

Empirical Analysis of Text Embedding Algorithms in Audio Files: A Proposed Strategy

Rusul Ali Radhi¹^{*}, Haitham Maarouf¹

¹Modern University for Business and Science, Beirut, Lebanon.

*Corresponding Author: Rusul Ali Radhi

DOI: <https://doi.org/10.55145/ajest.2024.03.01.005>

Received June 2023; Accepted August 2023; Available online September 2023

ABSTRACT: Security has become one of the main tasks to maintain the safety of transmitted or stored information. Text encryption is one of the essential tools for text hiding. On the other hand, steganography coding is an effective tool to increase the security. This paper presents a proposed security which combine with a hiding technique for an important text with a selected audio. The encryption file hiding by phase coding in compressed audio. Such procedure aims to increase security and reduce overall transmitted data. As a result, the hiding and showing processing may affect the selected audio and lose some spectral data. To address this problem, an enhancement based on the Wiener filter is deployed to re-extract the original audio after decompression in the received file. The results, show that high security with achieved by obtaining the hidden text and complete audio spectral data of used audio and proposed system achieved an improvement in encryption, compression, and masking at the same time.

Keywords: Cybersecurity, Caesar cipher, DCT Compression, Phase Coding Stenography



1. INTRODUCTION

Security means to the laws taken to protect something of value from harm, damage, theft, or anything else from malicious activity. In the activity of electronic governance and information activity [1][2]. Security refers to protecting computer systems, networks, and data from unauthorized access, use, disruption, and destruction [3]. Modern cryptographic algorithms are laws and regulations. Encryption algorithms are designed on mathematical principles and are usually characterized by their efficiency and ease of implementation. Modern cryptographic algorithms are constantly evolving to meet the increasing security needs of modern applications. On the other hand, cryptographic algorithms are usually combined with other technologies. To ensure security from attacks for the system [4]. The encryption technique may be a powerful distortion for some audio components because of the heading, leading to the loss of some information. To address this issue, an enhancement method must be involved to compensate for the damaged part of the audio components [5]. Similarly, data compression is an important technique to reduce the amount of information, including voice, video, image, and text. Such a method reduces the storage size and improves the communication system, which becomes faster and more accessible [6]. Private information can be put inside an audio file utilizing the technique of audio steganography. Early audio steganography techniques employed the human auditory system (HAS) to transmit hidden messages. Regardless, more sophisticated statistical steganalysis techniques, like the ones in, have recently been made available. Three critical needs (embedding capacity, transparency, and robustness) must all be met simultaneously in audio steganography, which is the main issue [7]. The term "speech enhancement" explains techniques that can be utilized to enhance voice communication system performance, boost intelligibility, and lessen hearing fatigue caused by noisy speech [8].

2. LITERATURE REVIEW

Usman et al., [9] have suggested an updated image steganography strategy for protecting medical data. Before integrating the payload into the cover image, lossless compression and many levels of encryption are applied to it utilizing swapped Huffman tree coding. The secret data is also exclusively embedded in the cover image's edge regions,

offering strong imperceptibility. The findings demonstrate that the proposed strategy assures patient information confidentiality and secrecy while retaining imperceptibility. Sadkhan et al., [10] have proposed sound steganography is a variety of techniques used to conceal a hidden message (sound or anything else) in an audio cover file. These techniques used digital audio formats, including WAV, MP3, and AU. The findings demonstrated that most research employed LSB to incorporate hidden messages but with alternative encryption systems for LSB family strength. Others altered LSB to create a better technique. Studies generally focus on widely used techniques or how to combine them to develop new, effective strategies. Most studies lacked one or more of the measures of robustness and invisibility. Kapoor and Kapil [11] advanced combining cryptography and steganography have proven to be effective. Covertly convey text data within an audio recording. Metrics including PSNR, MSE, and SNR, have been used to evaluate the technique. Suggests echo hiding with the same text size and audio samples. The results show that changes in the PSNR and SNR values can be observed with the sample audio signal change. Test Case values for Bipolar Forward and Backward Echo Hiding are text size (KB) 0.18 capacity of CD (bits) 115409 PSNR 59.9365 MSE 1.51833e-06 SNR 47.7626 encoding time(sec) 0.5564 decoding time(sec) 0.4431. Test Case Results for backward-forward Echo Hiding is PSNR 58.1249 MSE 5.04112e-07 SNR 44.351 Encoding Time(sec) 0.66393 decoding time(sec) 0.36757. Test case results for Bipolar Echo Hiding are PSNR 58.7002 MSE 5.06983e-07 SNR 45.5264 encoding time(sec) 0.928183 decoding time(sec) 0.544499. It can be clearly seen that LWT-DCT with bipolar forward-backward echoes hiding gives better results compared to bipolar and forward-backward echo hiding. Lesser the text size higher the PSNR and MSE values. In [12] have indicates that the Vigenère and Caesar cypher designs are given. Block 4 offers strong encryption capabilities and programming efficiency. Using the suggested method for S-box chain chaos design, a very high level of safety is offered. Due to the suggested method's minimal resource usage, the implementation's results demonstrate its suitability for lightweight cryptography. This study employs a different expansion technique to enhance the information lurking in photos. Besides, it intends to incorporate S-block, probabilistic, and data-hiding techniques. In order to explain the goal of S-block-based data hiding, reflect recent developments, and bring attention to specific research challenges for the future, the thesis also presents a study of reversible S-block-based data concealing strategies that have been developed so far. This paper hypothesizes that combining steganography and cryptography can result in a robust security application. The application uses the development of both skills to create a powerful cross-platform application that can be used for high-security and protection requirements for files and data. In a study conducted by Timothy et al.[13], have sought to offer a solution for creating a reliable and effective audio steganography system to protect the information, whether in storage or being sent through the Internet. The Signal to Noise Ratio (SNR) results of the designed system's performance evaluation show minimal distortion. The resultant compression ratio is similarly one (1), demonstrating that the cover audio file and the resulting stego file are identical.

3. MODELS

In this paper, it has been to embedding encryption text in a compress audio. There are three steps in this paper namely, DCT algorithm to compress audio, encryption text by caser method, and steganography encryption text to audio compression by phase coding. The block diagram of the procedure for the proposed method is shown in figure 1. Firstly, it has been using a text of various size by adding 10 bytes for each step. The text is small letter and spaces. Such text will be encrypted and hidden. The chosen text has been encrypted using Caesar algorithm. On the other hand, the audio will be used as a various size, it was chosen randomly with a size of 156 KB, 2.15 MB, 4.37 MB and 8.74 MB. Each one is compressed using DCT algorithm. To hide the encrypted text, it has been used phase coding to hide it with compressed audio. The phase coding will be produce a stego audio which will be send as a signal.

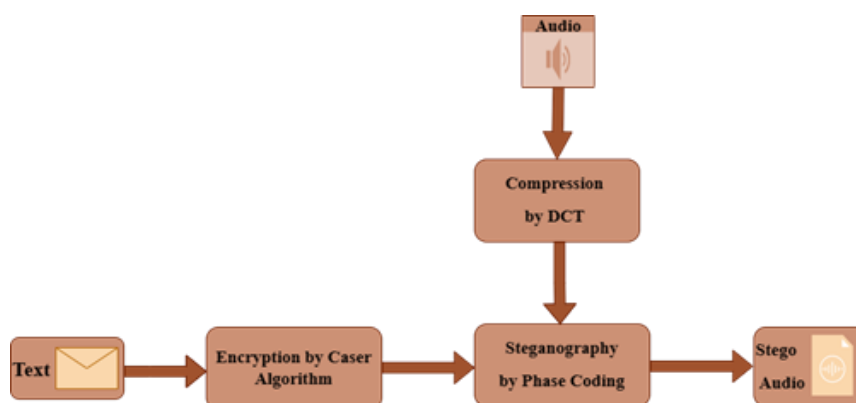


FIGURE 1. - The block diagram of proposed Embedding

At the received side, the stego audio will be feeds to the extracting block to achieve the compress audio. Such audio will be decompressed to reconstruct the original audio. The extracted text will be decrypted by caser method to

produce the original text as shown in the block diagram 2-(a). It is worth to mention, the decompressed audio may be loss some spectral components. To address this problem, wiener filter is used to enhance the weak audio to re-extract the original audio as mentioned in block diagram 2-(b).

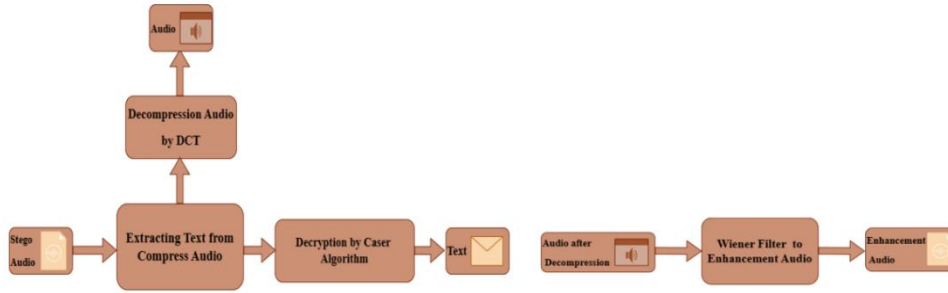


FIGURE 2. - (a): The block diagram of proposed Extracting. (b): The block diagram of proposed Enhancement Audio

3.1 COMPRESSION ALGORITHM

Data is transmitted within groups of text, audio, images, and video. Big data requires longer and larger storage spaces on the network. The compression process reduces data, time, and network bandwidth. compression algorithm is divided in to two main categories, lossy and lossless. This paper concentrate on lossy compression. These two technologies reduce the cost of storage, but lead to a loss of sound quality [14, 15]. Lossy algorithm is one of the compression techniques used that compresses audio data in order to reduce the cost of storage. This is called irreversible compression, as this technique leads to a loss sound quality. Compressed data requires less bandwidth to transfer it through devices or the Internet. These are used on a large scale as broad as Amazon prim, Netf4lix, VoIP or dial-up via the Internet [14]. There are some techniques of lossy compression, the most important techniques used is DCT. It uses a set of perfect sine functions at different frequencies to represent the energy compression data. It is suitable for using lossy compression (sound and image processing) in audio. Low-frequency data is concentrated. This technique is applied to blocks of audio. The central equation of a one-dimensional DCT is defined by the equation given the equation given as [16]:

DCT is described by the equations (1) & (2) as follows:

$$F(u) = \alpha(u) \sum_{i=1}^{N_p-1} \cos \left[\frac{\pi \cdot u}{2N_p} (2i + 1) \right] f(i) \dots \dots \dots (1)$$

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N_p}} & , u = 0 \\ \sqrt{\frac{2}{N_p}} & , \text{otherwise} \end{cases} \dots \dots \dots (2)$$

The inverse of equation (1) is:

$$f(i) = \alpha(u) \sum_{u=1}^{N_p-1} \cos \left[\frac{\pi \cdot u}{2N_p} (2i + 1) \right] F(i) \dots \dots \dots (3)$$

where $f(i)$ denotes discrete data sequence of signal and $i = 1, 2, \dots, N_p - 1$. The first transform coefficient, $F(0)$ is called the DC coefficient of the signal, which indicates the average value of the discrete sequence. In contrast, the remaining coefficients are called AC coefficients. Figure 3 displays audio compression and decompression using the DCT algorithm.

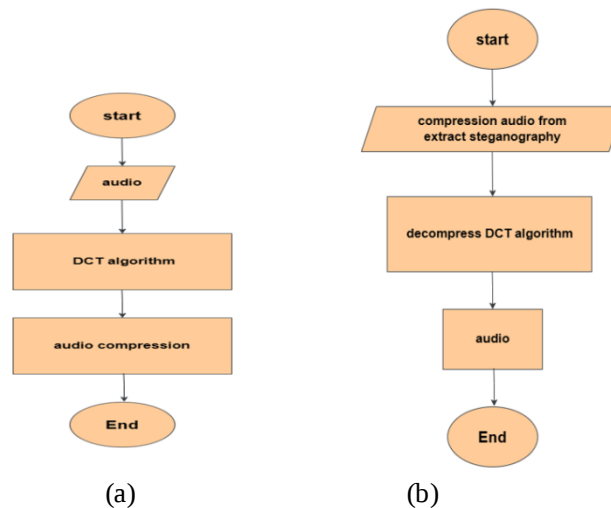


FIGURE 3. - DCT techniques (a) Compression (b) De compression

3.2 CAESAR CIPHER ALGORITHM

It is a crucial method of encoding and decoding in order to convert the original text into an unwanted encrypted text, such as when sending it over the Internet to the recipient. Given that the encryption operations are split into two main categories, symmetric key cryptographic algorithms like the caser cipher algorithm and asymmetric key cryptographic algorithms, show figure (4), the encrypted text is converted back to the original data during the decryption phase.

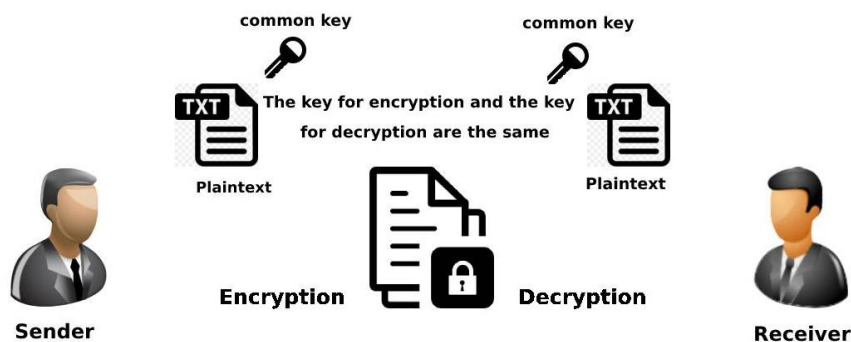


FIGURE 4. - Caesar Algorithm Symmetric key

The algorithm includes replacing a portion of the blades, and this algorithm is very simple, and the length of 26 was created by the Julius Caesar in, where it replaces each letter of the alphabet with another alphabet with another 26 length [17]. The encryption and decryption of cipher techniques can be representing the following equation:

$$\text{Encryption : } E(r) = r + K \text{ mod } 26 \dots\dots\dots (4)$$

$$\text{Decryption : } E(r) = r - K \text{ mod } 26 \dots\dots\dots (5)$$

Where K is the keyword used to shift each character (r) [17]. The caser method can be represented as flowchart shown in figure; caser method(5).

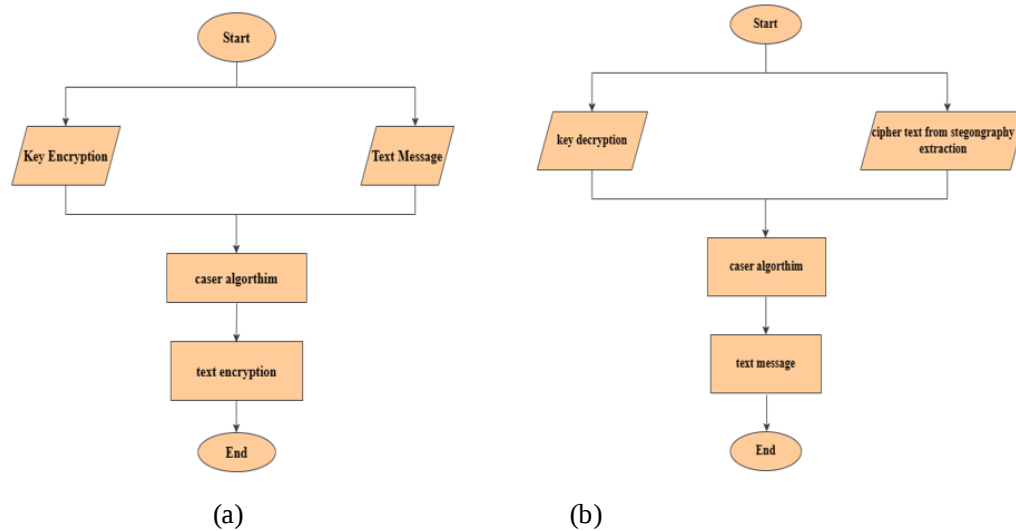


FIGURE 5. - Caser Method (a)Encryption (b)Decryption caser

3.3 PHASE CODING

In steganography, the message is hidden to appear invisible, because the cipher text message may raise suspicion, while the hidden message is more secure. Steganography uses audio signal modification to transmit a message that is concealed in the cover. Audio steganography is useful, so that anyone cannot distinguish between low voice and high voice. Image masking can be compared to sound masking. Audio files are relatively larger in size compared to the image format, so that they can accommodate a greater number of messages [19]. Phase coding works by replacing an initial audio segment with a reference phase that represents the data. Phase coding is the most efficient method in terms of perceived signal-to-noise ratio.

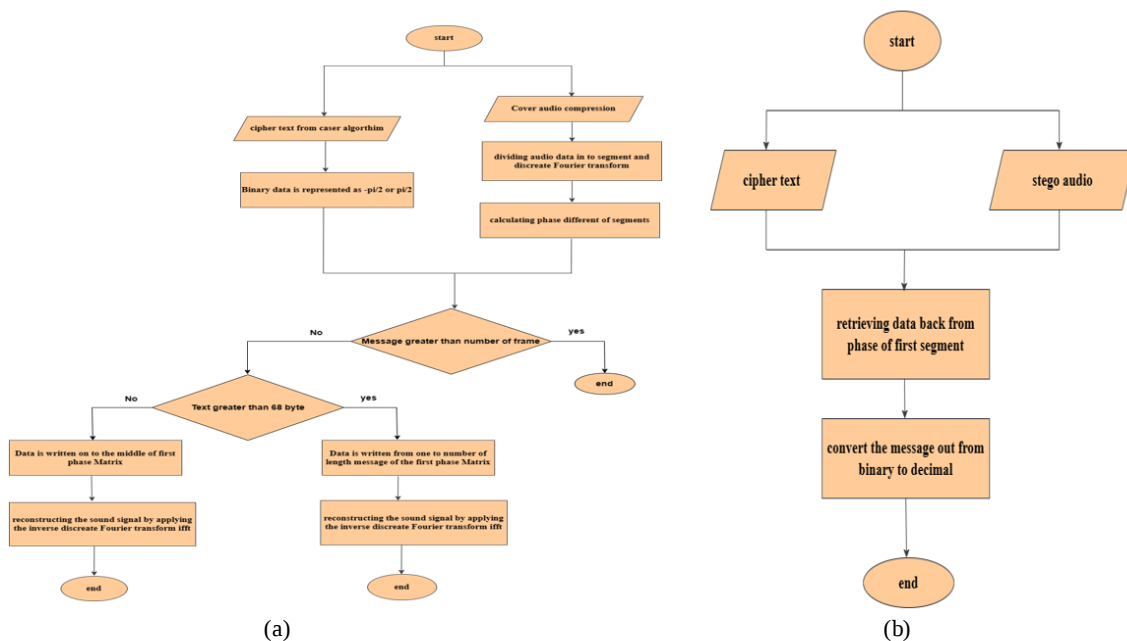


FIGURE 6. - Phase coding (a) Embedding (b)Extracting

The audio signal is broken down into segments with a signal length equal to the size of the bit to be encoded and Fast Fourier Transform (FFT) is applied to each segment to create a matrix of the phases and magnitudes, Store the phase difference between adjacent segments. Phase changes between successive segments can be quickly identified. To put it another way, while the segments, absolute phases can be altered, the relative phase disparities between neighboring segments must be maintained. As a result, just the following secret message is placed into the first signal segment's phase vector:

$$phase_new = \begin{cases} \frac{\pi}{2}, & \text{if message bit} = 0 \\ -\frac{\pi}{2}, & \text{if message bit} = 1 \end{cases} \dots\dots\dots(6)$$

A new phase matrix is created using the new phase of the first segment and the original phase differences. The audio signal is rebuilt by applying the IFFT and reconcatenating the audio segment. Stenography audio techniques is briefer phase coding is an effective and accurate way to hide the message in the audio file because it does not include many distortions other than phase shift [19]. procedure for phase coding is instruct in figure (6).

3.3.1 BIT ERROR RATE (BER)

Here, this tool is implemented by comparing the bit set of the original message with an extracted message from the decoder. So, this test is one of the criteria that must be considered in cryptographic research, and the value of BER in the extracted results is zero. Accordingly, the value of the bit error rate made is adequate.

$$BER = \left(\frac{l}{L}\right) * 100\% \dots\dots\dots(7)$$

In the extracted hidden information, l stands for the number of false bits, and L represents the total number of bits [21].

3.3.2 NORMALIZED CORRELATION (NC)

In order to test the robustness, the NC is operated to measure reliability. It measures the level of correlation encryption message embedded and the encrypted message extracted. The values of NC are between 0 and 1. The normalized coefficient can also be used to determine how similar the extracted hidden information objectively and the original hidden information are if this information is a matrix of $A \times B$. This procedure is implemented through Equation (8):

$$NC = \frac{\sum_{i=1}^A \sum_{j=1}^B W(i,j) w'(i,j)}{\sum_{i=1}^A \sum_{j=1}^B W(i,j)^2 \sqrt{\sum_{i=1}^A \sum_{j=1}^B W'(i,j)^2}} \dots\dots\dots(8)$$

Where $W(i,j)$ stands for the pixel value in the original hidden information and $W'(i,j)$ stands for the pixel value in the extracted hidden information[20].

3.3.3 PEAK SIGNAL TO NOISE RATIO (PSNR)

This test compares the quality of the compressed audio with that of the same audio after encryption and decryption. In this study, the testing was conducted PSNR on four compressed audios under different conditions, which can be calculated by Equation 9:

$$PSNR = 10 \log_{10} \frac{NX^2}{\|x - x'\|^2} \dots\dots\dots(9)$$

Where N is the length of reconstructed signal, X is the maximum absolute square value of signal x , and $\|x - x'\|^2$ is the level of the difference between the original and reconstructed signal[22].

4. WIENER FILTER ALGORITHM

The extracted audio signal from decompression process may be loss some data. To address this problem, wiener filter is one of the most frequently utilized tools in signal processing and enhancement. The Short Time Fourier Transform (STFT) is utilized in the time-frequency domain in audio, where signals are not steady but temporarily stationary[23]. Depending on the signal-to-noise ratio (SNR), short time noise reduction approaches in the algorithm are most frequently described as a spectral gain. The well-known decision directed (DD) strategy significantly reduces the amount of musical noise, but the predicted beforehand SNR is distorted since it depends on the previous frame's speech spectrum estimation. Due to the gain function being adjusted to match the previous frame rather than the current one, noise reduction is less effective. This bias has the unwelcome reverberation effect as a result. The two-steps noise reduction (TSNR) solution that we provide resolves this issue while preserving the advantages of the decision directed approach. In a further phase, the calculation of the a priori SNR is improved to eliminate the bias of the DD technique

and hence the reverberation effect. Nevertheless, because estimators for low signal-to-noise ratios are unreliable, traditional short-time noise reduction approaches, in clouding TSNR, create harmonic distortion in boosted speech. This is primarily because noise power spectrum density (PSD) estimation in single-microphone methods is a challenging task. We suggest a technique termed harmonic regeneration noise reduction to address this issue HRNR. The distorted signal's degraded harmonics are effectively recovered by the employment of nonlinearity. To improve the priori SNR required to calculate a spectral gain capable of preserving the speech harmonics, a fake signal is created [24-29]. The procedure of wiener filter used in this paper is shown in figure (7).

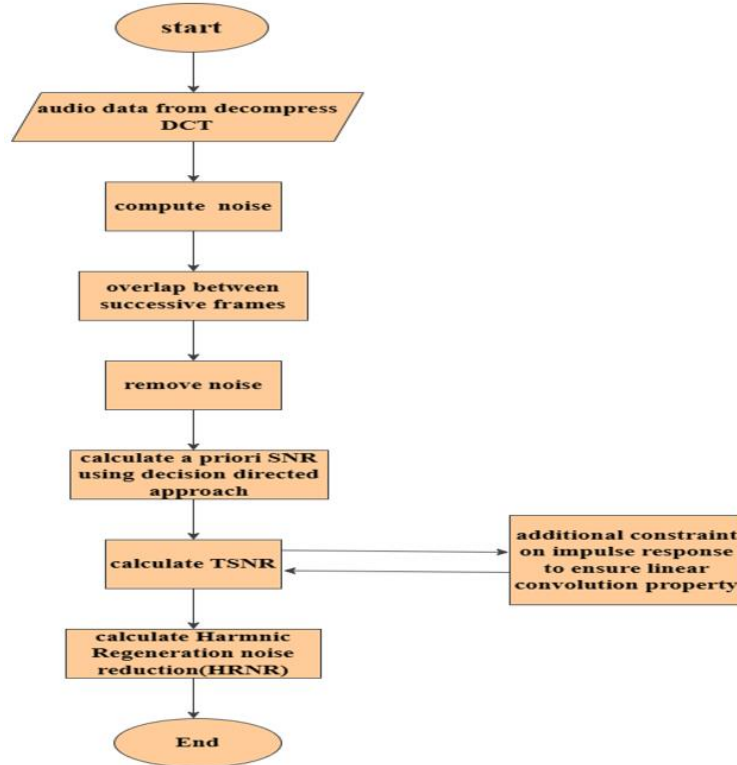


FIGURE 7. - Enhancement of Wiener Filter used

4.1 CORRELATION

The correlation function, it is possible to determine the correlation between two audio streams both before and after enhancement. Here's the equation (10) for calculating the cross-correlation function between two enhanced audio signals $x(n)$ and $y(n)$ with a lag of l :

$$R_{xy(l)} = \text{sum}(x(n) * y(n + l)) \dots \dots \dots (10)$$

Where the *sum* is taken over all values of n for which both $x(n)$ and $y(n + l)$ are defined[30].

4.2 EQUATION RATIO

This equation is provided calculates the ratio of the length of a message to the length of an audio signal, Specifically, equation (11) is organized as follows:

$$\text{ratio} = \left(\frac{Len_{\text{text}}}{Len_{\text{audio}}} \right) * 100 \dots \dots \dots (11)$$

Where Len_{text} is the length of the message in bits or bytes, and Len_{audio} is the length of the audio signal in bits or bytes. This can be valuable in applications of audio steganography, where a message is embedded inside an audio signal without seriously changing its perceptual quality.

5. RESULTS AND DISCUSSION

In this paper, it has been employed audio signals with various sizes of frequencies to encrypt a message. Message size ranges from 28 bytes to 128 bytes. The embedded text message from the following 28 bytes is “messa to be hidden in audio”, will a message size increase by 10 bytes for each step. Control increases by showing that BER results are not equal to zero, NC is not similar to one, or the message size is long from audio frames. The results show that in system, when increasing message size, PSNR are decreasing, text hidden inside compressed audio leads to increase noise so that less quality audio. The correlation equation is operated to measure the strength and direction of the relationship between the original sound and the sound after enhancement. Table 1,2,3 presents the message size of (18,28,38,48,58,68,88,98,108,118 and 128) bytes which are converted into decimal form listed in the second left-hand column. The following third column in table 1 shows the percentage ratio of message size to the audio frame size of 80000 within the audio size of 156 KB listed in the fourth column. The best quality for audio with a value of 156 KB, the value of the PSNR is 21.2085 when the message size is 68 bytes, but the lowest quality when the value of the PSNR is 16.7957 for the hide message of length 58 bytes. Subsequently, Table 2 shows the best quality for audio with a value of 2.15 MB, the value of the PSNR is 28.1565 when the message size is 68 bytes, but the lowest quality when the value of the PSNR is 23.1251 for the concealed message of length 58 bytes. Table 3 show that, the sufficient quality for audio with a value of 4.37 MB, the value of the PSNR is 31.4145 when the message size is 68 bytes, but the lowest quality when the value of the PSNR is 29.0855 for the concealed message of length 58 bytes. In order to measure the number of bit errors that occur in the stenography system as a percentage of the total number of bits sent and to measure the quality of the communication link, BER is utilized in the 156 KB audio when the audio cover is 80000. The message size ranges (18, 28, 38, 48, 58, 68, 88,98,108,118, and 128) bytes that all BER values are zeros. Likewise, NC is employed to evaluate the deterioration of signal quality. In some cases, BER and NS are connected, and Table 5 shows that the value of NC is one. Tables 1→3 exhibit effects similar to Table 1, with different parameters. The correlation equation is operated to measure the strength and direction of the relationship between the original sound and the sound after enhancement. Table 1 shows a beep size of 156KB. The weakest correlation is when the message size is 48 bytes, and the correlation value is 4.90E-01. Then, by Table 2, the volume is 2.15MB, which is the weakest correlation when the message size is 68 bytes, and the correlation value is 7.61E-01. While Table 3 shows that the volume is 4.37 MB, it is the weakest correlation when the message size is 78 bytes, and the correlation value is 9.92E-01.

Table 1.- The results of various text with an audio size of 156 KB

Text size(byte)			Audio size (156 KB)	Evaluation System			
				BER	NC	PSNR	Correlation
message size	message number in decimal	%	(Cover audio)				
18	192	2.40E-01	80000	0	1	20.2758	9.99E-01
28	280	3.50E-01	80000	0	1	18.9612	9.99E-01
38	360	4.50E-01	80000	0	1	18.0198	9.99E-01
48	392	4.90E-01	80000	0	1	17.5907	4.90E-01
58	472	5.90E-01	80000	0	1	16.7957	9.99E-01
68	552	6.90E-01	80000	0	1	21.2085	9.99E-01
78	640	8.00E-01	80000	0	1	20.229	9.99E-01
88	720	9.00E-01	80000	0	1	19.6647	9.99E-01
98	800	1.00E+00	80000	0	1	18.8983	9.99E-01
108	880	1.10E+00	80000	0	1	18.3134	9.99E-01
118	960	1.20E+00	80000	0	1	18.0595	9.99E-01
128	Error						

Table 2. - The results of various text with an audio size of 2.15 MB

Text size(byte)			Audio size (2.15 MB)	Evaluation System			
				BER	NC	PSNR	Correlation
message size	message number in decimal	%	(Cover audio)				
18	160	1.42E-02	1127424	0	1	28.0001	7.71E-01
28	232	2.06E-02	1127424	0	1	26.3803	8.16E-01
38	312	2.98E-02	1127424	0	1	24.4741	9.25E-01
48	392	3.48E-02	1127424	0	1	24.0215	9.60E-01
58	472	4.19E-02	1127424	0	1	23.1251	9.07E-01
68	552	4.90E-02	1127424	0	1	28.1565	7.61E-01
78	640	5.68E-02	1127424	0	1	27.2531	7.71E-01
88	720	6.39E-02	1127424	0	1	26.1801	8.59E-01
98	800	7.10E-02	1127424	0	1	25.498	8.99E-01
108	880	7.81E-02	1127424	0	1	24.9137	9.19E-01
118	960	8.51E-02	1127424	0	1	24.415	9.70E-01
128	Error						

Table 3. - The results of various text with an audio size of 4.37MB

Text size(byte)			Audio size (4.37 MB)	Evaluation System			
				BER	NC	PSNR	Correlation
message size	message number in decimal	%	(Cover audio)				
18	160	6.97E-03	2294240	0	1	31.3208	9.95E-01
28	232	1.01E-02	2294240	0	1	30.635	9.94E-01
38	312	1.71E-02	2294240	0	1	30.0319	9.98E-01
48	392	1.71E-02	2294240	0	1	29.5286	9.95E-01
58	472	2.06E-02	2294240	0	1	29.0855	9.98E-01
68	552	2.41E-02	2294240	0	1	31.4145	9.94E-01
78	640	2.79E-02	2294240	0	1	31.0615	9.92E-01
88	720	3.14E-02	2294240	0	1	30.7334	9.96E-01
98	800	3.49E-02	2294240	0	1	30.4207	9.97E-01
108	880	3.84E-02	2294240	0	1	30.1954	9.97E-01
118	960	4.18E-02	2294240	0	1	29.9359	9.95E-01
128	error						

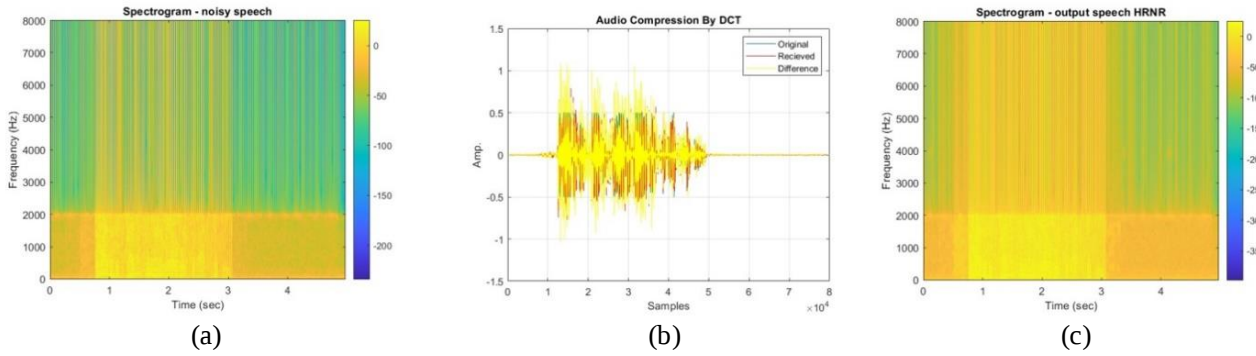


FIGURE 8. - (a) Noisy audio size 156 KB and text size 28 byte, (b) DC Tcompression audio size 156 KB and text size 28 byte, (c) Enhancement audio size 156 KB and text size 28 byte

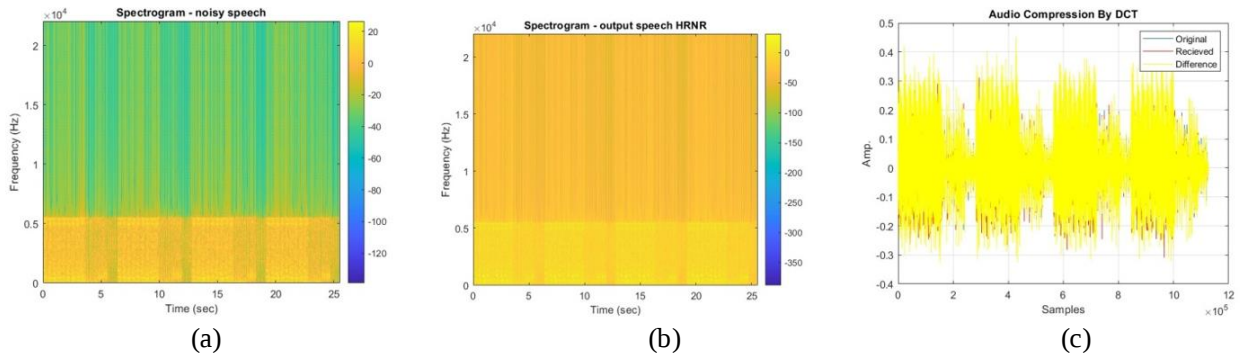


FIGURE 9. - (a) Noisy audio size 2.15 MB and text size 28 byte, (b) DC Tcompression audio size 2.15 MB and text size 28 byte, (c) Enhancement audio size 2.15 MB and text size 28 byte

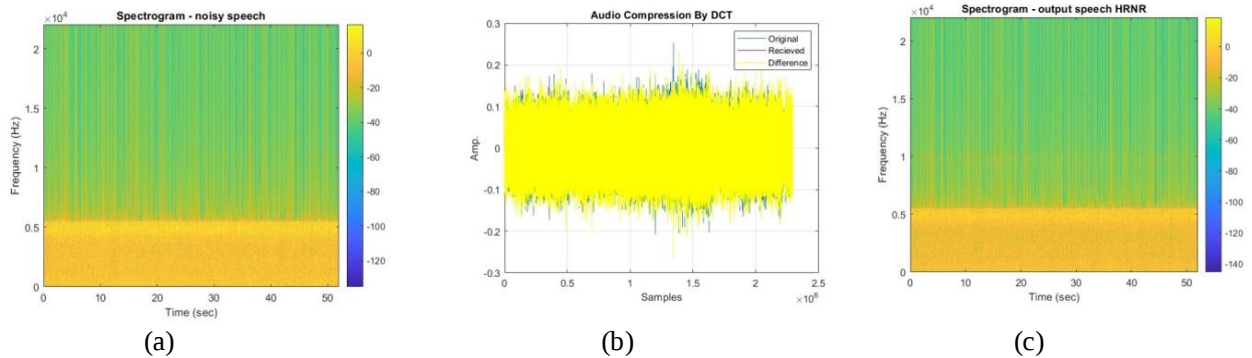


FIGURE 10. - (a) Noisy audio size 4.37 MB and text size 28 byte, (b) DC Tcompression audio size MB and text size 28 byte, (c) Enhancement audio size 4.37 MB and text size 28 byte

6. CONCLUSIONS

In this paper, the hidden process is deployed to increase security. This procedure is involved in this work to protect the selected text. The outcomes display that a message size between 18→118 bytes can be encoded and masked with various audio compression envelopes. The Caesar Cipher algorithm is utilized to encrypt text. This algorithm is straightforward. In this scenario, text consisting of lowercase letters and spaces with a maximum length of 118 bytes is entered. When the volume increases, the text volume increases. In the audio compression stage, the DCT algorithm removes redundant and unnecessary data and achieves high compression rates. This procedure can compress any audio size in kilobytes or megabytes. Phase coding is used to perform high data transfer rates through improved algorithms and is resistant to interference and noise. In order to enhance the quality of the audio extracted from the compression, the Winner filter algorithm is involved in reducing noise, improving the audio signal, and adding data to the signal. The system procedure can use various texts in order to secure a piece of important information and send it to anyone without understanding it from any third party. The outcomes show that the proposed work accomplished improved encryption, compression, and steganography simultaneously. In addition, the effect of compression and masking on

data quality must be considered. The reduction can lead to the loss of some information that may be adequate for the specific application. DCT audio is compressed, and several parameters can be optimized to enhance the compression ratio and audio quality, such as the number of frequency bands, the quantization level, and the coding system employed for the parameters or exchange using lossless algorithms. In order to use the phase coding algorithm, the carrier signal and phase coding method must be specified to ensure that the encoded signal can be easily retrieved at the receiver end. Likewise, the least significant bit (LSB) can be used for the down sampling phase.

FUNDING

No funding received for this work

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their efforts.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

- [1] A. Haider and A. Koronios, "Promises of Open Source Software for Australian Government Agencies – An Exploratory Study," in Assoc. for Information Systems (AIS) Electronic Library, Hyderabad, India, Jul. 10–12, pp. 1–9, 2009.
- [2] M. M. Mijwil, R. Doshi, K. K. Hiran, A. H. Al-Mistarehi, and M. Gök, "Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects," *Mesopotamian J. Cybersecurity** vol. 2022, pp. 1–4, 2022.
- [3] I. H. Sarker, H. Furhad, and R. Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," *SN Comput. Sci.*, vol. 2, no. 173, pp. 1–18, 2021.
- [4] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of internet of things based on cryptographic algorithms: a survey," *Wireless Netw.*, vol. 27, pp. 1515–1555, 2021.
- [5] M. Pill, "Towards a funding mechanism for loss and damage from climate change impacts," *Climate Risk Manage.*, vol. 35, p. 100391, 2021.
- [6] D. Pandey, S. Wairya, R. S. Al Mahdawi, S. A. M. Najim, H. A. Khalaf, et al., "Secret data transmission using advanced steganography and image compression," *Int. J. Nonlinear Anal. Appl.*, vol. 12, pp. 1243–1257, 2021.
- [7] A. H. Ali, L. E. George, and M. R. Mokhtar, "An Adaptive High Capacity Model for Secure Audio Communication Based on Fractal Coding and Uniform Coefficient Modulation," *Circuits, Syst., Signal Process.*, vol. 39, pp. 5198–5225, Apr. 2020.
- [8] V. R. Balaji, S. Maheswaran, M. R. Babu, M. Kowsigan, E. Prabhu, and K. Venkatachalam, "Combining statistical models using modified spectral subtraction method for embedded system," *Microprocess. Microsyst.*, vol. 73, p. 102957, 2020.
- [9] M. A. Usman and M. R. Usman, "Using image steganography for providing enhanced medical data security," in *IEEE Annu. Consum. Commun. Netw. Conf.*, Las Vegas, NV, USA, Jan. 12–15, 2018, pp. 1–6.
- [10] S. B. Sadkhan, A. A. Mahdi, and R. S. Mohammed, "Recent Audio Steganography Trails and its Quality Measures," in *Proc. Int. Conf. Computer Appl. Sci.*, Baghdad, Iraq, Dec. 18–19, 2019.
- [11] K. Kapoor, "Data Security with combination of Cryptography and Audio Steganography," in *MSc Project Submission Sheet*, pp. 1–20, 2019.
- [12] S. B. H. Hasan, "An application on combining of cryptography and steganography for improving security," in *Fen Bilimleri Enstitüsü*, pp. 1–84, 2019.
- [13] A. O. Timothy, A. A. Olusola, and G. A. Junior, "Embedding Text in Audio Steganography System using Advanced Encryption Standard, Text Compression and Spread Spectrum Techniques in Mp3 and Mp4 File Formats," *Int. J. Comput. Appl.*, vol. 177, no. 41, pp. 46–51, 2020.
- [14] M. A. Onabid, C. G. A. Otele, P. S. Assembe, and J. R. Takala, "Design and Implementation of an Automatic Deep Stacked Sparsely Connected Auto-Encoder (Adssca) Neural Network Architecture for Lithological Mapping Under Thick Vegetation Using Remote Sensing: A Case Study of Landsat-8 Images in Some Parts of the South Region of Cameroon," *SSRN*, pp. 1–39, 2022.
- [15] S. Rahmani, "Comparing Different Audio Compression Techniques," in *Proc. EasyChair Preprints*, pp. 1–5, 2020.

- [16] M. A. Almaiah, Z. Dawahdeh, O. Almomani, A. Alsaaidah, A. Al-Khasawneh, and S. Khawatreh, "A new hybrid text encryption approach over mobile ad hoc network," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 6, pp. 6461–6471, 2020.
- [17] K. Lapatin, "Buried by Vesuvius: The Villa dei Papiri at Herculaneum," *J. Paul Getty Museum*, vol. 1, pp. 1–276, 2019.
- [18] R. Hammad, K. A. Latif, A. Z. Amrullah, Hairani, A. Subki, et al., "Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message," *J. Phys.: Conf. Ser.*, vol. 2279, p. 012006, 2022.
- [19] M. Verma and H. S. Saini, "Analysis of various techniques for audio steganography in data security," *Int. J. Sci. Res. Netw. Secur. Commun.*, vol. 7, no. 2, pp. 1–5, 2019.
- [20] M. S. Yadnya, B. Kanata, and M. K. Anwar, "Using Phase Coding Method for Audio Steganography with the Stream Cipher Encrypt Technique," in *Proc. First Mandalika Int. Multi-Conf. Sci. Eng.*, 2022, pp. 66–75.
- [21] S. Masurkar and V. Dalal, "Enhanced Model For Detection Of Phishing URL Using Machine Learning," *Ethics Inf. Technol.*, vol. 2, no. 2, pp. 158–163, 2020.
- [22] Afnan, F. Ullah, Yaseen, J. Lee, S. Jamil, and O. Kwon, "Subjective Assessment of Objective Image Quality Metrics Range Guaranteeing Visually Lossless Compression," *Sensors*, vol. 33, no. 3, pp. 1–17, 2023.
- [23] M. Gogate, K. Dashtipour, A. Adeel, and A. Hussain, "CochleaNet: A robust language-independent audio-visual model for real-time speech enhancement," *Inf. Fusion*, vol. 63, pp. 273–285, 2020.
- [24] M. K. Singh, D. Lavanya, C. A. Madhuri, P. Ramesh, and V. Satyanarayana, "Improving Speech Quality Using Deep Neural Network-Based Manipulation of Cepstral Excitation," in *Recent Developments in Electronics and Communication Systems*, vol. 32, pp. 340–346, 2023.
- [25] M. M. Mijwil, M. Aljanabi, and ChatGPT, "Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime," *Iraqi J. Comput. Sci. Math.*, vol. 4, no. 1, pp. 65–70, 2023.
- [26] M. M. Mijwil, E. Sadıkoğlu, E. Cengiz, and H. Candan, "Siber Güvenlikte Yapay Zekanın Rolü ve Önemi: Bir Derleme," *Veri Bilimi*, vol. 5, no. 2, pp. 97–105, 2022.
- [27] M. M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview," *Mesopotamian J. Cybersecurity*, vol. 2023, pp. 57–63, 2023.
- [28] M. M. Mijwil, M. Aljanabi, and A. H. Ali, "ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information," *Mesopotamian J. Cybersecurity*, vol. 2023, pp. 18–21, 2023.
- [29] M. M. Mijwil, I. E. Salem, and M. M. Ismaeel, "The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review," *Iraqi J. Comput. Sci. Math.*, vol. 4, no. 1, pp. 87–101, 2023.
- [30] N. Phruksahiran, "Audio Feature and Correlation Function-Based Speech Recognition in FM Radio Broadcasting," *ECTI Trans. Electr. Eng., Electron., Commun.*, vol. 20, no. 3, pp. 403–413, 2022. doi: 10.37936/ecti-eec.2022203.247516.