MSE (Mean Square Error)**

It is the mean square deviation between the estimated and actual value. Below is the mathematical expression

$$MSE = \frac{1}{[N\times M]^2}\sum_{i=1}^{N}\sum_{j=1}^{M}[X_{ij} - Y_{ij}]^2$$

M and N are numbers of columns and rows. X_{ij} and Y_{ij} are the intensity of the X_{ij} and $Y_{ij\ pixels}$ in cover and stegno image respectively.

c) **SNR (Signal to Noise ratio)**

It is power to meaningful signal to the power of the noise signal (unwanted noise, transmission noise etc).

SNR= P_{Signal}/P_{Noise}

d) **Spectrogram**

Spectrogram of signal represents the short time Fourier Frequencies or spectrum frequencies with time.(“spectrogram (Signal Processing Toolbox),” n.d.)

5 Design Specification

5.1 Architecture

5.1.1 Encoding

The below figure 2 represents the architecture of proposal. AES, LWT-DCT and echo hiding algorithms are main components of the method. The Ultrasonic audio signal is selected, and LWT is applied on the cover audio. The DCT transformation is applied on selected LWT coefficient to get the embedding area. The plain text input is encrypted with AES algorithm and resultant text is converted into the binary. With echo hiding technique the embedding is done in the embedding block. The result of embedding block is the stegno signal.

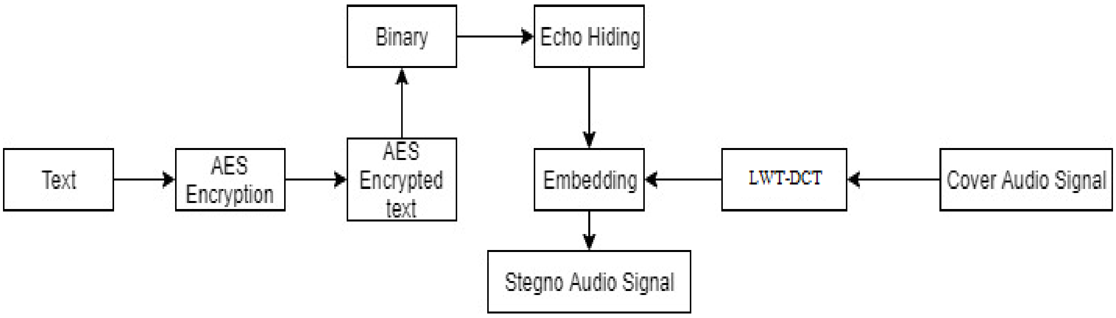


Figure 2 Encoding Architecture

5.1.2 Bipolar Backward and Forward Echo Hiding

It is a combination of the Forward-Backward echo kernel and Bipolar kernel also known as positive negative kernel. In this the bipolar kernel is mirrored. Figure 3 describes the kernel available in this technique used in BBFEH.

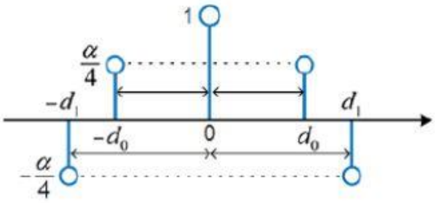


Figure 3 Bipolar Forward-Backward Kernel (Tekeli and Aşlıyan, 2017)

5.1.3 Decoding

The steganographic signal is exposed to the LWT-DCT algorithm and extraction area is selected. Inverse of the echo hiding that is use of cepstral analysis is done to recover the embedded bits. These bits are then decrypted by AES algorithm to get the plain text as shown in figure 4

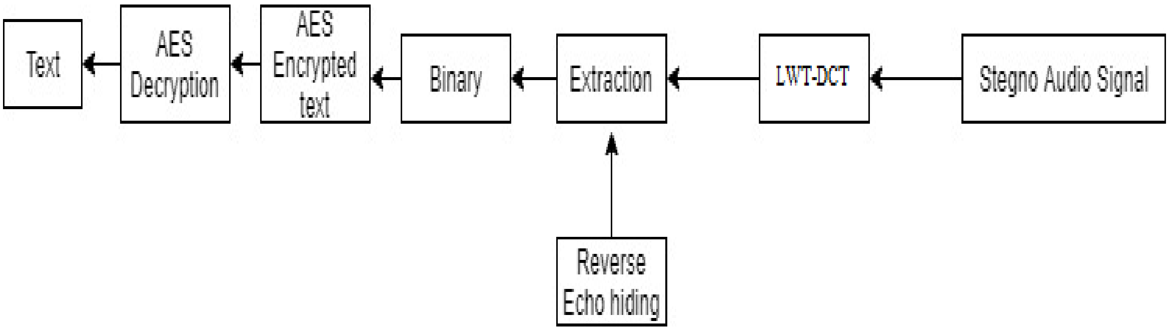


Figure 4 Decoding Architecture

6 Implementation

6.1 Encryption

It involves the plain text and AES Algorithm. The plain text is taken as input is fed to the encryption algorithm AES code developed by modification and taking references of the two different codes by Jonna(Jonna, 2019) and Nicholas Lau(Lau, 2017) to get AES encrypted text or cipher text. It is symmetric key algorithm as it used the same key for the encryption and decryption. The step by step implementation of AES is as follows.

1. User data converted into ASCII of int64
2. Key generation for encryption
3. Data conversion to square matrix and ASCII integer.
4. Adding key to data.
5. Repeats the following function and process in repetition.
   5.1 Shift the row
   5.2 Creates an array based on the column and multiplies them.
   5.3 Add key to data.
6. Shift row one last time.
7. Add key to data one last time.

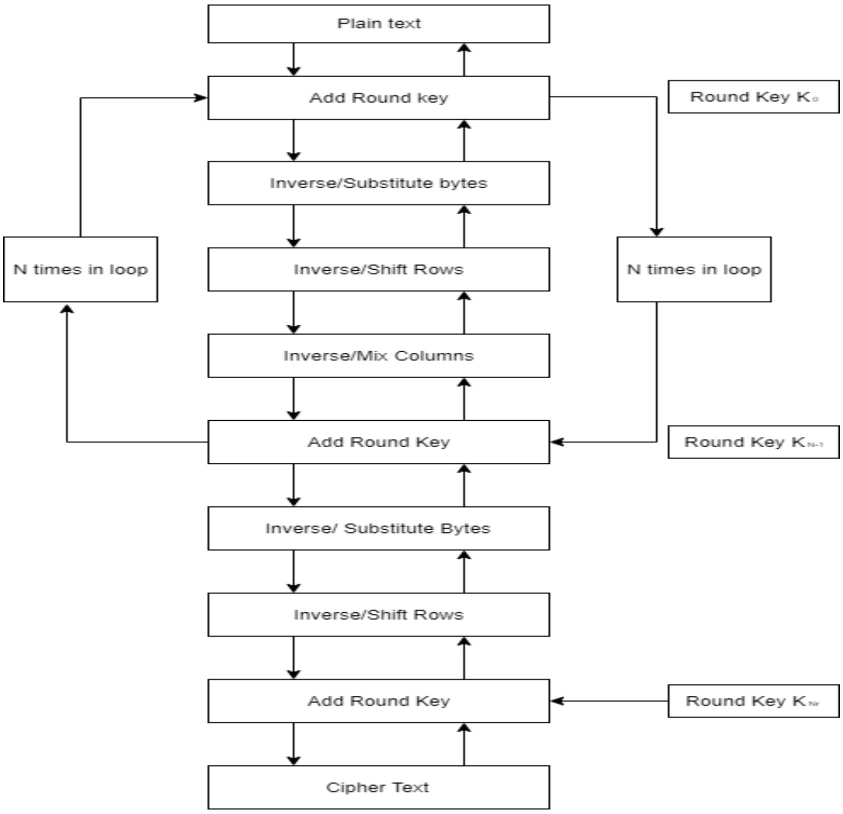


Figure 5 AES Implementation

Figure 5 represents the functioning of AES algorithm. The plain text comes across all the block and is converted to cipher text called encrypted text and process referred as encryption. The cipher text acts as input to our next step. Reverse of whole process is called decryption as shown in figure the flow form cipher text to plain text. The text is converted into its binary after encryption.

6.2 Steganography

On the audio file LWT transformation is applied. It gives a low and high frequency component of the signal as shown in figure 6. The high frequency components (CD) is selected for the embedding. The CD is selected as input for the DCT which give us a single output which is used for embedding. The combination of LWT-DCT provides the required robustness and lossless compression.

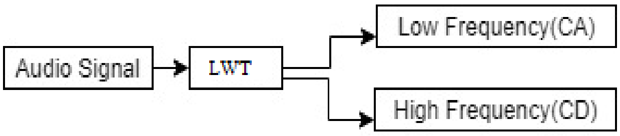


Figure 6 LWT Transformation

6.2.1 Encode

Bipolar forward and backward echo hiding is used for embedding. An echo signal is created by convolving the echo kernel and audio. The audio signal is divided into L number of segments where is L is number of bits to be embedded. Every segment is echo with delay correlating to data bits. L be the number if bits to be encoded and K be the length of the segment. Here K must be such that L.K must not exceed length of audio signal. An echo signal is generated which is filtered with mixer signal before adding to audio signal.

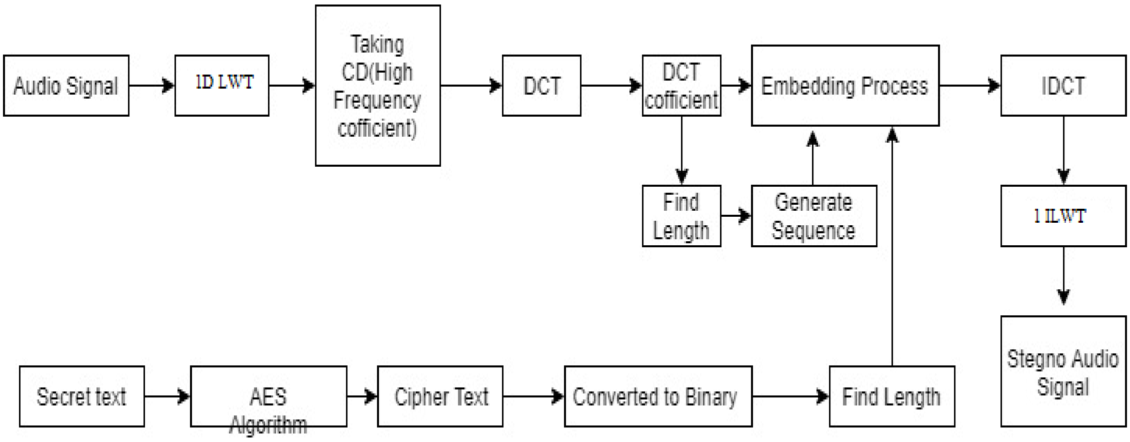


Figure 7 Encoder Implementation

The LWT algorithm is applied to the audio signal to divide it into low and high frequency coefficients, high frequency coefficient is taken and is given as input for the DCT algorithm with give back a DCT coefficient. The length is calculated to generate the sequence. The ciphertext converted into binary is taken as input for the bipolar forward and backward echo hiding process. mixer signal is generated for reducing distortion of adjacent segments. The

number of bits to be inserted are used to divide the block and length of audio signal is used to decide the length of blocks. The echoes are inserted with their delay corresponding data bits. Also, these echoes are added onto the DCT coefficient signal which was taken for embedding filtering with mixer signal.
The output signal is fed to IDCT algorithm the resultant signal and low frequency component is taken as inputs for the IWT, hence we get Stegno audio signal as shown in figure 7

6.2.2 Decode

The Stegno audio signal is taken, 1WLT is applied to CD coefficient which undergo DCT transformation and output length is calculated, the length is calculated, and the embedding block is fed with length and the DCT coefficient. The signal is divided in frames and Cepstrum analysis are used to get binary message vector as shown in figure 8.

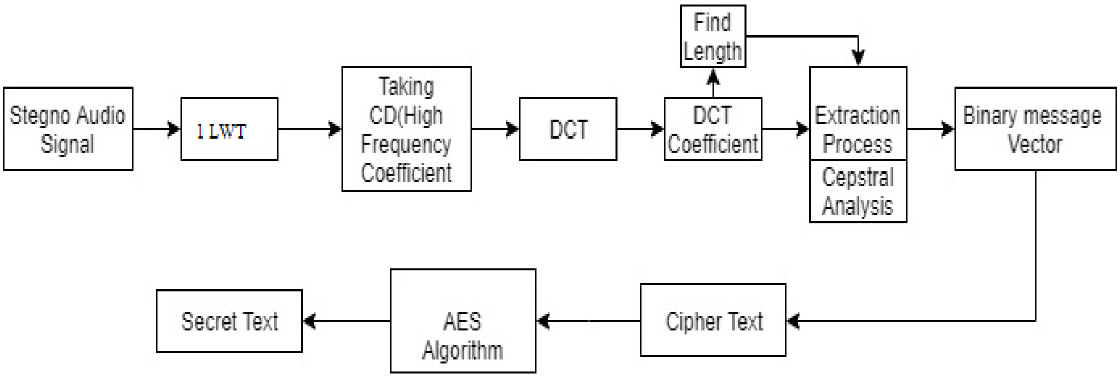


Figure 8 Decoder Implementation

This binary message vector is converted into the decimal values. These decimal values are converted to ASCII characters also called ciphertext. These ASCII values are used as input for the AES algorithm.

6.3 Decryption

The cipher text or ASCII values obtained from the decoder are used as input for the decryption process in the AES algorithm shown in figure 6. The Same key is used for decryption as used in encryption. The data is converted to ASCII of int64. Key for encryption is used and all encryption steps are performed form bottom to up as shown in figure 3.
Thus, secret text is obtained from AES decryption.

7 Evaluation

The stegno audio signal is evaluated to get the quality of steganography based on parameters like PSNR, MSE and SNR. The elapse time for whole encoding and decoding process is calculated for speed of process.

7.1 Case Study 1

The text size of 0.18 is embedded using the echo hiding after encryption in audio 1 and PSNR, MSE and SNR values are 59.9365, 1.51833e^{-06} and 47.7626. Figure shows the spectrogram variation before and after embedding.

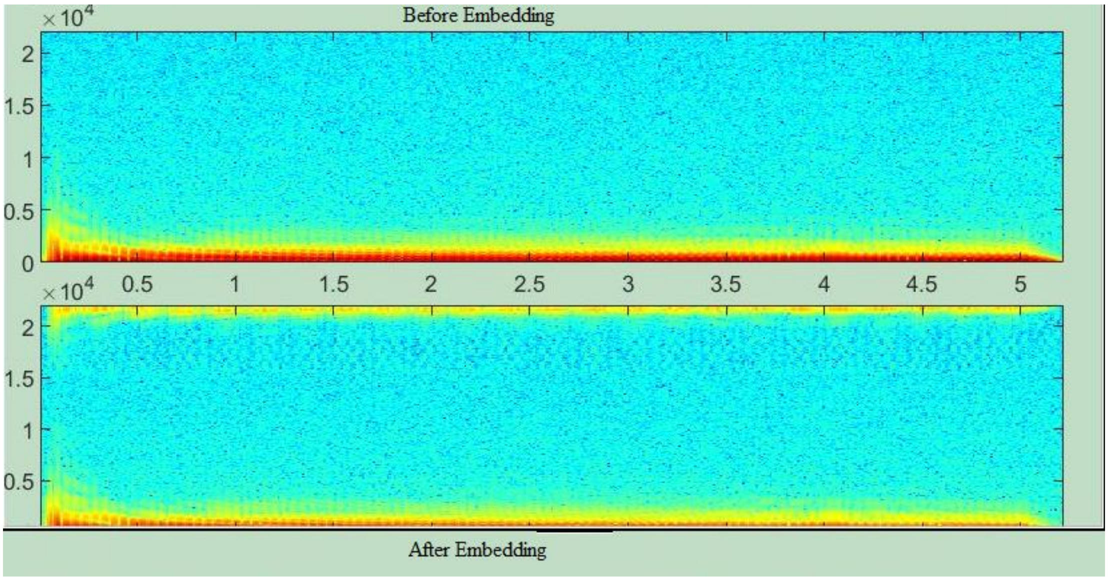


Figure 9 Cover Spectrogram for Audio 1

7.2 Case Study 2

The text size of 0.18 kb is embedded in the audio 2 and PSNR, SNR and MSE recorded are 44.2568, 0.00014877 and 27.8958. The figure shows the spectrogram variation.

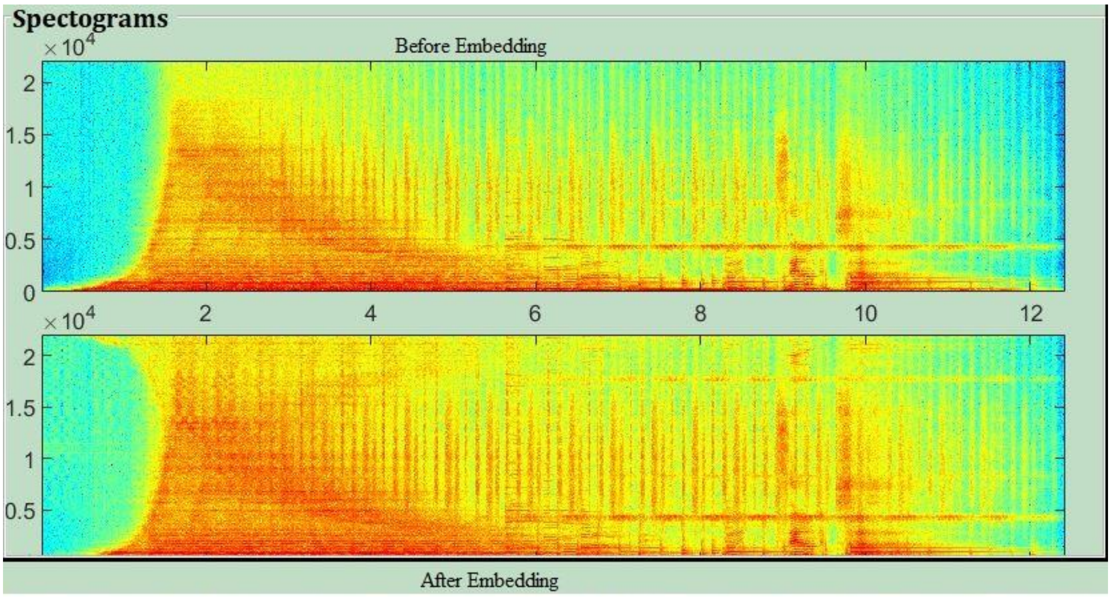


Figure 10 Cover Spectrogram for Audio 2

7.3 Discussion

The test case results have been recoded below with different text size along with corresponding PSNR, MSE and SNR. Higher PSNR and SNR values indicate better quality and low MSE value shows less errors. The experiment was done with 2 different types of echo hiding with same text size and audio samples. The results are shown in table 3 and 4.

Text Size (KB)	Audio	Capacity of CD (bits)	PSNR	MSE	SNR	Encoding Time(sec)	Decoding Time(sec)
0.18	Audio 1	115409	59.9365	1.51833e^{-06}	47.7626	0.5564	0.4431
0.18	Audio 2	274263	44.2568	0.00014877	27.8958	1.4484	0.5043

Table 3 Test Case values for Bipolar Forward and Backward Echo Hiding.

Text Size (KB)	Audio	Capacity of CD (bits)	PSNR	MSE	SNR	Encoding Time(sec)	Decoding Time(sec)
0.18	Audio 1	115409	58.1249	5.04112e^{-07}	44.351	0.66393	0.36757
0.18	Audio 2	274263	42.9588	5.03867e^{-05}	26.5978	1.1360	0.3952

Table 4 Test Case Results for Backward-Forward Echo Hiding.

Text Size (KB)	Audio	Capacity of CD (bits)	PSNR	MSE	SNR	Encoding Time(sec)	Decoding Time(sec)
0.18	Audio 1	115409	58.7002	5.06983e^{-07}	45.5264	0.928183	0.544499
0.18	Audio 2	274263	43.1726	4.79661e^{-05}	26.8116	1.01854	0.46752

Table 5 Test Case Results for Bipolar Echo Hiding.

The change in the PSNR, SNR values can be observed with change in the sample audio signal. It can be clearly seen the LWT-DCT with bipolar Forward-Backward echo hiding gives better results compared to Bipolar and Forward-Backward echo Hiding. With the change in text size PSNR and MSE values also change. Lesser the text size higher the PSMR and MSE values.

8 Conclusion and Future Work

The exchange of the simple text is not secure and can easily be intercepted. To make the text exchange secure a hybrid model of cryptography and steganography is proposed. The echo hiding embedding schema is used which provides the robustness against the transmission noise in contrast to the other techniques. Bipolar Forward-Backward kernel for embedding is used which has most robustness as compared to other kernels. The kernel is combination of the Bipolar and forward-backward kernel. Moreover, embedding in the transform domain with a hybrid model of LWT-DCT provides better compression, reconstruction of signal, Imperceptibility and extraction of the text. The text encryption using the AES algorithm promises the data confidentiality if key is kept safe. Here three-layer protection model is proposed for secure transmission of data. Even if intruder breaks one level security, other level keeps the data safe.

The approach is evaluated by PSNR, MSE and SNR values. The technique was successfully able to embed and extract the text with average PSNR, SNR and MSE values. The change of values is observed with change in carrier signal. The better values of PSNR and SNR were observed with Bipolar backward- forward echo hiding than bipolar and backward- forward echo hiding. The text size has reverse effect on the values large text size has lower PSNR and SNR.

With advancement in modern technology new threats are coming up and confidentiality gets breached by the intruders. With the help proposed technique text data can be sent securely over the internet. In future the technique would be tested with more suited echo hiding parameters for even better results. For evaluation more parameters will be added for accuracy. The paper is only for the text data, other kinds of data will be transmitted by hiding in the audio file.

References

Abood, O.G., Guirguis, S.K., 2018. A Survey on Cryptography Algorithms. Int. J. Sci. Res. Publ. IJSRP 8. https://doi.org/10.29322/IJSRP.8.7.2018.p7978

Delforouzi, A., Pooyan, M., 2007. Increasing Payload of Echo Hiding Scheme Using Dual Backward and Forward Delay Kernels, in: 2007 IEEE International Symposium on Signal Processing and Information Technology. Presented at the 2007 IEEE International Symposium on Signal Processing and Information Technology, pp. 375–378. https://doi.org/10.1109/ISSPIT.2007.4458194

Gupta, G., Khunteta, A., 2017. Hiding text data in image through image watermarking using DCT DWT: A research paper, in: 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). Presented at the 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), pp. 447–450. https://doi.org/10.1109/ICPCSI.2017.8392335

Hashim, J., Hameed, A., Abbas, M.J., Awais, M., Qazi, H.A., Abbas, S., 2018. LSB Modification based Audio Steganography using Advanced Encryption Standard (AES-256) Technique, in: 2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS). Presented at the 2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), pp. 1–6. https://doi.org/10.1109/MACS.2018.8628458

Jain, M.P., 2013. Effective Audio Steganography by using Coefficient Comparison in DCT Domain. Int. J. Eng. Res. 2, 7.

Jonna, 2019. dbossnirvana/AES_MATLAB.

Kabra, R.G., Agrawal, S.S., 2016. Robust embedding of image watermark using LWT and SVD, in: 2016 International Conference on Communication and Signal Processing (ICCSP). Presented at the 2016 International Conference on Communication and Signal Processing (ICCSP), pp. 1968–1972. https://doi.org/10.1109/ICCSP.2016.7754516

K.P., S., S., K.K., 2009. Extended Bipolar Echo Kernel for Audio Watermarking, in: 2009 International Conference on Advances in Recent Technologies in Communication and Computing. Presented at the 2009 International Conference on Advances in Recent Technologies in Communication and Computing, pp. 487–489. https://doi.org/10.1109/ARTCom.2009.131

Lahiri, S., 2016. Audio Steganography using Echo Hiding in Wavelet Domain with Pseudorandom Sequence. Int. J. Comput. Appl. 140, 16–22. https://doi.org/10.5120/ijca2016909223

Lau, N., 2017. nick1au/AES-MATLAB.

Matsumoto, T., Sonoda, K., 2015. Audible Secret Keying for Time-Spread-Echo Based Audio Watermarking, in: 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP). Presented at the 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 164–167. https://doi.org/10.1109/IIH-MSP.2015.112

Meligy, A., Nasef, M., Eid, F., 2015. An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys. Int. J. Comput. Netw. Inf. Secur. 7, 24–29. https://doi.org/10.5815/ijcnis.2015.07.03

Panyavaraporn, J., Horkaew, P., 2018. DWT/DCT-based Invisible Digital Watermarking Scheme for Video Stream, in: 2018 10th International Conference on Knowledge and Smart Technology (KST). Presented at the 2018 10th International Conference on Knowledge and Smart Technology (KST), pp. 154–157. https://doi.org/10.1109/KST.2018.8426150

(PDF) A REVIEW AND COMPARISON OF STEGANOGRAPHY TECHNIQUES [WWW Document], n.d. URL https://www.researchgate.net/publication/330162221_A_REVIEW_AND_COMPARISON_OF_STEGANOGRAPHY_TECHNIQUES (accessed 12.9.19).

(PDF) Review of Transform Domain Techniques for Image Steganography [WWW Document], n.d. URL https://www.researchgate.net/publication/287210148_Review_of_Transform_Domain_Techniques_for_Image_Steganography (accessed 12.9.19).

Performance analysis of DCT and DWT audio watermarking based on SVD - IEEE Conference Publication [WWW Document], n.d. URL https://ieeexplore.ieee.org/document/7530129 (accessed 12.9.19).

Preet, C., Aggarwal, R.K., 2017. Multiple image watermarking using LWT, DCT and arnold transformation, in: 2017 International Conference on Trends in Electronics and Informatics (ICEI). Presented at the 2017 International Conference on Trends in Electronics and Informatics (ICEI), pp. 158–162. https://doi.org/10.1109/ICOEI.2017.8300908

Priyanka, B.G., Sathyanarayana, S.V., 2014. A steganographic system for embedding image and encrypted text, in: 2014 International Conference on Contemporary Computing and Informatics (IC3I). Presented at the 2014 International Conference on Contemporary Computing and Informatics (IC3I), pp. 1351–1355. https://doi.org/10.1109/IC3I.2014.7019666

Saleem, S., Thomas, A., Mathew, D., 2017. Secure reversible data hiding in color images using LWT and hyper chaotic encryption, in: 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT). Presented at the 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), pp. 1385–1389. https://doi.org/10.1109/ICICICT1.2017.8342772

Semwal, P., Sharma, M.K., 2017. Comparative study of different cryptographic algorithms for data security in cloud computing, in: 2017 3rd International Conference on Advances in Computing,Communication Automation (ICACCA) (Fall). Presented at the 2017 3rd International Conference on Advances in Computing,Communication Automation (ICACCA) (Fall), pp. 1–7. https://doi.org/10.1109/ICACCAF.2017.8344738

spectrogram (Signal Processing Toolbox) [WWW Document], n.d. URL http://matlab.izmiran.ru/help/toolbox/signal/spectrogram.html#:~:targetText=spectrogram%20computes%20the%20short%2Dtime,the%20input%20signal%20vector%20x%20. (accessed 12.9.19).

Tabara, B., Wojtuń, J., Piotrowski, Z., 2017. Data hiding method in speech using echo embedding and voicing correction, in: 2017 Signal Processing Symposium (SPSympo). Presented at the 2017 Signal Processing Symposium (SPSympo), pp. 1–6. https://doi.org/10.1109/SPS.2017.8053697

Tekeli, K., 2019. ktekeli/audio-steganography-algorithms.

Tekeli, K., Aşlıyan, R., 2017. A COMPARISON OF ECHO HIDING METHODS. Presented at the The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (2602-3199), pp. 397–403.

Tewari, T., Saxena, V., Gupta, J., 2014. A digital audio watermarking scheme using selective mid band DCT coefficients and energy threshold. Int. J. Speech Technol. 17. https://doi.org/10.1007/s10772-014-9234-8

Torvi, S.D., ShivaKumar, K.B., Das, R., 2016. An unique data security using text steganography, in: 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom). Presented at the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 3834–3838.

What is Cryptography? | Cryptographic Algorithms | Types of Cryptography, 2018. . Edureka. URL https://www.edureka.co/blog/what-is-cryptography/ (accessed 12.9.19).