

2

# 3 **LSB-BASED AUDIO STEGANOGRAPHICAL** 4 **FRAMEWORK FOR SECURING DATA IN** 5 **TRANSIT**

6

7

8

## 9 **ABSTRACT**

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

28 *Keywords: Cryptography, Communication, Data, Least Significant Bit, Security, Steganography*

29

30

## 31 **I. INTRODUCTION**

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

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

47 The need to communicate information as safely and as securely as feasible has been a subject of  
48 much debate for several years. Data is considered a valuable resource for the 21<sup>st</sup> century  
49 establishments including businesses and government agencies. Data therefore, plays a key role in  
50 the operational success of these establishments. Availability of large volumes of data comes with  
51 the challenge of its misuse or malicious manipulation. Data security measures have become a  
52 major issue of concern to all firms especially those that handle confidential data. Whichever

53 system is chosen for secure communication; the issue of major concern is the extent to which the  
54 system is safe.

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

61  
62 The security of information on open channels demands that, robust safety measures are  
63 integrated into data communication systems through the web [4]. Steganography is part of the  
64 great technologies which aid in the attainment of the general target of secure transfer of  
65 information from senders to approved recipients. Steganography is the method of hiding a file,  
66 image, or message inside a different file, image, or message. The term steganography has a  
67 Greek root which denotes "covered writing" or "concealed writing" [5] . In [3] the authors  
68 defined steganography as the art and science of concealing information during communication so  
69 that it is not discovered by a third party.

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

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

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

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

100

101

## 102 **II. RELATED WORK**

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

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

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

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

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

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

126 The major objective of steganography is to ensure secure communication in a totally untraceable  
127 method [16] and to prevent drawing attention to the concealed information being exchanged  
128 [17]. Its purpose is not to prevent unauthorized people from decoding the concealed information,  
129 but rather to prevent them from perceiving that its existence. If a steganography technique makes  
130 somebody to be suspicious of the carrier medium, then the technique is not successful [18]. Until  
131 recently, steganography has not received much attention as compared to cryptography. This  
132 situation has however changed rapidly and can be attributed to following reasons [19]. First and  
133 foremost, the interest of publishing and broadcasting firms in hiding encrypted copyright marks  
134 and serial numbers in digital files have increased tremendously. Secondly regulations by  
135 successive governments to restrict the availability of encryption services have motivated  
136 researchers to study methods by which private messages can be embedded in seemingly  
137 innocuous cover messages.

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

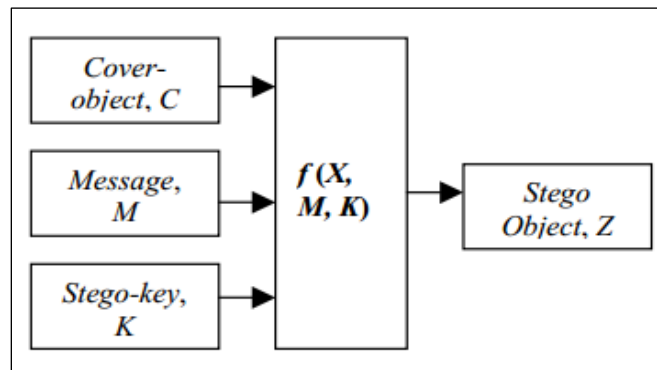


Figure 1: Basic Steganography Model

148

149

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

152 **Cryptography And Steganography**

153

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

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

164 *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 is 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.

165

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

169 **Steganography Techniques**

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

172 **1. Least Significant Bits**

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

178 Digital data is computed in binary format, and similarly to numerical notation, the rightmost  
 179 digit is considered the lowest digit whereas the leftmost is considered the highest digit in  
 180 terms of significance. Due to the positional notation, the least significant bit is also known as  
 181 the rightmost bit. It is the opposite of the most significant bit, which carries the highest value  
 182 in a multi-bit binary number as well as the number which is farthest to the right. In a multi-

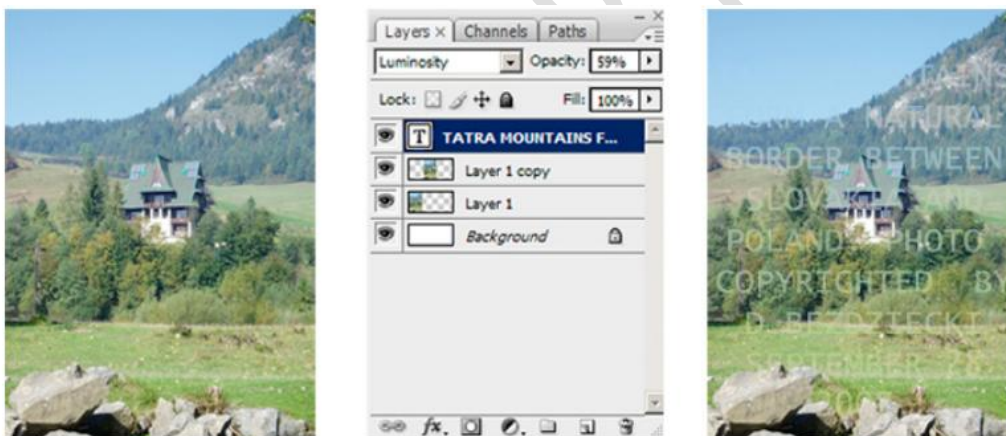
183 bit binary number, the significance of a bit decreases as it approaches the least significant bit.  
184 In the binary number system, the most significant bit can be either 0 or 1.  
185 When a transmission of binary data is done with the least significant bit first technique, the  
186 least significant bit is the one which is transmitted first, followed by other bits of increasing  
187 significance. The least significant bit is frequently employed in hash functions as in [29] [30]  
188 [31], and checksums and pseudorandom number generators [32].  
189 LSB insertion is a simple approach to embedding information in a file. The simplest  
190 steganographic techniques embed the bits of the message directly into the least significant bit  
191 plane of the cover-object in a deterministic sequence. Modulating the least significant bit  
192 does not result in human perceptible difference because the amplitude of the change is small.  
193 In recent times, the LSB embedding technique is one of the most important steganography  
194 techniques [33]. LSB techniques is mostly implemented in the spatial domain. In this method  
195 the least significant bit of some or all the bytes inside an image or media is replaced with bits  
196 of the secrete message. The LSB embedding approach has become the basis of many  
197 techniques that hide messages within multimedia carrier data. LSB embedding can also be  
198 applied in the data domains for example, embedding a hidden message into the color values  
199 of RGB bitmap data, or into the frequency coefficients of a JPEG image.

200

## 201 **2. Masking and Filtering**

202 Masking and filtering techniques are usually restricted to 24 bits and gray scale images.  
203 These techniques hide information by marking an image, in a manner similar to paper  
204 watermarks. The techniques perform analysis of the image, thus embed the information in  
205 significant areas so that the hidden message is more integral to the cover image than just  
206 hiding it in the noise level [34]. This technique is much more robust than the LSB  
207 replacement with respect to compression since the information is hidden in the visible parts

208 of the image. However, this technique can be applied only to gray scale images and restricted  
209 to 24 bits thereby making it unsuitable for audio steganography implementation [35].  
210 According to N. F. Johnson and S. Jajodia, Masking and filtering techniques is the process of  
211 hiding information by marking the image, in a manner similar to paper watermarks.  
212 Watermarking techniques may be applied without fear of image destruction due to lossy  
213 compression because they are more integrated into the image [17].  
214 Figure 2, illustrates how masks and filters can be embedded into images without destroying  
215 the original quality of a photographic image [36]. The entire photograph has been  
216 watermarked. To perform steganography within an image, the luminance of the masked area  
217 is increased by 15 percent. The luminance must be changed by a smaller percentage, so the  
218 mask would be undetected by the human eye [37].

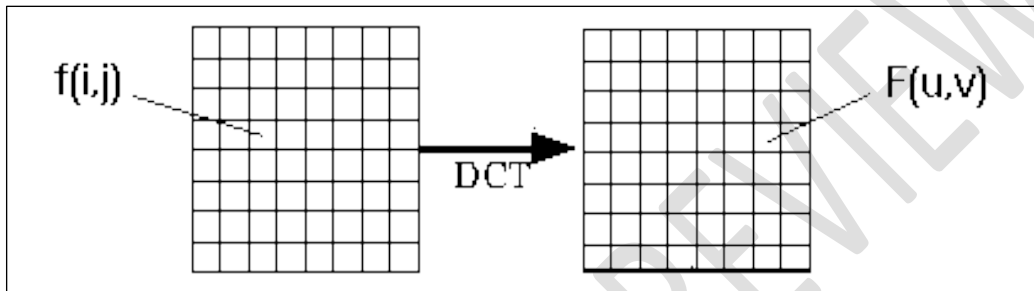


219  
220 *Figure 2: Masking and Filtering Method*

### 221 3. Transforms Techniques

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

227 DCT is one of the general orthogonal transform for digital image processing with advantages  
 228 such as high compression ratio, small bit error rate and good information integration ability  
 229 [38]. DCT coefficients are used for JPEG compression. It separates the image into parts of  
 230 differing importance. It transforms a signal or image from the spatial domain to the  
 231 frequency domain as shown in Figure 3. It can separate the image into high, middle and low  
 232 frequency components.



233  
 234 *Figure 3: The Discrete Cosine Transform (DCT)*

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

241  
 242 The general equation for a 1D (N data items) DCT is defined by the following equation:

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

243  
 244 The general equation for a 2D (N by M image) DCT is defined by the following equation:

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

245 A wavelet is a small wave which oscillates and decays in time domain. The Discrete Wavelet  
246 Transform is a relatively recent and computationally efficient technique. Wavelet analysis is  
247 advantageous as it performs local analysis and multi-resolution analysis. Analyzing the signal  
248 at different frequencies with different resolutions is called multi-resolution analysis (MRA).  
249 Wavelet analysis can be of two types: continuous and discrete [38]. In Discrete Wavelet  
250 Transform (DWT) based steganography approaches the wavelet coefficients of the cover  
251 image(object) are modified to embed the secret message [40].

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

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

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

257

### 258 **Categories of Steganography**

259 There are a lot of digital file format currently in used today. All these digital formats are suitable  
260 for the implementation of steganography, however those digital formats with high degree of  
261 redundancy is more prefer and suitable than those with low degree of redundancy. For a file to be  
262 of high degree of redundancy implies that the bits of that file can be changed without detecting  
263 the change easily. Example of such objects is video, audio and image files. With this, image,  
264 video, and audio files are more suitable objects for the implementation of steganography. Figure  
265 2 shows the various categories of file formats that can be used for steganography.

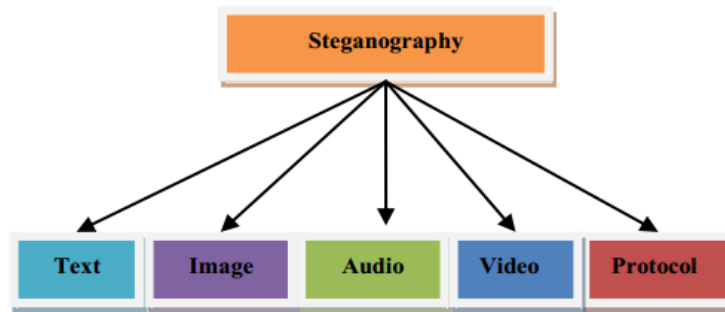


Figure 4: Categories of Steganography

266

267

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

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

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

- 281 • **Substitution system** replace unneeded parts of a cover with a secrete data.
- 282 • **Transform domain techniques** embed secrete message in a transform space of the  
 283 signal (e.g., in frequency domain).
- 284 • **Spread spectrum techniques** implement ideas from spread spectrum communication.
- 285 • **Statistical methods** encode data by changing several statistical properties of a cover and  
 286 use assumption testing in the extraction process.

287 • **Distortion methods** accumulate data by signal alteration and measure the deviation from  
288 the original cover in the decoding step.

289 • **Cover generation schemes** encode data in the approach a cover for secrete  
290 communication is created.

### 291 **Properties of Steganography**

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

294 • *Imperceptibility*: The goal of steganography is that object should appear identical before  
295 and after hiding.

296 • *Embedding Capacity*: It is the capacity of steganographic algorithm based on the  
297 quantum of message it can secretly transmit. Capacity is one of the challenging case in  
298 steganography.

299 • *Robustness*: Robustness refers to the degree of difficulty required to tear down embedded  
300 information without destroying the cover object itself.

301 • *Undetectability*: This property is as important as imperceptibility. It is the rate and  
302 accuracy at which a media containing an embedded data cannot be detected using  
303 statistical or technological means.

304

## 305 **III. SYSTEM DESIGN AND METHODOLOGY**

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

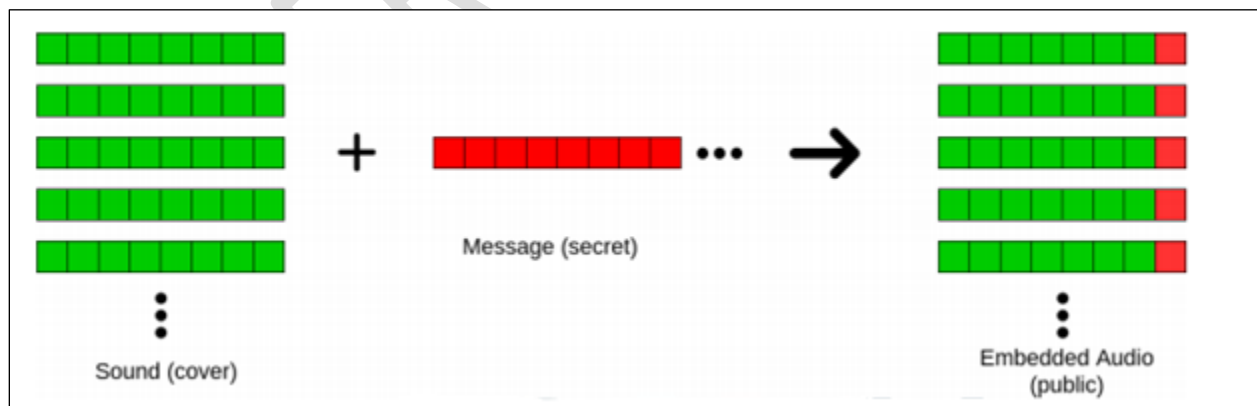
### 309 **The Least Significant Bit (LSB) Audio Steganography Implementation**

310

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

320 LSB algorithm is a classic Steganography method used to conceal the existence of secret data  
321 inside a “public” cover. The LSB or “Least Significant Bit”, in computing terms, represents the  
322 bit at the unit’s place in the binary representation of a number. For example, we can represent the  
323 decimal number 170 in binary notation as 10101010. The least significant bit, in this case, is 0.  
324 In the simplistic form, LSB algorithm replaces the LSB of each byte in the “carrier” data with  
325 one bit from the “secret” message [44].

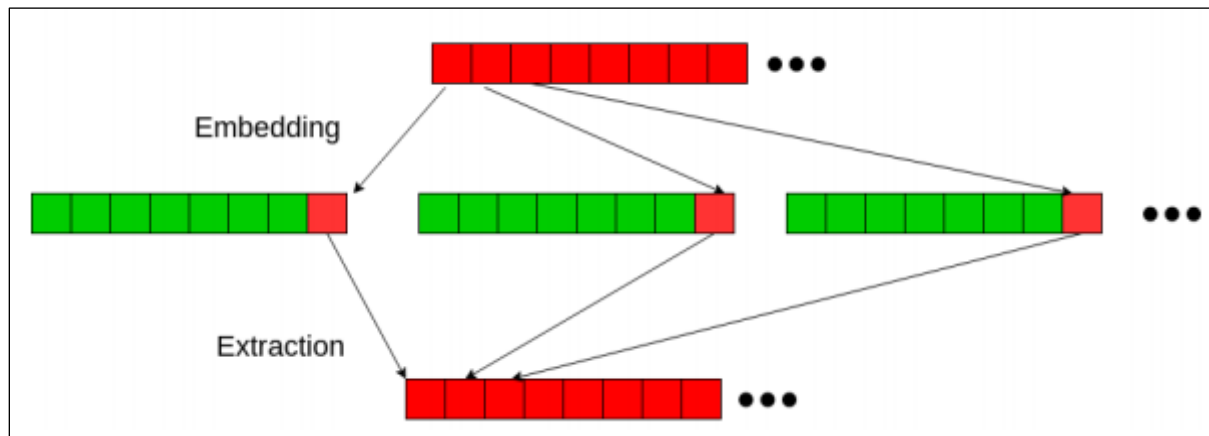
326



327  
328

*Figure 5:Encryption process*

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



332

333

*Figure 6: Embedding and Extraction process*

334

The advantage of the LSB techniques lies in its ease of implementation and simplicity. The LSB

335

method allows high embedding capacity and uses different frequency levels for more security.

336

Hiding the secret data using audio lowers the chances of the secret data being detected. This

337

techniques for audio files work smoothly for all audio format as implemented in Java. Using

338

these algorithms for encoding and decoding, one can retrieve the secret message exactly as the

339

original data.

340

#### 341 **IV. RESULTS AND IMPLEMENTATION**

342

The purpose of this study is the implementation of steganography using Least Significant Bit

343

methods. This section seeks to present the result of the study by analyzing and interpreting the

344

data collected, methods and techniques used in conducting the study. Different approaches were

345

put in place in order to have better and deeper representation of the results by implementing LSB

346

technique for hiding data in audio objects. For the implementation of the systems, the above

347

stated scenario was considered and implemented using Java Programming Language. In all,

348

testing was done through the normal viewing using the human senses to distinguish the original

349

and the resultant object. The implementation of the Secure Transit Data System (STDS) was

350 implemented in two folds, that is, encoding and decoding Audio Steganography presented using  
351 the LSB processes.

### 352 **Audio Steganography Implementation**

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

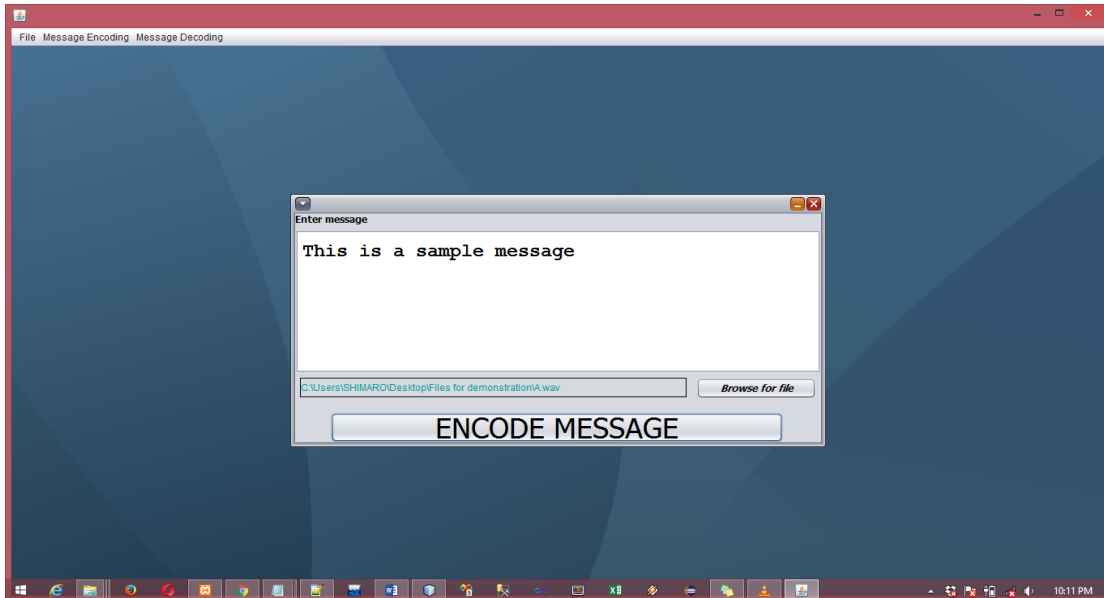
359 Looking at the binary code of numbers from 0 to 9, and from A (a) to P (p) for both casing, it can  
360 be observed that, these characters are only different in their respective last 4 bits. Thus, their first  
361 4 bit are similar, thereby implying that, any number or alphabet can easily be represented by the  
362 last 4 bits and adding either 0 or 1 at its first position. To differentiate whether the character is  
363 number, uppercase alphabet or lowercase alphabet control symbols are used which is of the same  
364 type as that of number or alphabet.

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

### 370 **Audio Steganography Encoding Process**

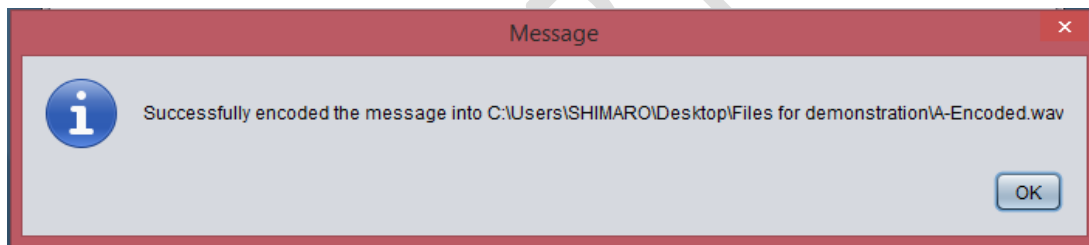
371 The underlying technology for the encoding process is the LSB. In summary, the encoding  
372 algorithm takes in a text to be embedded as an input, convert the text into a 5-bit code by  
373 checking the redundancy in the binary coding structure of the characters involved. The next is to  
374 the read the audio file as the cover object. The selected audio file or the cover object is then used

375 to hide the converted 5-bit code of text using the proposed methodology. This process is repeated  
376 until the entire message is embedded successfully into the audio file.



377  
378

*Figure 7: Audio Embedding user interface*



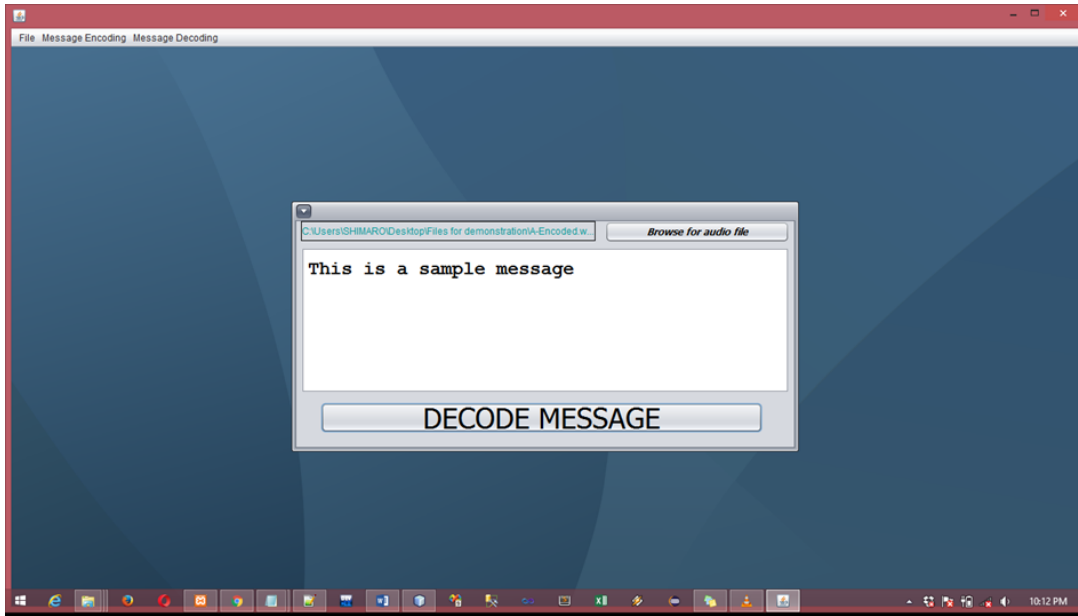
379  
380

*Figure 8: Audio Encoding Status dialog*

381

### 382 **Audio Steganography Decoding Process**

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



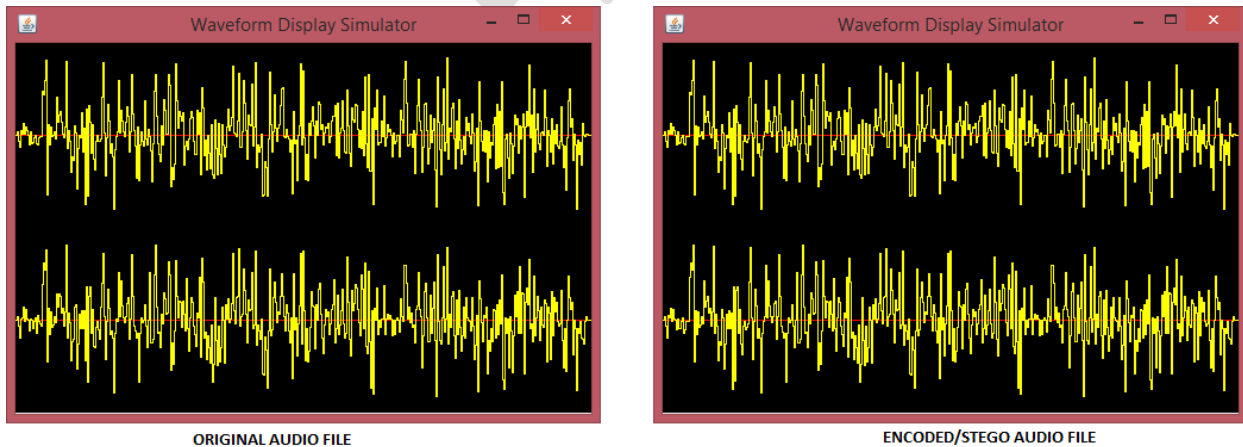
388

389

*Figure 9:Audio Decoding User Interface*

390 **Experimental Result**

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

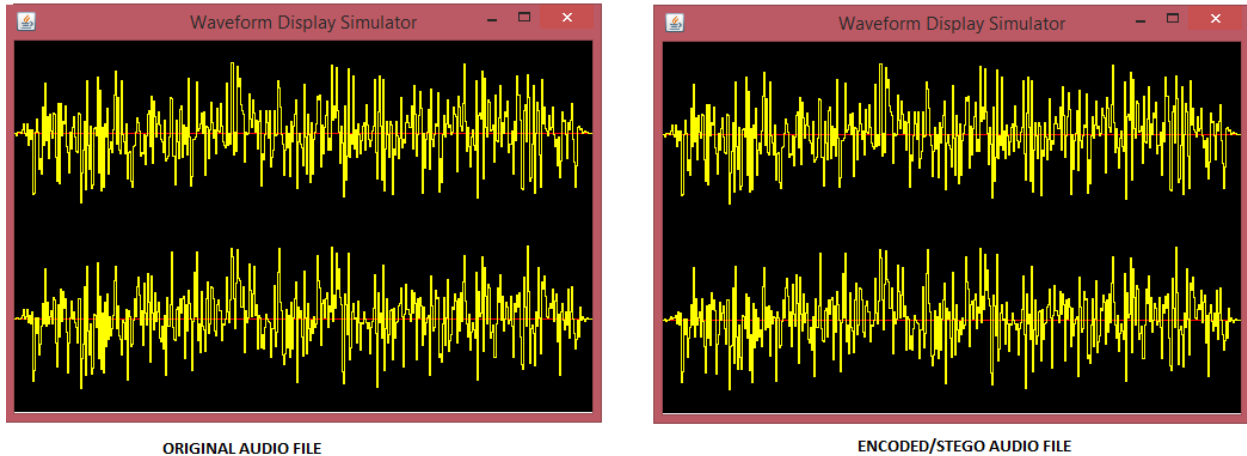


395

396

*Figure 10:Audio file sample A waveform*

SAMPLE B

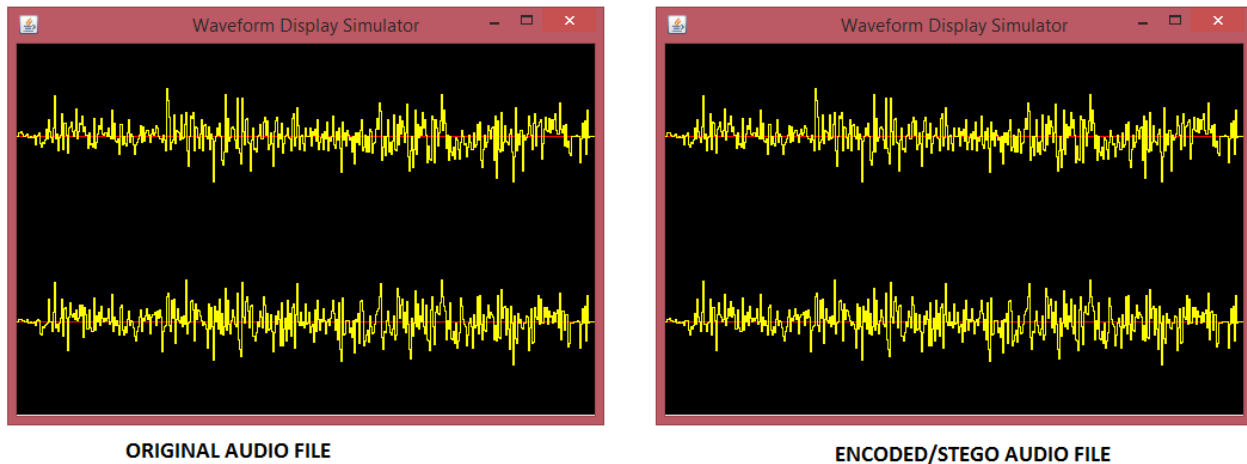


397  
398

Figure 11:Audio file sample B waveform

399

WAVEFORM SAMPLE C



400  
401

Figure 12:Audio file sample C waveform

402  
403

## V. CONCLUSION

404 This study set out to secure data in transit using audio steganography. Steganography is one of  
405 the ways by which data in transit can be secured without attracting unnecessary attention from  
406 intruders. The algorithm used in this research proves to be one of the simplest ways of securing  
407 data using audio steganography. The methods employ the LSB approaches by using audio files  
408 as the stego object for the implementation based in Java Programming Language. The  
409 experimental results also proved to be one of the best methods of implementing steganography.

410 The accuracy of the stego objects as compared to the original objects is of high quality and  
411 similarity. The processing time of both the encoding and decoding algorithms as compared to  
412 other implementation is faster, more robust and efficient.

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

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

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

424

425 **Ethical Approval:**

426 As per international standard or university standard ethical approval has been collected and  
427 preserved by the authors.

428

429

430 **VI. REFERENCES**

431

- [1] IBM, "Data Security," IBM, 18 June 2018. [Online]. Available: <https://www.ibm.com/topics/data-security>. [Accessed 15 December 2021].
- [2] B. Dickson, "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] i. T. M. a. D. S. Ibrahim, "Effect of Communication Channel on Transferred Data," *Diyala Journal of Pure Science*, vol. 9, no. 4, pp. 75-92, October 2013.
- [4] M. A. Qadir and I. Ahmad, "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] J. M. a. S. Mangal, "An Overview of Image Steganography using LSB Technique," *IJCA Proceedings on National Conference on Advances in Computer Science and Applications (NCACSA 2012)*, vol. 3, pp. 10-13, 2012.
- [6] N. P. P. Honeyman, "Detecting Steganographic Content on the Internet," University of Michigan, Michigan, 2001.
- [7] S. Alekhya Orugonda, "Hiding the Military Secret Message by Reversible Data Hiding," *International Journal of Engineering and Innovative Technology(IJEIT)*, vol. 3, no. 4, pp. 165-168, 2013.
- [8] T.-J. W. J.-M. C. Shin-Yan Chiou, "Design and Implementation of a Mobile Voting System Using a Novel Oblivious and Proxy Signature," *Security and Communication Networks*, vol. 2017, pp. 1-16, 2017.
- [9] C. R. C. K. R. V. a. L. M. P. K. B. Raja, "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] N. S. M. S. B. Ayush Singhal, "An Advanced Approach for Implementation of Audio Steganography," *International Journal For Science, Technology and Engineering*, vol. 1, no. 12, pp. 66-71, 2015.
- [11] R. Tanwar and M. Bisla, "Audio Steganography," in *2014 International Conference on Reliability Optimization and Information Technology (ICROIT)*, 2014.
- [12] R. S. Kazem Qazanfari, "A new steganography method which preserves histogram: Generalization of LSB++,," *Information Sciences*, vol. 277, pp. 90-101, 2014.
- [13] Y. V. M. Baritha Begum, "LSB Based Steganography based on Text Compression," *Procedia Engineering*, vol. 30, pp. 703-712, 2012.
- [14] Y. Wiseman, "Protecting Seaport Communication System by Steganography Based Procedures," *International Journal of Security and Its Applications*, vol. 8, no. 4, pp. 25-36,

2014.

- [15] S. C. a. A. Jadhav, "Steganography an Art of Hiding Data," *International Journal on Computer Science and Engineering(IJCSE)*, 2009.
- [16] J. S. Johnson N.F., 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] N. F. J. a. S. Jajodia, "Exploring steganography: Seeing the unseen,," *Computer*, vol. 31, no. 2, pp. 26-34, 1998.
- [18] P. H. N. Provos, "Detecting Steganographic Content on the Internet," CITI Technical Report 01-11, Michigan, 2021.
- [19] R. Anderson, "Analysis of LSB Based Image Steganography Techniques," *IEEE*, pp. 474-481, 1998.
- [20] C. Cachin, "An Information-Theoretical Model for Steganography," in *In Proceeding of 2nd Information Hiding Workshop*, 1998.
- [21] F. P. S. Katzenbeisser, "Defining security in Steganographic Systems," in *Proc. SPIE 4675, Security and Watermarking of Multimedia Contents IV*,, 2002.
- [22] R. J. A. a. M. G. K. F. A. P. Petitcolas, "Information hiding-a survey," in *In Proceedings of the IEEE*, 1999.
- [23] C. H. Gary C. Kessler, "Chapter 2- An Overview of Steganography," in *Advances in Computers*, vol. 83, Marvin V. Zelkowitz, Ed., Elsevier, 2011, pp. 51-107.
- [24] J. F. T. H. Miroslav Goljan, "New blind steganalysis and its implications," in *Proceedings Volume 6072, Security, Steganography, and Watermarking of Multimedia Contents VIII*,, San Jose, 2006.
- [25] M. Parahar, "Difference between Steganography and Cryptography," TutorialPoint, 15 April 2020. [Online]. Available: <https://www.tutorialspoint.com/difference-between-steganography-and-cryptography>. [Accessed 16 December 2021].
- [26] M. Gasser, *Building A secure Computer Systems*, USA: Van Nostrand Reinhold Co, 1998.
- [27] S. L. N. F. M. a. L. O. J. T. Brassil, "Electronic marking and identification techniques to discourage document copying,," *IEEE Journal on Selected Areas in Communications*,, vol. 13, no. 8, pp. 1495-1504, 1995.
- [28] Techopedia, "Least Significant Bit(LSB)," Janalta Interactive, 2021. [Online]. Available: <https://www.techopedia.com/definition/8030/least-significant-bit-lsb>. [Accessed 11 December 2021].
- [29] M. H. Abood, "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] M. S. Ms.Shridevishetti, "A Secure Image Steganography based on RSA Algorithm and Hash-LSB Technique," *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ICESMART*, vol. 3, no. 19, pp. 1-7, 2015.
- [31] B. R. al, "Hash Based Least Significant Bit Technique For Video Steganography," *International Journal of Engineering Research and Applications*, vol. 4, no. 1.3, pp. 44-49, 2014.
- [32] D. C. Peterson, "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] A. D. S. B. a. S. D. 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*, vol. 2, no. 5, pp. 89-95, 2014.
- [34] S. a. R. K. Tiwari, "Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization," *International Journal of Computer Science and Network Security*, vol. 8, no. 1, pp. 228-233, 2008.
- [35] J. A. C. a. D. Vaishali, "Image steganographic techniques with improved embedding capacity and robustness," in *2011 International Conference on Recent Trends in Information Technology (ICRTIT)*, Chennai, India, 2011.
- [36] P. K. S. a. D. R. K. Gupta, "A Review of Digital Image Steganography," *Journal of Pure and Applied Science & Technology*, vol. 2, no. 1, pp. 98-106, 2012.
- [37] M. Project, "Image Steganography Techniques," M4JPEG Project, 2018. [Online]. Available: <https://digitnet.github.io/m4jpeg/about-steganography/image-steganography-techniques.htm>. [Accessed 17 December 2021].
- [38] V. P. a. P. Bhat, "Transform Domain Techniques for Image Staganography," *INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING*, vol. 3, no. 1, pp. 65-58, 2015.
- [39] A. Watson, "Image Compression Using the Discrete Cosine Transform," *Mathematical Journal*, vol. 4, no. 1, pp. 81-88, 1994.
- [40] V. K. a. D. Kumar, "Performance evaluation of DWT based image steganography," in *2010 IEEE 2nd International Advance Computing Conference (IACC)*, Patiala, India, 2010.
- [41] G. E. G. & C. P. Tzanetakis, "Audio Analysis using the Discrete Wavelet Transform.," *Semantic Scholar*, pp. 1-6, 2001.
- [42] D. Marshall, "Dave Marshall Multimedia," 10 April 2001. [Online]. Available: <https://users.cs.cf.ac.uk/Dave.Marshall/Multimedia/node228.html>. [Accessed 17 December 2021].
- [43] B. S. a. R. Shanthakumari, "Efficient Adaptive Steganography for Color Images Based on LSBMR Algorithm," *ICTACT Journal on Image and Video Processing*, vol. 02, no. 03, pp. 387-392, 2012.
- [44] S. K. Arora, "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] M. Ramkumar and A. N. Akansu, "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.

432

433

434

435

436