ISSN 2348-375X

Unique Journal of Engineering and Advanced Sciences

Available online: www.ujconline.net

Research Article

# GENERAL FRAMEWORK TO REVERSIBLE DATA HIDING USING MODIFIED COEFFICIENT-BIAS ALGORITHM

Jadhav CM[1*], Dabane Sachin M[2]

[1]Professor, Department of Computer Science and Engineering, Bharat Ratna Indira Gandhi College of Engineering, Kegaon, Solapur, India
[2]M.E (Final Year), Department of Computer Science and Engineering, Bharat Ratna Indira Gandhi College of Engineering, Kegaon, Solapur, India

Received: 30-08-2014; Revised: 28-09-2014; Accepted: 26-10-2014

*Corresponding Author: **Prof. C. M. Jadhav**
Department of Computer Science and Engineering, Bharat Ratna Indira Gandhi College of Engineering, Kegaon, Solapur, India

## ABSTRACT

Principally the lossless reversible data hiding schemes are able to carryover up to 256 characters only. In this case the hole also well thought-out as a character. Since low data are only able to hide in an audio signal. There is no more proof for origin of the data in another node after broadcast through a communication channel. In a proposed system maximum characters are able to embed in an audio signal and a different frame work for hiding and extracting are provided at both end of the channel. A simple lossless data hiding method based on the modified coefficient-bias algorithm by embedding bits in both spatial field and frequency field is proposed. In spatial field, each pixel in a host audio signal is first subtracted from the block-mean. Then, a stego audio signal is generated by embedding a large amount of bits (or the primary message) in the mean-removed blocks via the modified coefficient-bias algorithm. To provide an extra security and robustness, the stego signal is transformed to frequency field by integer wavelet transform (IWT).The whole project is going to realize using MATLAB software.

**Keywords:** Reversible Data Hiding, Stego Audio Signal, Modified Coefficient-Bias Algorithm, Steganography, Low Bit Encoding.

## INTRODUCTION

Data hiding is also known as steganography. In contrast to cryptography, this focuses on rendering messages unintelligible to any unauthorized persons who might intercept them, the heart of steganography lies in devising astute and undetectable methods of concealing messages themselves. An obvious application is a covert communication using innocuous cover signals, like a telephone conversation or an image. Another application, known as (digital) watermarking, refers to embedding an unremarkable scratch into an object, which can be used to recognize the object. For example, a digital watermark can be inserted into a piece of music, so that radio and TV broadcasts can be monitored automatically for royalty payment purposes. Many other applications, such as piracy detection and/or prevention, proof of performance (e.g. monitoring time and duration of advertisement broad-casts), integrity confirmation (to detect tampering of a cover signal), traitor tracing, (e.g. to identify a source of a leak), transaction detection, automatic record, copy control, secondary information addition, etc., have been reported[2-5].

The express development of the Internet and the digital information revolution caused major changes in the overall society. Broadband Internet connections almost an errorless broadcast of facts helps people to share out large multimedia files and make identical digital copies of them. In modern communication system[6-8] data hiding is most essential for Network Security issue. Sending sensitive messages and files over the Internet are transmitted in an unsecured form but everyone has got something to keep in secret. Audio data hiding technique is one of the most efficient ways to defend your privacy[10-11, 19, and 20].

In today's world, the communication is the basic need of every growing area. Everyone needs the confidentiality and security of their conversing data. In our day to day life, we use many secure paths like internet or telephone for transferring and sharing information, but it is not safe at a definite level. In order to share the information in a secured manner two techniques could be used. These are cryptography and steganography. In cryptography, the message content is modified in an encrypted form with the help of encryption key which is known to sender and receiver only. This message cannot be accessed by anyone without using the encryption key. However, the transmission of encrypted message may

easily arouse attacker's suspicion, and the encrypted message may thus be intercepted, attacked or decrypted violently. In order to overcome the limitation of cryptographic techniques, steganography techniques have been developed.

Steganography covers the subsistence of information so that no one can detect its occurrence. The Figure 1 shows the process of steganography.

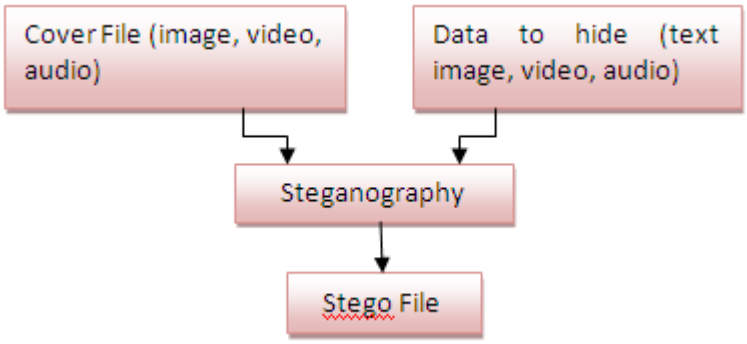


**Figure 1: Steganography Application Scenario**

Security of information is one of the most important factors of information technology and communication. Security of information often lies in the secrecy of its existence and/or the secrecy of how to decode it. Mainly there are two ways of concealing information: cryptography and steganography. Steganography differs from cryptography which is the art of secret writing, and is planned to create a message scribbled by a third festivity however does not hide the survival of the furtive message. Even though steganography is split and separate from cryptography, there are lots of similarities between the two, and some novelists classify steganography as a structure of cryptography since concealed communication is a shape of secret writing. Steganography conceals the hidden significance but not the truth that two parties are communicates with each other.

For both the one dimensional and two dimensional data, the Median filtering is widely used to remove the noises with the restriction while acquire and preserves edges for removing noise[12]. Steganography is an ancient art that encompasses a variety of data thrashing method, intend to implant a covert information into a carrier. Steganographic methods are aimed at hiding the very existence of the communication and therefore keep any third-party observers innocent of the occurrence of the steganographic substitute. Steganographic carriers have evolved through the ages and are related to the evolution of the methods of communication between people. Thus, it is not surprising that current telecommunication networks are a natural target for steganography and in particular, IP telephony is attracting the attention of the steganography research community. Various Technical Systemic processes, approaches, methodologies, techniques are used in various articles related to data security are published recently[4].

The basic biological process of controlling the color in an epithelial tissue by a tint unit, known as melanocytes is transformed here as a data hiding approach. The pixel pair mapping concept is used to select the pixel, randomly to embed the data bit in the RGB image. The main objective of the task is to enhance robustness, imperceptibility and increased capacity simultaneously. A new informed color image data hiding scheme with a minimum elapsed time complexity of 1.512x10-3sec at an information rate of 1/150 bit/pixel is proposed. While compare the proposed approach with conservative methods, the image idleness is oppressed, thereby implanting presentation is enhanced. The high image quality is preserved, due to slight variation in the pixel values[17].

**EXISTING WORK**

This section presents some common methods used for hiding secret information in audio. Many package realizations of those ways area unit offered on the online and area unit listed within the relatives section. A number of the latter ways want previous facts of signal process techniques, Fourier analysis, and different areas of high level arithmetic. once increasing a data-hiding technique for audio, one in every of the first reflections is that the doubtless environments the sound signal can travel between secret writing and decryption. There area unit two main areas of modification that we are going to take into account. First, the storage surroundings, or digital depiction of the signal that may be used, and next the transmission path the signal may travel[18].

**Parity coding**

One of the previous works in audio knowledge concealment technique is parity cryptography technique. Instead of breaking a symbol down into individual samples, the parity cryptography technique breaks a symbol down into separate regions of samples and encodes every bit from the key message in an exceedingly sample region's bit. If the bit of a specific region does not match the key bit to be encoded, the method flips the LSB of one of the samples within the region. Thus, the sender has a lot of of a selection in encryption the key bit, and also the signal is distorted in an exceedingly a lot of ordinary approach. Figure 2, shows the parity coding procedure.

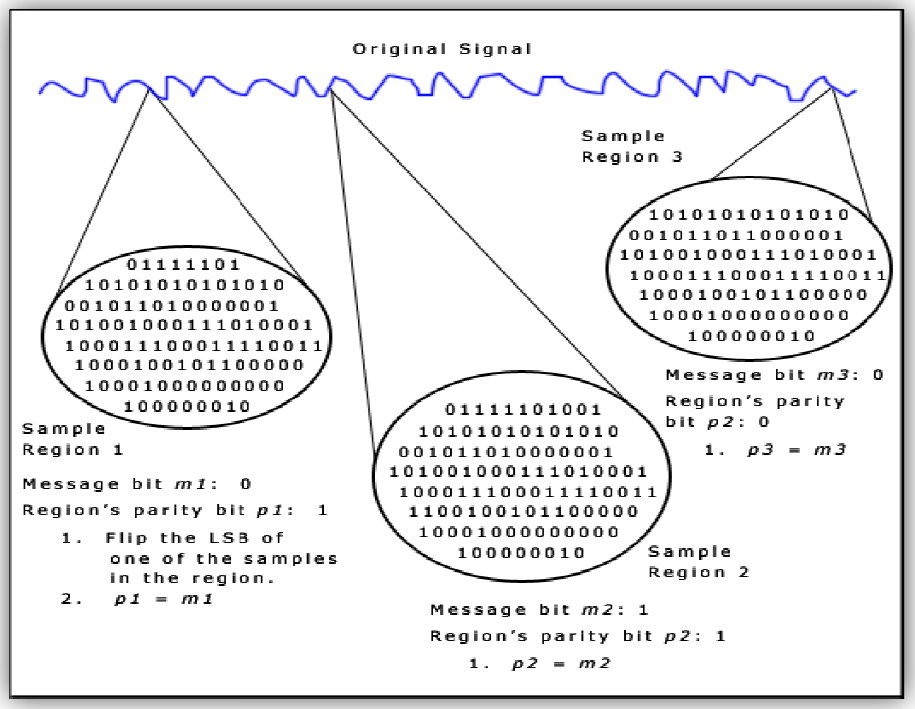


**Figure 2: Parity Coding Procedure.**

## Phase Coding

The phase coding method employs by alternating the phase of a preliminary audio section with a orientation phase that characterizes the data. The phase of succeeding segments is adjusted in order to protect the comparative phase between segments. Phase secret writing is one in every of the foremost prosperous secret writing strategies in terms of the signal-to perceived noise magnitude relation. Once the section relative between every incidence module is perceptibly altered, obvious section dispersion can occur. However, as long because the modification of the section is sufficiently little (sufficiently little depends on the observer; professionals in broadcast radio will notice modifications that area unit indiscernible to a typical observer), associate muted secret writing are often reached.

Phase coding relies on the reality that the phase apparatus of resonance are not as audible to the person ear as noise. To a definite extent than introducing perturbations, the method encodes the message bits as part moves within the part spectrum of a digital signal, achieving a muted cryptography in conditions of signal-to-perceived noise magnitude relation[5].

Phase coding is explained in the following:

- The unique sound signal is broken up into slighter sections whose lengths equivalent the size of the significance to be encoded.
- A Discrete Fourier Transform (DFT) is applied to every part, to create a matrix of the phases and Fourier transforms magnitudes.
- Phase differences between adjacent regions are designed.
- Phase shifts between successive segments are simply noticed. Therefore the secret significance is simply inserted in the phase vector of the first signal section as follows:

✓ A new phase matrix is shaped using the new phase of the primary division and the imaginative phase dissimilarities.

✓ Using the new phase environment and original scale matrix, the resonance signal is restructured by applying the converse DFT and then concatenating the sound fragments back simultaneously.

✓ To extract the secret communication as of the sound file, the recipient must recognize the fragment span. The recipient can afterward utilize the DFT to obtain the phases and obtain the information (consider Figure 3 for phase coding procedure).

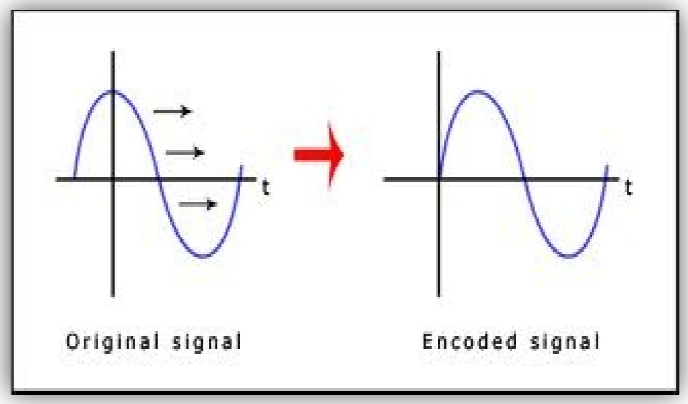


**Figure 3: The signals before and after Phase coding procedure.**

**PROPOSED WORK**

To outline our classification design, we have a tendency to should initial very state what our purpose that may acquire system performance at a similar one among our purpose is to construct an expertise, that is not solely distinctive to the (user) shopper, however additionally makes him feel that he has loyal attachment to the system and approaches us whenever he/she wants. To realize higher results and success by apply computerized method in its place of manual method. We have a tendency to square measure of the conviction that the best way to keep one thing from snooping eyes is to position it right ahead of the person craving for it and build it look as innocuous as possible. Everybody features a style for a kind of music. Hence, it is over probably that the person can have that sort of music on the device of his computer. Also, it is quite common case wherever individuals share and transfer totally different music files to at least one an extra. If one were able to hide the message will be. Also, transfer of this message will be done quite handily while not raising any eyebrows[13]. Our aim is to come back up with a way of activity the message within the audio come in such the simplest way, that there would be no perceivable changes within the audio file when the message addition. At a similar time, if the message that is to be hidden were encrypted, the extent of security would be raised to quite a satisfactory level. Now, even if the hidden message were to be discovered the creature making an attempt to induce the message would solely be able to lay his hands on the encrypted message with no way of having the ability to rewrite it [14].

**AUDIO STEGANOGRAPHY**

Audio steganography in audio signals is very exacting, as a result of the Human sensory system (HAS) operates over a large energetic vary. The HAS observes over a series of power superior than one billion to individual and a spread of frequencies bigger than thousand to at least one. Sensitivity to additive random noise is additionally acute. The perturbations in a very sound file are often detected as low jointly half in 10 million that is 80dB below close level. But there area unit some 'holes' accessible. Where as it is an outsized dynamic vary, it is a reasonably tiny differential vary. As a result, loud sounds tend to mask out the quieter sounds. To boot, the HAS is unable to understand absolute section, solely relative section. Finally there are some ecological distortions so common as to be unnoticed by the perceiver in most cases.

**LOW-BIT ENCODING**

Low-bit secret writing is that the one in every of the simplest way to enter information into different data structures. By commutation the smallest amount of every sampling spot by a coded twin string, we will cipher an oversized amount of knowledge in associate degree audio signal. Ideally, the channel capability is 1 KB per second (kbps) per 1kilohertz (kHz), e.g., during a quiet channel, the bit rate are eight kbps during an eight kilohertz sampled sequence and forty four kbps in a 44kHz sampled sequence. Reciprocally for this huge data rate, perceptible noise is introduced. The impact of this noise may be a direct operates of the content of the host signal, e.g., crowd noise throughout a live sports event would mask low-bit secret writing noise that will be simple to listen to during a string foursome presentation. Adaptive information attenuation has been wont to compensate this variation. the main advantage of this methodology is its poor immunity to manipulation. Encoded info may be destroyed by channel noise, re-sampling, etc., unless it's encoded mistreatment redundancy techniques. So as to be sturdy, these techniques scale back the information rate that may end in the need of a bunch of upper magnitude, typically by one to two orders of magnitude. In observe, this methodology is helpful exclusively in closed, digital-to-digital environments.

**STEGANOGRAPHY `MODULES AND THEIR DESCRIPTION**

Data hiding and extracting from an audio file is done in two main divisions.

- ✓ Data hiding part.
- ✓ Data extraction part.

**Data hiding part**

In this module, the primary step is choosing an input audio file. The choice is formed from facet to facet gap a replacement window and therefore the pathway hand-picked is displayed through a textbox. The second step is choosing AN output audio go into that text information or a computer file is embedded. The third step is selecting a computer file or writing any text message for embedding. Fourth step is choosing a key file. Within the fifth step regardless of the files that we have hand-picked area unit viewed and confirmation of the trail is completed. Within the sixth method information is embedded in to the audio file exploitation low bit encryption technique. When embedding the content each the audio files area unit contend and an auditor cannot notice any distinction between the audios.

In a data hiding, data significance is hidden within a cover signal (object) in the block called embeddor using a stego key, which is a secret set of parameters of a known hiding algorithm. The output of the embeddor is called stego signal (object). After transmission, recording, and other signal processing which may contaminate and bend the stego signal, the embedded message is regained using the appropriate stego key in the block called extractor. A number of different cover objects (signals) can be used to carry concealed messages in Figure 4. Data hiding in audio signals use flaw of human aural system known as audio masking. The human sound organism operates over a wide active range, so data hiding in the audio signal is a challenging one.

**Data extraction part**

In this module, the primary step is that the method of culling the encrypted audio file. this can be the file that a utiliser has got to extract data from the output audio. Second method concerned in culling associate degree early document to exhibit the embedded message. Symmetric cryptography methodology is used here, that the key culled throughout the embedding method is used in decrypting the message. The entire processes area unit exhibited utilizing a listing box and once and for all the embedded message may be viewed with the avail of a file or in an exceedingly textbox. The

human sensory system perceives over a variety of efficiency additional predominate than one billion to at least one and a variety of frequencies additional predominate than one thousand to at least one. Sensitivity to additive discretionary noise is all the same acute. The perturbations in an exceedingly sound file may be detected as low united half in 10 million (80 sound unit below close level).

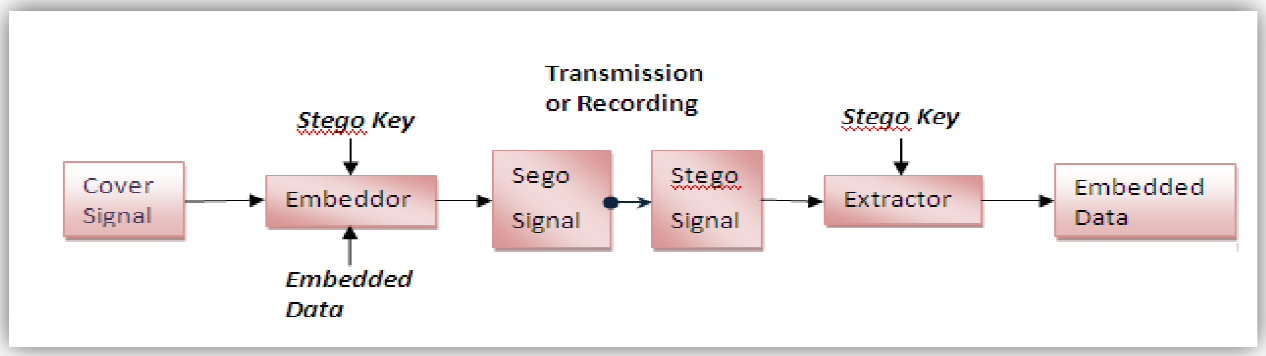


**Figure 4: Block diagram of encoding and decoding**

## MODIFIED COEFFICIENT-BIAS ALGORITHM

The idea of the modified coefficient-bias algorithm is to implant data bits in both spatial field and frequency field. That is, a stego signal is first generated by embedding the major message in the spatial field. Then, the stego-signal is decomposed to IWT domain for hiding the secondary Stego key. The schematic view of the proposed method steps are given in the following:

- ✓ A audio signal
- ✓ contains a covert message
- ✓ Contains stego key.
- ✓ The IWT field obtained from encrypted signal.
- ✓ A mixed signal contains a secret message and a stego key. According to both the stego key and the secret message would be lossless extracted and the host signal are completely re-established at receiver site. The details of the modified coefficient-bias algorithm are specified in the following sections.

In the transmitter section, First step is to enter the secret message to hide in the audio signal which is shown in the simulation output Figure 5, and also enter the secret key to hide the text. After enter the secret key select the wav file (audio file) to hide the secret message (see figure 6), then select 'Hide The Text' in the highlighted tab. Finally give exit. In receiver section, select the encrypted audio signal then enter the appropriate secret key in the 'key' box. After that select 'Display data', finally the hidden text in the audio signal where displayed in the command window, show in Figure 7 and Figure 8 respectively.

## RESULTS

**Transmitter Side:**

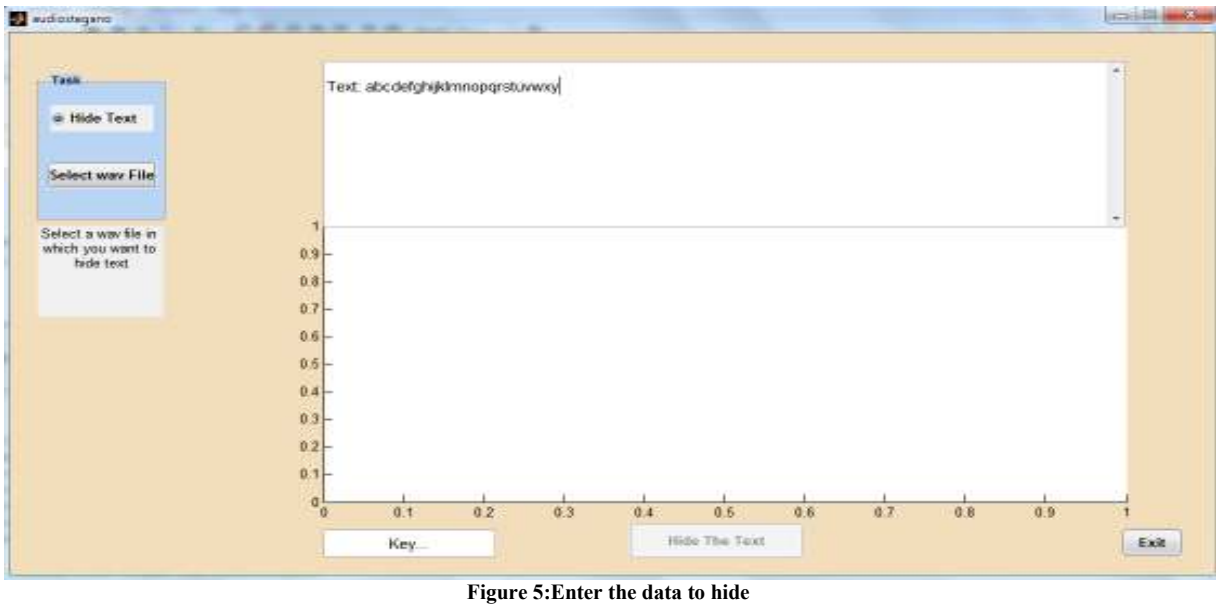


**Figure 5:Enter the data to hide**

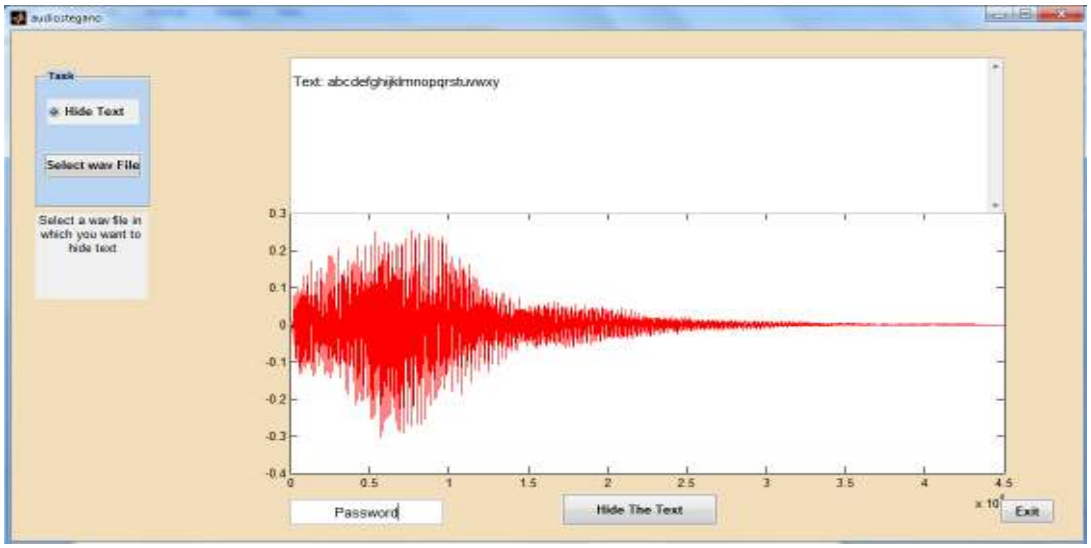


Figure 6: Select audio file

**Receiver Side:**

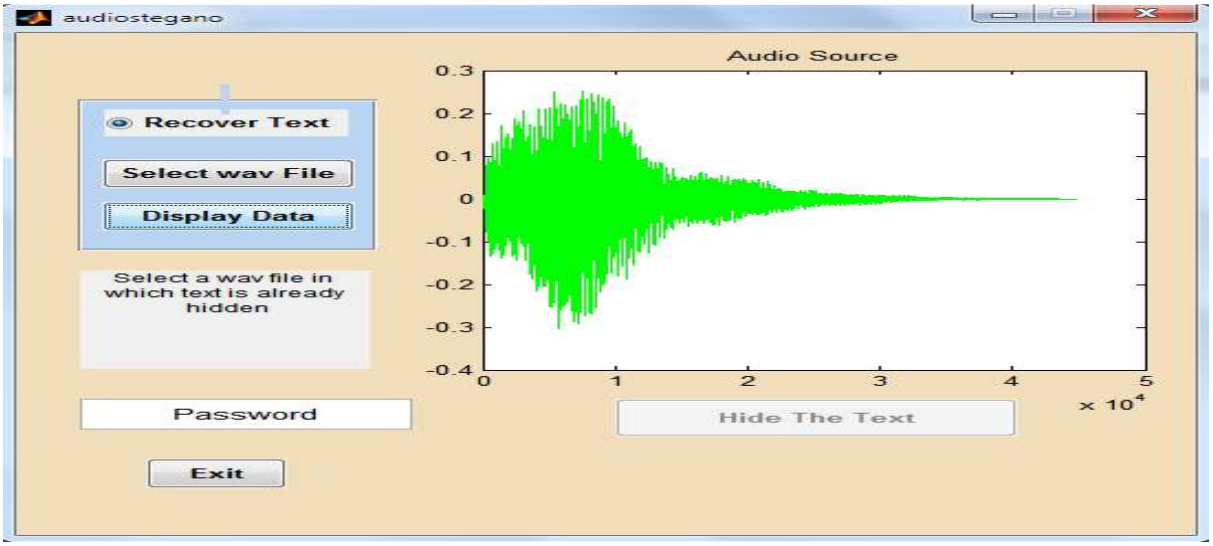


Figure 7:Select encripted audio signal

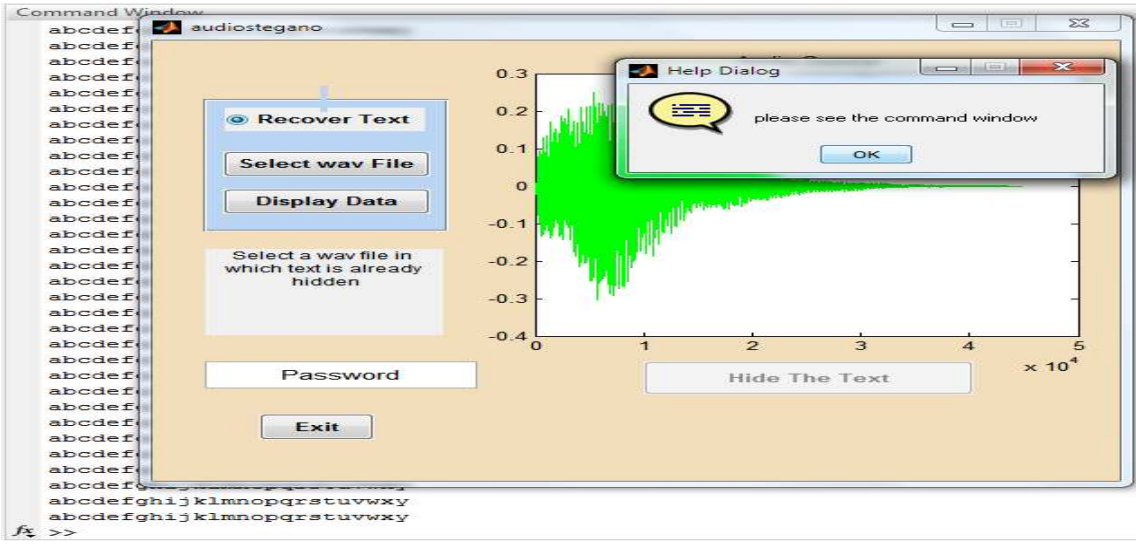


Figure 8: Decrypted Data

## CONCLUSION

In this paper we initiated a self preconception method of invisible audio data hiding. This system is to provide a good, competent method for hiding the data from hackers and sent to the target in a safe way. This proposed system will not modify the size of the file even after training and also appropriate for any type of audio file arrangement. Thus we bring to a close that audio data hiding techniques can be used for a number of purposes other than tracing the data, storing the secured data, corrupt detection and secret report. So similarly these operations described above can be further modified as it is in the world of information technology. After designing any process every developer has a thought that develop it by adding up more features to it.

## REFERENCES


1. Alattar.M, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Trans. Image Process., 2004; 13 (8): 1147–1156.
2. Caldelli R, Filippini F and Becarelli R, Reversible watermarking techniques: An overview and a classification, Eur. Assoc. Signal Process. J. Inf. Security, 2010; 2: 1–19.
3. Celik MU, Sharma G, Tekalp AM and Saber E, Lossless generalized-LSB data embedding, IEEE Trans. Image Process., 2005; 14 (2): 253–266.
4. Lalli, G., et al. "Feature Recognition on Retinal Fundus Image–A Multi-Systemic Comparative Analysis." International Journal of Advanced Research in Computer Science and Software Engineering, 2013; 3(11): 427-434.
5. Coltuc D, Low distortion transform for reversible watermarking, IEEE Trans. Image Process., 2012; 21 (1): 412–417.
6. Fridrich J, Goljan M and Du R, Lossless data embedding-new paradigm in digital watermarking," Eur. Assoc. Signal Process. J. Appl. Signal Process., 2002; 2:185–196.
7. Gao XL. An Yuan Y, Tao D and Li X, Lossless data embedding using generalized statistical quantity histogram, IEEE Trans. Circuits Syst. Video Technol., 2011; 21 (8): 1061–1070.
8. Hu Y, Lee HK and Ji L, DE-based reversible data hiding with improved overflow location map," IEEE Trans. Circuits Syst. Video Technol., 2009; 19 (2): 250–260.
9. Lalli, G., et al. "A development of knowledge-based inferences system for detection of breast cancer on thermogram images." Computer Communication and Informatics (ICCCI), 2014 International Conference on. IEEE, 2014.
10. Luo L, Chen Z, Chen M, Zeng X, and Xiong Z, Reversible image watermarking using interpolation technique, IEEE Trans. Inf. Forens. Security, 2010; 5 (1): 187–193.
11. Li X, Yang B, and Zeng T, Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection, IEEE Trans. Image Process., 2011; 20 (12): 3524–3533.
12. Lalli, G., et al. "A Perspective Pattern Recognition Using Retinal Nerve Fibers With Hybrid Feature Set." Life Science Journal 10.2 , 2013.
13. Thodi DM and Rodriguez JJ, Expansion embedding techniques for reversible watermarking, IEEE Trans. Image Process., 2007; 16 (3): 721–730.
14. Tian J, Reversible data embedding using a difference expansion, IEEE Trans. Circuits Syst. Video Technol., 2003; 13 (8): 890–896.
15. Tai WL, Yeh CM and Chang CC, Reversible data hiding based on histogram modification of pixel differences," IEEE Trans. Circuits Syst. Video Technol., 2009; 19 (6): 906–910.
16. Weng S, Zhao Y, Pan JS and Ni R, Reversible watermarking based on invariability and adjustment on pixel pairs, IEEE Signal Process. Lett., 2008; 15 (11): 721–724.
17. Manikandaprabu, N., et al. "Data Hiding in Color Images. Int. J. Novel. Res. Eng & Pharm. Sci 1.05: 1-7.
18. Coltuc D and Chassery JM, Very fast watermarking by reversible contrast mapping," IEEE Signal Process. Lett., 2007; 14 (4) 255–258.
19. Kamstra L and Heijmans.HJAM, Reversible data embedding into images using wavelet techniques and sorting, IEEE Trans. Image Process., 2005; 14 (12): 2082–2090.
20. Peng F, Li X, and Yang B, Adaptive reversible data hiding scheme based on integer transform," Signal Process., 2012; 92 (1): 54–62


**Source of support: Nil, Conflict of interest: None Declared**