Asian Journal of Research in Computer Science

12(4): 97-110, 2021; Article no.AJRCOS.78612
ISSN: 2581-8260

LSB-based Audio Steganographical Framework for Securing Data in Transit

Nuku Atta Kordzo Abiew [a*], Maxwell Dorgbefu Jnr. [b] and William Brown-Acquaye [a]

[a] *Faculty of Computing and Information Systems, GCTU, Ghana.*
[b] *Department of Information Technology Education. AAMUSTED, Ghana.*

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2021/v12i430297
Editor(s):
(1) Prof. G. Sudheer, GVP College of Engineering for Women, India.
Reviewers:
(1) Yair Wiseman, Bar-Ilan University, Israel.
(2) Sura Ibrahim Mohammed Ali, Al-Muthanna University, Iraq.
Complete Peer review History, details of the editor(s), Reviewers and additional Reviewers are available here:
https://www.sdiarticle5.com/review-history/78612

Review Article

Received 09 October 2021
Accepted 18 December 2021
Published 19 December 2021

ABSTRACT

The benefits that individuals and organizations derive from the digital era comes with its own challenges. Globally, data has become one of the greatest assets for decision making and operational improvements among businesses, government agencies and even individuals. Data on its own and at its source does not make so much contribution to business processes. Data is transmitted from one location to another towards attainment of its goal as a critical resource in decision making. However, data including sensitive or confidential ones are transmitted via public channels such as the Internet. The data so transmitted via the Internet is vulnerable to interception and unauthorized manipulation. This demands that data in transit is protected from the prying eyes of the malicious internet users. One of such strategies for transmitting data via public channels such as the Internet without attracting attention from intruders is steganography. In this paper, the least significant bit algorithm was used with an audio file for hiding data in transit. The algorithm used in this research proves to be one of the simplest ways of securing data using audio steganography. The method employed the LSB technique by using audio files as the stego object for the final implementation in the Java programming language. The experimental results proved to be one of the best methods of implementing steganography. The accuracy of the stego objects shows high quality, and similarity scores with an improved processing time.

*Corresponding author: E-mail: akordzo@gctu.edu.gh;

Keywords: Cryptography; communication; data; least significant bit; security; steganography.

1. INTRODUCTION

According to [1], data security is defined as “the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle.” The internet has proven to be the less expensive way of exchanging large amounts of information confidentially between the communicating parties. It is critical to protect the data being transmitted as well as the users involved in its transmission. users, and the data they exchange. Today, digital steganography is one of the important components in the toolboxes of spies and malicious hackers, as well as human rights activists and political dissidents [2]. The use of the internet as the major source of transmitting confidential data has brough about profound changes in lives. The many advantages posed by the Internet have also generated new security challenges and opportunities for innovation [3].

This trend has resulted in huge losses to both content producers and owners. To ensure the security of information on open channels, efforts to establish safety should be integrated into data communication systems over the web. The incorporation of safety measures into data communication systems is the surest way of protecting and safeguarding data transmission over public channels such as the Internet.

The need to communicate information as safely and as securely as feasible has been a subject of much debate for several years. Data is considered a valuable resource for the 21st century establishments including businesses and government agencies. Data therefore, plays a key role in the operational success of these establishments. Availability of large volumes of data comes with the challenge of its misuse or malicious manipulation. Data security measures have become a major issue of concern to all firms especially those that handle confidential data. Whichever system is chosen for secure communication; the issue of major concern is the extent to which the system is safe.

Data security is the process or the art of protecting data from vicious forces or users and the unsolicited activities of unapproved users. An enormous quantity of confidential data is transferred through the web or the Internet as it is the cheapest and commonly available method. This technological growth and advancement have additionally rendered digital information highly susceptible to interception and probable unapproved access and or use and have resulted in major economic losses to content creators and rights holders.

The security of information on open channels demands that, robust safety measures are integrated into data communication systems through the web [4]. Steganography is part of the great technologies which aid in the attainment of the general target of secure transfer of information from senders to approved recipients. Steganography is the method of hiding a file, image, or message inside a different file, image, or message. The term steganography has a Greek root which denotes "covered writing" or "concealed writing" [5] . In [3] the authors defined steganography as the art and science of concealing information during communication so that it is not discovered by a third party.

The goal of steganography is to provide secret correspondence between communicating parties by concealing the information being transmitted from a third party [6]. Steganography is regularly mistaken for cryptography because the two have some similarities as they are used for securing critical data. They vary because steganography consists of hiding data to create the impression that no message is covered at all. Cryptography on the other hand, encrypts the information prior to its transmission via a public channel. Whiles steganography hides the intended message in other files to conceal the message from adversaries, cryptography converts the original message into a cipher text.

One major drawback with most of the information that is transmitted on the internet is that information is transmitted in a format which intruders can read and understand without difficulty. After successfully acquiring the information illegally, intruders might divulge sensitive data such trade secrets to the public or other organizations, distort the information to malign a person or an organization or sometimes it is used to initiate attacks on these individuals and organizations. Steganography is one of the best methods that can be employed to curb this unpleasant and devastating act and trend.

With the current increase in usage of traffic security systems, the military and other security organizations secure their data by concealing the sender, the receiver and the content of the message using steganography [7]. In digital elections, similar approaches are being proposed and adopted using mobile phone systems [8]. A few of the methods utilized as part of steganography are based on domain tools such as Least Significant Bit (LSB) for embedding and noise manipulation, and the Discrete Cosine Transformation and Wavelet Transformation. Nonetheless, there are implementations that used two or more of the techniques for the concealment [9].

Although several stenographical methods are known for securing data in transit, they involve considerable overheads, making them impractical, especially compared to the format used in their implementation. It is sometimes possible to devise data security techniques and methods that can secure data in transit without the use of formats readable by human beings. Such techniques and methodologies offer the benefits of securing data from an unauthorized usage without sacrificing efficiency. In this paper, we used the LSB technique with audio file as the stego object to implement a simple but robust framework for securing data in transit.

1.1 Related Work

In the year 2015, Ayush Singhal et al [10] proposed that for cover objects, different types of digital media can be used and they used .wav audio as their cover file in the research work. They were able to hide the secret message inside the audio cover file.

In the year 2014, Rohit Tanwar and Monika Bisla [11] advised that one of the most important goal of any audio steganographic technique is that the process should be robust and the audio cover file generated must be resistant to malicious attacks as that is the main aim of the steganography process.

In 2014, Kazem Qazanfari and Reza Safabakhsh [12] proposed an improved version of LSB++ approach. In this improved LSB++ they make distinction between sensitive pixels and allow protecting them from the embedding of extra bits, which results in the lower distortion in co-occurrence matrices.

In the year 2012, M. Baritha Begum and Y. Venkataramani [13] proposed an algorithm that included compression that reduces the redundancy of data. In their audio steganographic technique, dictionary based compression bits were hidden in the least significant bit of audio signals and the signal to noise ratio (SNR) was calculated. This audio Steganography was used to conduct for various compression algorithms with dictionary-based compression.

A novel secured way of protecting communication between seaports within the maritime industry based on Steganography was proposed by Y. Wiseman. [14]. The procedure was achieved by transmitting encrypted messages in images compressed in the JPEG format leading to the modification of the image bits which is totally unnoticeable.

In the year 2009, S. Channalli and A. Jadhav [15] proposed a new LSB based method in which common bit pattern is used to hide data which can be used in audio steganography as well while using the bit patterns with different frequencies of audio signal.

The major objective of steganography is to ensure secure communication in a totally untraceable method [16] and to prevent drawing attention to the concealed information being exchanged [17]. Its purpose is not to prevent unauthorized people from decoding the concealed information, but rather to prevent them from perceiving that its existence. If a steganography technique makes somebody to be suspicious of the carrier medium, then the technique is not successful [18]. Until recently, steganography has not received much attention as compared to cryptography. This situation has however changed rapidly and can be attributed to following reasons [19]. First and foremost, the interest of publishing and broadcasting firms in hiding encrypted copyright marks and serial numbers in digital files have increased tremendously. Secondly regulations by successive governments to restrict the availability of encryption services have motivated researchers to study methods by which private messages can be embedded in seemingly innocuous cover messages.

Figure 1 shows a basic steganography model consisting of Carrier, Message and Password proposed by Cachin [20]. Carrier is also known as *cover-object*, which the message is embedded and serves to hide the presence of the message. This model presented the technical details of steganography however not practical implementation was given by Cachin or any other researcher, thereby making the model not to be practically proven. According to the theoretical implementation of the model, message is the data that the sender wishes to remain as confidential, and this can be in any digital readable format [21]. Password is known as *stego-key*, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from the *cover-object*. The *cover-object* with the secretly embedded message is known as the *stego-object*.

There are several suitable media that can be used as cover-objects such as network protocols, audio, a text file, video and image files [22].

1.2 Cryptography and Steganography

For a steganographic algorithm with a stego-key, given any cover object the embedding process generates a stego object. The extraction process takes the stego object, and uses the shared key and applies the inverse algorithm to extract the hidden message.

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from a malicious people, whereas steganography even conceals the existence of the message. According to Kessler, “The goal of cryptography is to make data unreadable by a third party, the goal of steganography is to hide the data from a third party” [23]. The most important requirement of any steganographic system is that it should be impossible for an eavesdropper to distinguish between ordinary objects and objects that contain secret data [24].

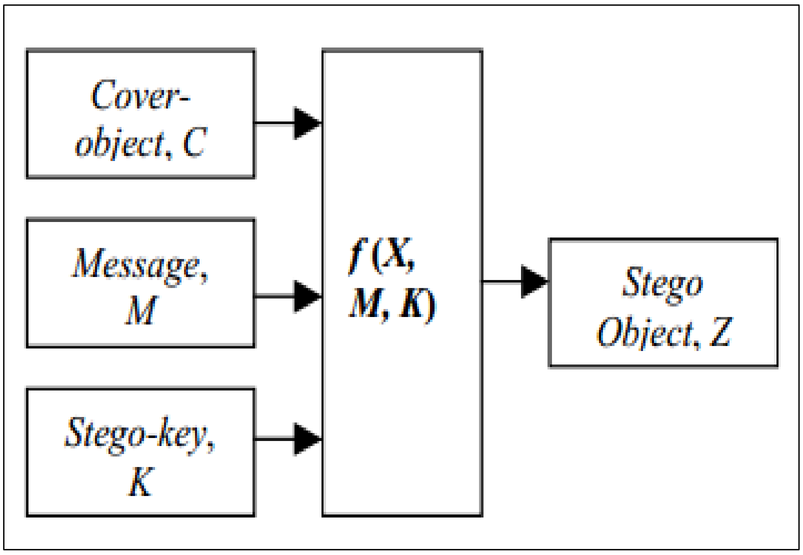


Fig. 1. Basic Steganography Model

Table 1. Features of Steganography and Cryptography [25]

Steganography	Cryptography
Steganography refers to Cover Writing	Cryptography refers to Secret Writing
Steganography is less popular than Cryptography.	Cryptography is more popular than Steganography
Structure of data remains same.	Structure of data can be altered.
Attack in Steganography is termed as Steganalysis.	Attack in Cryptography in termed as Cryptanalysis.
Steganography supports Confidentiality and Authentication.	Cryptography supports Confidentiality, Authentication, Data integrity and Non-repudiation.
Steganography requires a parameter like key.	Cryptography may not need any key.

Steganography is often thought of only as a tool for a malicious user to subvert a security policy, but there are three fundamental classes of applying steganography. These includes subliminal communication [26], integrity and authentication, and illicit exfiltration of data [27].

1.3 Steganography Techniques

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed [17]. We discuss a few subsequently.

1.3.1 Least significant bits

In computing, the least significant bit (LSB) is the bit which is farthest to the right and holds the least value in a multi-bit binary number. For example, given a four-bit binary number; abcd where a, b, c, d belongs to the set of binary bits, {0,1}, d is the least significant bit. As binary numbers are largely used in computing and other related areas, the least significant bit holds importance, especially in the transmission of binary numbers [28].

Digital data is computed in binary format, and similarly to numerical notation, the rightmost digit is considered the lowest digit whereas the leftmost is considered the highest digit in terms of significance. Due to the positional notation, the least significant bit is also known as the rightmost bit. It is the opposite of the most significant bit, which carries the highest value in a multi-bit binary number as well as the number which is farthest to the right. In a multi-bit binary number, the significance of a bit decreases as it approaches the least significant bit. In the binary number system, the most significant bit can be either 0 or 1.

When a transmission of binary data is done with the least significant bit first technique, the least significant bit is the one which is transmitted first, followed by other bits of increasing significance. The least significant bit is frequently employed in hash functions as in [29] [30] [31], and checksums and pseudorandom number generators [32].

LSB insertion is a simple approach to embedding information in a file. The simplest steganographic techniques embed the bits of the message directly into the least significant bit plane of the cover-object in a deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. In recent times, the LSB embedding technique is one of the most important steganography techniques [33]. LSB techniques is mostly implemented in the spatial domain. In this method the least significant bit of some or all the bytes inside an image or media is replaced with bits of the secrete message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding can also be applied in the data domains for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image.

1.3.2 Masking and filtering

Masking and filtering techniques are usually restricted to 24 bits and gray scale images. These techniques hide information by marking an image, in a manner similar to paper watermarks. The techniques perform analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level [34]. This technique is much more robust than the LSB replacement with respect to compression since the information is hidden in the visible parts of the image. However, this technique can be applied only to gray scale images and restricted to 24 bits thereby making it unsuitable for audio steganography implementation [35]. According to N. F. Johnson and S. Jajodia, Masking and filtering techniques is the process of hiding information by marking the image, in a manner similar to paper watermarks. Watermarking techniques may be applied without fear of image destruction due to lossy compression because they are more integrated into the image [17].

Figure 2, illustrates how masks and filters can be embedded into images without destroying the original quality of a photographic image [36]. The entire photograph has been watermarked. To perform steganography within an image, the luminance of the masked area is increased by 15 percent. The luminance must be changed by a smaller percentage, so the mask would be undetected by the human eye [37].

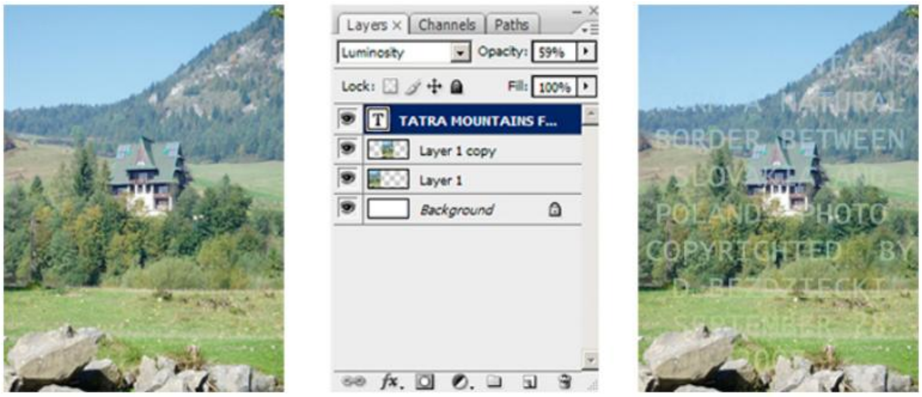


Fig. 2. Masking and Filtering Method

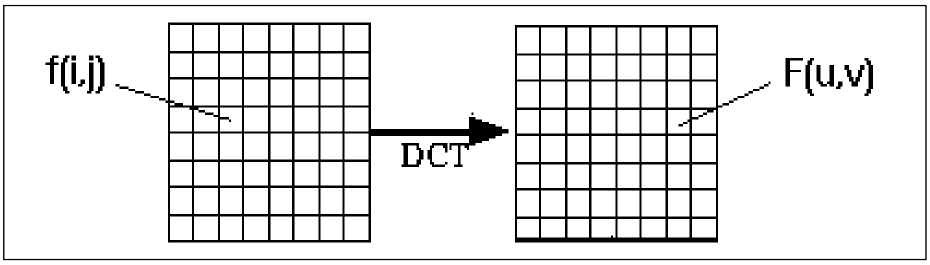


Fig. 3. The Discrete Cosine Transform (DCT)

1.3.3 Transforms techniques

Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-object, which make them more robust to attack. Transformations can be applied over the entire object, to block throughout the object, or other variants.

DCT is one of the general orthogonal transform for digital image processing with advantages such as high compression ratio, small bit error rate and good information integration ability [38]. DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain as shown in Figure 3. It can separate the image into high, middle and low frequency components.

The DCT technique is applied to image pixels in spatial domain in order to transform them into a frequency domain in which redundancy can be identified. The DCT can be employed on both one-dimensional and two dimensional signals like audio and image, respectively. The discrete cosine transform is the spectral transformation, which has the properties of Discrete Fourier Transformation [39]. DCT uses only cosine functions of various wave numbers as basic functions and operates on real valued signals and spectral coefficients.

The general equation for a 1D (N data items) DCT is defined by the following equation:

$$F(u) = \left(\frac{2}{N}\right)^{1/2} \sum_{i=0}^{N-1} A(i).\cos\left[\frac{\pi.u}{2.N}(2i + 1)\right] f(i)$$

The general equation for a 2D (N by M image) DCT is defined by the following equation:

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} A(i).A(j).cos\left[\frac{\pi.u}{2.N}(2i + 1)\right] cos\left[\frac{\pi.v}{2.M}(2j + 1)\right].f(i,j)$$

A wavelet is a small wave which oscillates and decays in time domain. The Discrete Wavelet

Transform is a relatively recent and computationally efficient technique. Wavelet analysis is advantageous as it performs local analysis and multi-resolution analysis. Analyzing the signal at different frequencies with different resolutions is called multi-resolution analysis (MRA). Wavelet analysis can be of two types: continuous and discrete [38]. In Discrete Wavelet Transform (DWT) based steganography approaches the wavelet coefficients of the cover image(object) are modified to embed the secret message [40].

More specifically, the DWT provides high time resolution and low frequency for high frequencies and the vice versa. The DWT is similar to the human ear which shows similar time-frequency resolution characteristics. It provides a compact representation of a signal in time and frequency domains that can be effectively and efficiently computed [41].

The DWT is defined by the following equations [42]:

$$F(u) = \frac{1}{N}\sum_{x=0}^{N-1} f(x)e^{-2\pi ixu/N}$$

1.4 Categories of Steganography

There are a lot of digital file format currently in used today. All these digital formats are suitable for the implementation of steganography, however those digital formats with high degree of redundancy is more prefer and suitable than those with low degree of redundancy. For a file to be of high degree of redundancy implies that the bits of that file can be changed without detecting the change easily. Example of such objects is video, audio and image files. With this, image, video, and audio files are more suitable objects for the implementation of steganography. Figure 2 shows the various categories of file formats that can be used for steganography.

Currently, most of the steganographic systems uses objects like video, image, and audio to implement data hiding Systems. This is because of the tendency at which digital images, audio and video are transmitted over the Internet in the form of emails. From Figure 2, these are the most widely used objects apart from the text.

Protocol steganography is receiving much attention in recent years due to the emergence of social media platforms for transmitting messages. The term protocol steganography refers to the technique of embedding data within messages and network control protocols used in network transmission. In the layers of the OSI network model there exist hidden channels where steganography can be used. An example of where information can be hidden is in the header of a TCP/ IP packet in some fields that are either optional or are never used.

It is worth noting that, steganographic systems can also be classified according to the cover modification applied in the embedding process. This classification scheme can be divided into the following categories.

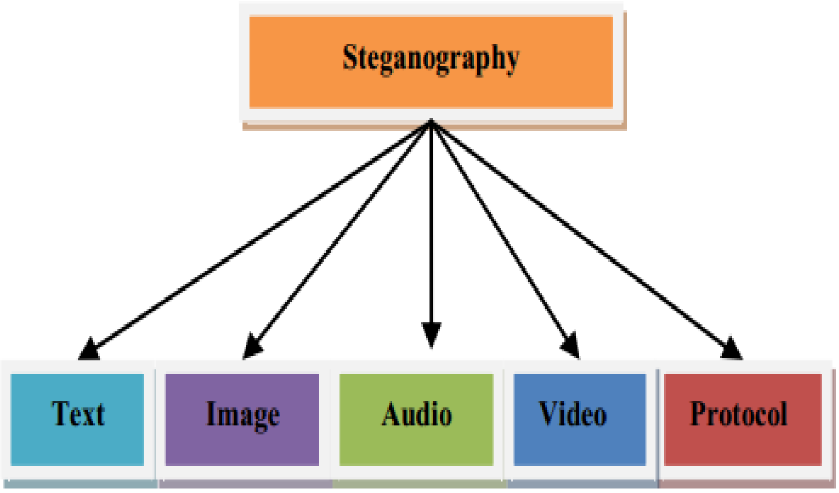


Fig. 4. Categories of Steganography

- **Substitution system** replace unneeded parts of a cover with a secrete data.
- **Transform domain techniques** embed secrete message in a transform space of the signal (e.g., in frequency domain).
- **Spread spectrum techniques** implement ideas from spread spectrum communication.
- **Statistical methods** encode data by changing several statistical properties of a cover and use assumption testing in the extraction process.
- **Distortion methods** accumulate data by signal alteration and measure the deviation from the original cover in the decoding step.
- **Cover generation schemes** encode data in the approach a cover for secrete communication is created.

1.5 Properties of Steganography

According to [43], there are few key properties that need must be taken into consideration when creating a digital data hiding system.

- *Imperceptibility*: The goal of steganography is that object should appear identical before and after hiding.
- *Embedding Capacity:* It is the capacity of steganographic algorithm based on the quantum of message it can secretly transmit. Capacity is one of the challenging case in steganography.
- *Robustness:* Robustness refers to the degree of difficulty required to tear down embedded information without destroying the cover object itself.
- *Undetectability:* This property is as important as imperceptibility. It is the rate and accuracy at which a media containing an embedded data cannot be detected using statistical or technological means.

2. SYSTEM DESIGN AND METHODOLOGY

In this study, we consider the Least Significant Bit approaches to implementing audio steganography for securing data. The scope of the study is limited to audio steganography as a result of its availability and memory usage utilization in shared memory systems.

2.1 The Least Significant Bit (LSB) Audio Steganography Implementation

The implementation of this technique involves all kinds of audio irrespective of the number of channels the audio has. This technology involves the hiding of data in audio files. The first bits of every audio sample of sixteen bits (16-bits) is either a plus or minus and the rest of the fifteen bits (15 bits) are divided into two groups. The first division has 7bits known MSB while the other division includes 8bits known as LSB. In this way the signals are interrupted, and data cannot be conveyed secure. For proper and secure conveyance, the payload is increased, and signals are improved.in the proposed audio steganography algorithm, an audio file will be considered as a cover object the message or text file is referred to as the secret message to be hidden in cover object.

LSB algorithm is a classic Steganography method used to conceal the existence of secret data inside a "public" cover. The LSB or "Least Significant Bit", in computing terms, represents the bit at the unit's place in the binary representation of a number. For example, we can represent the decimal number 170 in binary notation as 10101010. The least significant bit, in this case, is 0.

In the simplistic form, LSB algorithm replaces the LSB of each byte in the "carrier" data with one bit from the "secret" message [44].

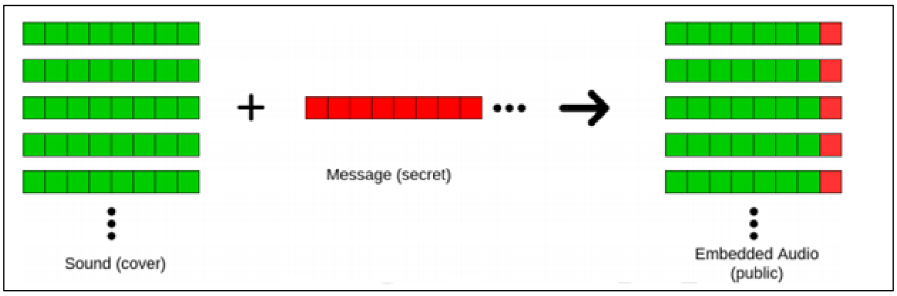


Fig. 5. Encryption process

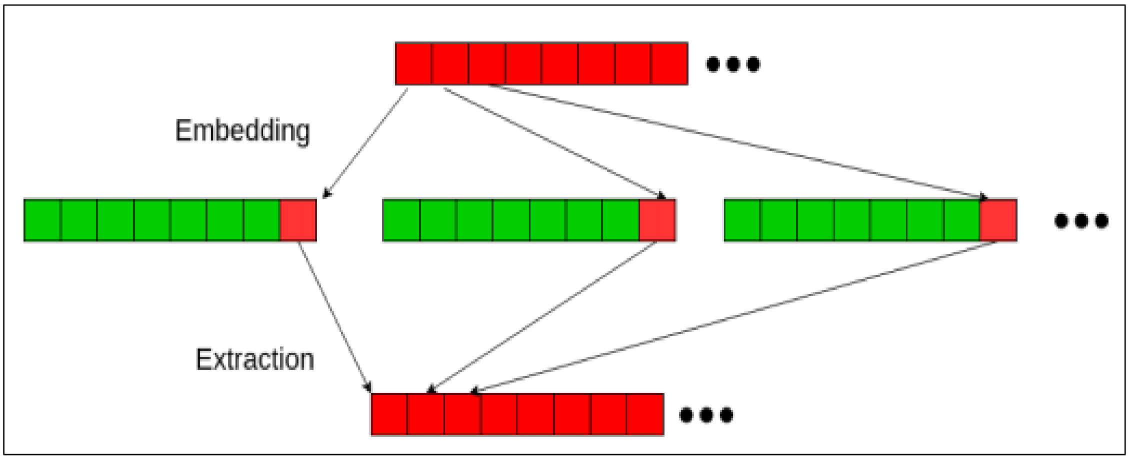


Fig. 6. Embedding and Extraction process

The sender performs "embedding" of the bits of secret messages onto the carrier data byte-by-byte. Whereas the receiver performs the "extraction" procedure by reading LSB bits of each byte of received data, this way the receiver reconstructs the secret message.

The advantage of the LSB techniques lies in its ease of implementation and simplicity. The LSB method allows high embedding capacity and uses different frequency levels for more security. Hiding the secret data using audio lowers the chances of the secret data being detected. This techniques for audio files work smoothly for all audio format as implemented in Java. Using these algorithms for encoding and decoding, one can retrieve the secrete message exactly as the original data.

3. RESULTS AND IMPLEMENTATION

The purpose of this study is the implementation of steganography using Least Significant Bit methods. This section seeks to present the result of the study by analyzing and interpreting the data collected, methods and techniques used in conducting the study. Different approaches were put in place in order to have better and deeper representation of the results by implementing LSB technique for hiding data in audio objects. For the implementation of the systems, the above stated scenario was considered and implemented using Java Programming Language. In all, testing was done through the normal viewing using the human senses to distinguish the original and the resultant object. The implementation of the Secure Transit Data System (STDS) was implemented in two folds, that is, encoding and decoding Audio Steganography presented using the LSB processes.

3.1 Audio Steganography Implementation

Audio signals have a characteristic redundancy and unpredictable nature that make them ideal to be used as a cover to hide secret information. Like image, audio files may be modified in such a way that it can contain some secret information using the LSB. In the case of audio or sound files, each sampling point of the file is substituted with the least significant bit. With this approach, large amount of data can easily be encoded onto the audio file. The redundancy of bits that exist in the binary coding of numbers, and alphabets forms the basis of this approach.

Looking at the binary code of numbers from 0 to 9, and from A (a) to P (p) for both casing, it can be observed that, these characters are only different in their respective last 4 bits. Thus, their first 4 bit are similar, thereby implying that, any number or alphabet can easily be represented by the last 4 bits and adding either 0 or 1 at its first position. To differentiate whether the character is number, uppercase alphabet or lowercase alphabet control symbols are used which is of the same type as that of number or alphabet.

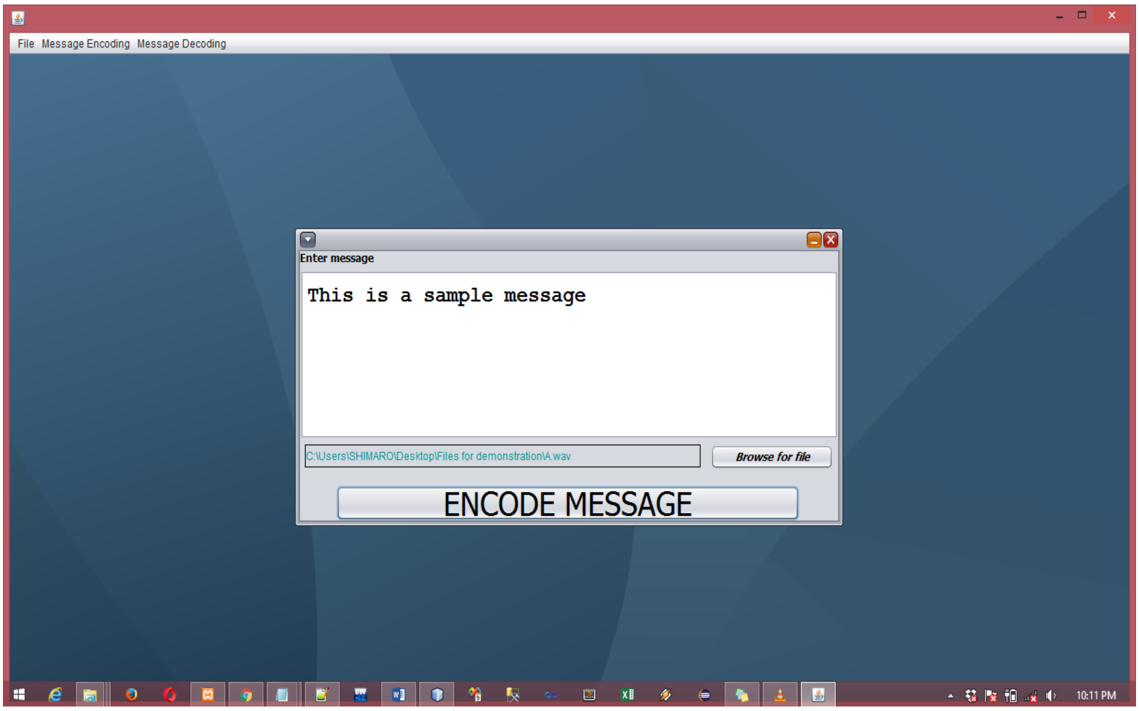
For special symbols like !, " , # , $, %, & , (, ,) , *, + , ', - , . , / is also observed and these special symbols can also be embedded in WAV file. When embedding the textual information in any audio file, first the audio signal is converted into bits. Then the message to be embedded is encrypted and converted. By applying LSB algorithm, the message is embedded into 16 bits or 8 bits audio sample.

3.2 Audio Steganography Encoding Process

The underlying technology for the encoding process is the LSB. In summary, the encoding algorithm takes in a text to be embedded as an input, convert the text into a 5-bit code by checking the redundancy in the binary coding structure of the characters involved. The next is to the read the audio file as the cover object. The selected audio file or the cover object is then used to hide the converted 5-bit code of text using the proposed methodology. This process is repeated until the entire message is embedded successfully into the audio file.

3.3 Audio Steganography Decoding Process

The decoding process is the reverse of the encoding process described above. The stego-object thus the cover audio that has the encoded message is read as an input. The message embedded is then extracted by reading the control symbols in samples using LSB. All the selected samples are stored with their LSB positions. The resultant array is then subjected to some minimal operation of division using the number of rows and columns leading to the final extraction of the messages.

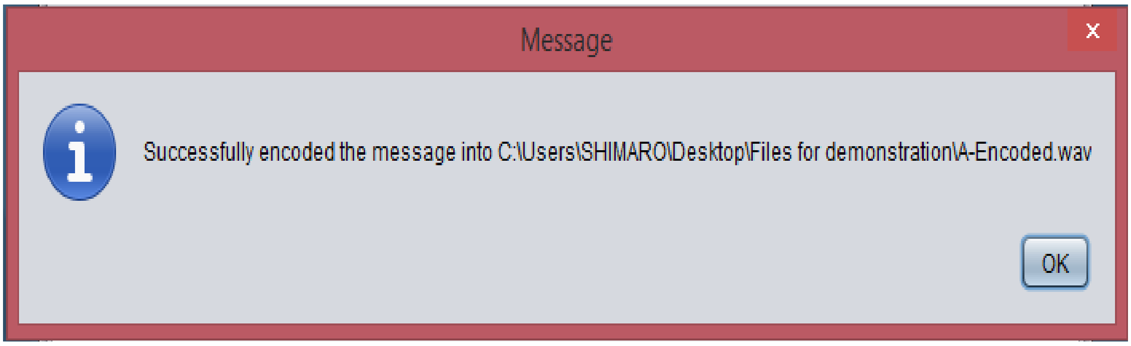


Enter message

This is a sample message

C:\Users\SHIMARO\Desktop\Files for demonstration\A.wav

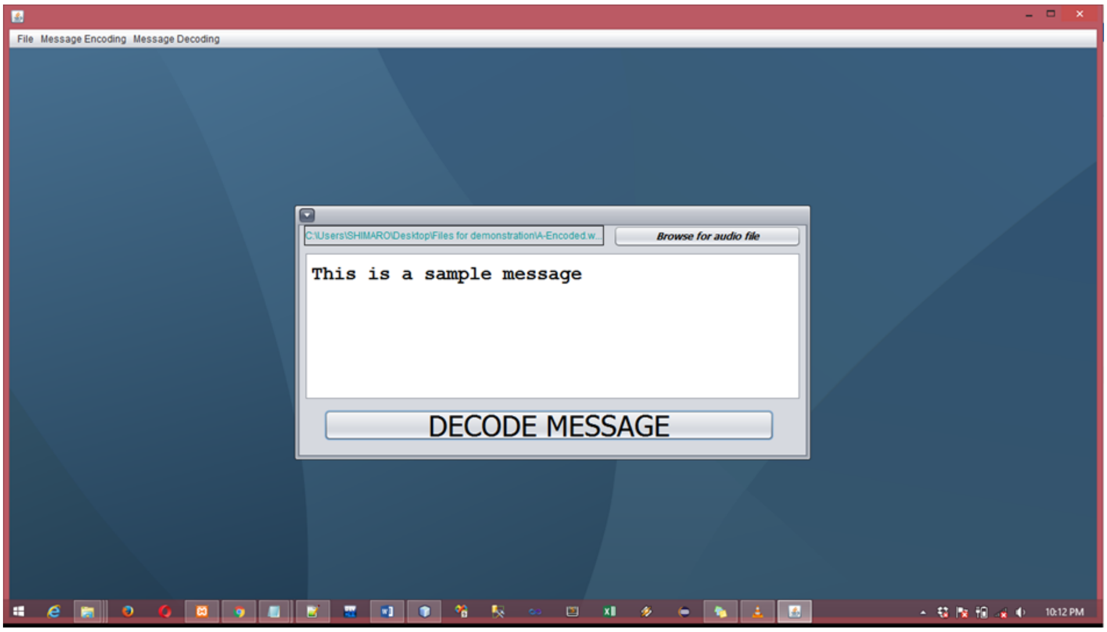
Fig. 7. Audio Embedding user interface



Message

Successfully encoded the message into C:\Users\SHIMARO\Desktop\Files for demonstration\A-Encoded.wav

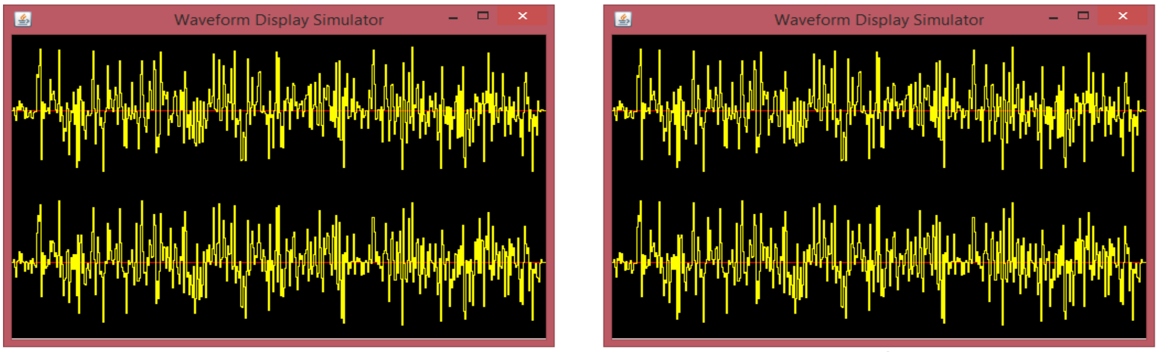
Fig. 8. Audio Encoding Status dialog



C:\Users\SHIMARO\Desktop\Files for demonstration\A-Encoded.w...

```
This is a sample message
```

Fig. 9. Audio Decoding User Interface

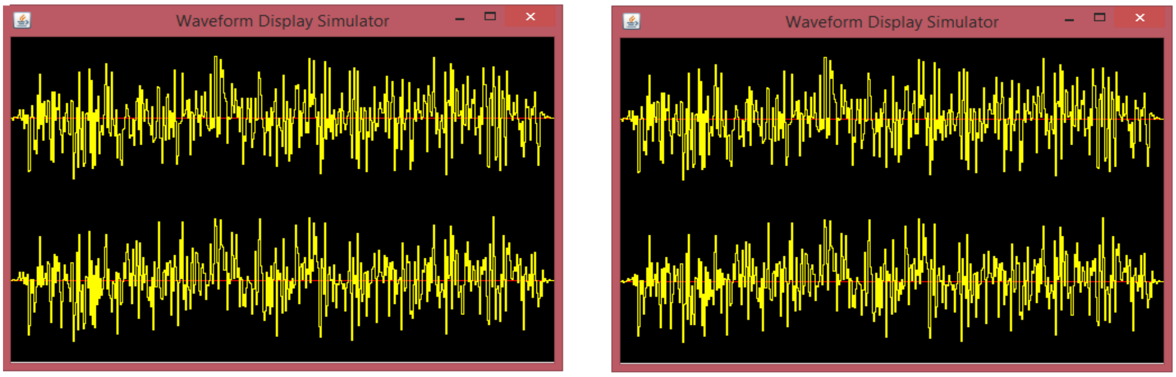


ORIGINAL AUDIO FILE

ENCODED/STEGO AUDIO FILE

Fig. 10. Audio file sample A waveform

SAMPLE B



ORIGINAL AUDIO FILE

ENCODED/STEGO AUDIO FILE

Fig. 11. Audio file sample B waveform

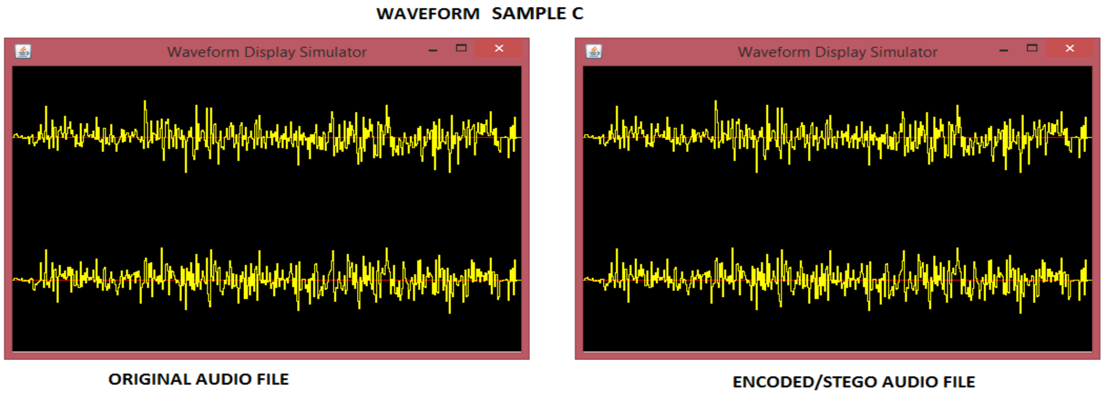


Fig. 12. Audio file sample C waveform

3.4 Experimental Result

After successful implementation of the embedding and the decoding process, a wave form was created from the two samples files. It can be observed from the figure below that, the encoded and the original files have the same wave forms. This shows that the proposed technology does not distort the audio file, thereby not attracting attention.

4. CONCLUSION

This study set out to secure data in transit using audio steganography. Steganography is one of the ways by which data in transit can be secured without attracting unnecessary attention from intruders. The algorithm used in this research proves to be one of the simplest ways of securing data using audio steganography. The methods employ the LSB approaches by using audio files as the stego object for the implementation based in Java Programming Language. The experimental results also proved to be one of the best methods of implementing steganography. The accuracy of the stego objects as compared to the original objects is of high quality and similarity. The processing time of both the encoding and decoding algorithms as compared to other implementation is faster, more robust and efficient.

Data is the backbone and the lifeline of every organization. Data security has become one of the major ways by which organization are committing their resources to. Therefore, there is the need to implement cheaper but robust and secure methods of securing data. The knowledge of this technology is still new to most practitioners in the area of Information Security.

In the future, more work should be carried out by technology and science-based institutions into the area of information hiding. It is the hope of the researcher that, future works can take two or more objects as input and embed the secret messages in them. Other quality metrics can also be used to analyze the performance of the proposed algorithms.

Finally, future researchers should try to include into their work how best this technology can be used in mobile phones and how best protocol steganography can be used to secure data on the Internet.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. IBM. "Data Security," IBM, 18 June; 2018. [Online]. Available:https://www.ibm.com/topics/data-security.
[Accessed 15 December 2021].
2. Dickson B. The Daily Swig: Cybersecurity news and views, PortSwigger, 06 February; 2020. [Online]. Available:https://portswigger.net/daily-swig/what-is-steganography-a-complete-guide-to-the-ancient-art-of-concealing-messages.
[Accessed 17 December 2021].
3. Ibrahim iTMaDS. Effect of Communication Channel on Transferred Data," Diyala Journal of Pure Science. October 2013;9(4):75-92.
4. Qadir MA, Ahmad I. Digital text watermarking: secure content delivery and

data hiding in digital documents. in Proceedings 39th Annual 2005 International Carnahan Conference on Security Technology; 2005.

5. Mangal JMaS. An Overview of Image Steganography using LSB Technique. IJCA Proceedings on National Conference on Advances in Computer Science and Applications (NCACSA 2012), 2012;3: 10-13.
6. Honeyman NPP. Detecting Steganographic Content on the Internet. University of Michigan. Michigan; 2001.
7. Alekhya Orugonda S. Hiding the Military Secret Message by Reversible Data Hiding," International Journal of Engineering adn Innovative Technology(IJEIT). 2013;3(4):165-168.
8. Shin-Yan Chiou TJWJMC. Design and Implementation of a Mobile Voting System Using a Novel Oblivious and Proxy Signature. Security and Communication Networks. 2017:1-16.
9. Raja CRCKRVaLMPKB. A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images. in 2005 3rd International Conference on Intelligent Sensing and Information Processing, Bangalore; 2005.
10. Ayush Singhal NSMSB. An Advanced Approach for Implementation of Audio Steganography. International Journal For Science, Technology and Engineering. 2015;1(12): 66-71.
11. Tanwar R, Bisla M. Audio Steganography. in 2014 International Conference on Reliability Optimization and Information Technology (ICROIT); 2014.
12. Kazem Qazanfari RS. A new steganography method which preserves histogram: Generalization of LSB++,," Information Sciences. 2014;277:90-101.
13. Baritha Begum YVM. LSB Based Steganography based on Text Compression," Procedia Engineering. 2012;30:703-712.
14. Wiseman Y. Protecting Seaport Communication System by Steganography Based Procedures. International Journal of Security and Its Applications. 2014;8(4): 25-36.
15. Jadhav SCaA. Steganography an Art of Hiding Data. International Journal on Computer Science and Engineering (IJCSE); 2009.
16. Johnson JS NF. Steganalysis of Images Created Using Current Steganography Software. In: Aucsmith D. (eds) Information Hiding.IH 1998. Lecture Notes in Computer Science, vol 1525, Berlin: Springer; 1998.
17. Jajodia NFJaS. Exploring steganography: Seeing the unseen. Computer. 1998;31(2): 26-34.
18. Provos PHN. Detecting Steganographic Content on the Internet. CITI Technical Report. Michigan; 2021:01-11.
19. Anderson R. Analysis of LSB Based Image Steganography Techniques. IEEE. 1998; 474-481.
20. Cachin C. "An Information-Theorectical Model for Steganography," in In Proceeding of 2nd Information Hiding Workshop; 1998.
21. Katzenbeisser FPS. Defining security in Steganographic Systems. in Proc. SPIE 4675, Security and Watermarking of Multimedia Contents IV; 2002.
22. Petitcolas RJAaMGKFAP. Information hiding-a survey. in In Proceedings of the IEEE; 1999.
23. Gary CH, Kessler C. Chapter 2- An Overview of Steganography," in Advances in Computers, Marvin V. Zelkowitz, Ed., Elsevier. 2011;83: 51-107.
24. Miroslav Goljan JFTH. New blind steganalysis and its implications. in Proceedings, Security, Steganography, and Watermarking of Multimedia Contents VIII;, San Jose. 2006;6072.
25. Parahar M. Difference between Steganography and Cryptography," Tutorial Point, 15 April; 2020. [Online]. Available:https://www.tutorialspoint.com/difference-between-steganography-and-cryptography.
[Accessed 16 December 2021].
26. Gasser M. Building A secure Computer Systems, USA: Van Nostrand Reinhold Co; 1998.
27. SLNFMaLOJT. Brassil. Electronic marking and identification techniques to discourage document copying. IEEE Journal on Selected Areas in Communications. 1995;13(8):1495-1504.
28. Techopedia. Least Significant Bit(LSB). Janalta Interactive; 2021.
[Online].
Available:https://www.techopedia.com/definition/8030/least-significant-bit-lsb.
[Accessed11 December 2021].
29. Abood MH. An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms. in 2017

Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), Baghdad, Iraq; 2017.

30. Ms.Shridevishetti MS. A Secure Image Steganography based on RSA Algorithm and Hash-LSB Technique," International Journal of Engineering Research & Technology (Ijert) Icesmart. 2015;3(19): 1-7.
31. BR al. Hash Based Least Significant Bit Technique For Video Steganography," International Journal of Engineering Research and Applications. 2014;4(1.3): 44-49.
32. Peterson DC. IOWA State University, Digital Repository," IOWA State University, 01 January; 2012.
[Online].
Available:https://dr.lib.iastate.edu/entities/publication/95da58ab-9d56-4afe-b1b4-75c039766ce5.
[Accessed 11 December 2021].
33. ADSBaSD, Vanitha T. A Review on Steganography-Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm. International Journal of Innovative Research in Computer and Communication Engineering. 2014;2(5): 89-95.
34. Tiwari SaRK. Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization," International Journal of Computer Science and Network Security. 2008;8(1): 228-233.
35. Vaishali JACaD. Image steganographic techniques with improved embedding capacity and robustness. in 2011 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, India; 2011.
36. Gupta PKSaDRK. A Review of Digital Image Steganography. Journal of Pure and Applied Science & Technology. 2012;2(1):98-106.
37. Project M. Image Steganography Techniques," M4JPEG Project; 2018. [Online].
Available:https://digitnet.github.io/m4jpeg/about-steganography/image-steganography-techniques.htm.
[Accessed 17 December 2021].
38. Bhat VPaP. Transform Domain Techniques for Image Staganography. International journal of innovative research in electrical, electronics, instrumentation and control engineering. 2015;3(1):65-58.
39. Watson A, Image Compression Using the Discrete Cosine Transform. Mathematical Journal, 1994;4(1):81-88.
40. Kumar VKaD. Performance evaluation of DWT based image steganography," in 2010 IEEE 2nd International Advance Computing Conference (IACC), Patiala, India; 2010.
41. GEG, Tzanetakis CP. Audio Analysis using the Discrete Wavelet Transform. Semantic Scholar, 2001;1-6.
42. Marshall D. Dave Marshall Multimedia. 10 April 2001. [Online].
Available:https://users.cs.cf.ac.uk/Dave.Marshall/Multimedia/node228.html.
[Accessed 17 December 2021].
43. Shanthakumari BSaR. "Efficient Adaptive Steganography for Color Images Based on LSBMR Algorithm. ICTACT Journal on Image and Video Processing. 2012;02(03):387-392.
44. Arora SK. Audio Steganography : The art of hiding secrets within earshot(part 2 of 2)," 17 June; 2018. [Online].
Available:https://sumit-arora.medium.com/audio-steganography-the-art-of-hiding-secrets-within-earshot-part-2-of-2-c76b1be719b3.
[Accessed 1 August 2021].
45. Ramkumar M, Akansu AN. "Some design issues for robust data hiding systems," in Conference Record of the Thirty-Third Asilomar Conference on Signals, Systems, and Computers (Cat. No.CH37020); 1999.

© 2021 Abiew et al.; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/78612