High Capacity Audio Steganography with RSA Encryption

Priyanka Sharma[1], Dr. Amit Shrivastava[2], Dr. Kapil Chaturvedi[3]

[1]M.tech. Student, [2]Guide and HOD, [3]Co-Guide

Department of Computer Science and Engineering, SIRT-S, Bhopal

Abstract-Transmission of information is being quite easy these days and in some microseconds. Development of technological facilities also added the leak or security breach of secure and sensitive information like bank account details, card details, net banking details, server information details of any company or different customer usage details. Information cannot not be kept secure which is being used many times, like passwords etc. So researchers have been working to secure these information using many ways like secure connection between transmitter and receiver, change the format of data i.e. encryption of data, and steganography. Steganography is the method of transferring information between two people by hiding behind some visible or audible media. Which is near impossible for common people to understand the existence of any secure/sensitive information can be with audio or with audio. In this work an efficient audio steganography algorithm is designed and to increase the security of secret message RSA encryption is used for being hidden with the audio. The audio used as a cover audio has negligible difference after adding secret information with the audio, so no one can predict that there is some information hidden. The secret information hidden using previous algorithm is 100 byte in size and with proposed algorithm 547 bytes of data can be hidden with audio, which is added feature of proposed algorithm.

Keywords - Audio, RSA, Reversible, Steganography, Secret Message.

I. INTRODUCTION

Because of the wide range of applications for which Computers are being used, providing security to data has become important. The data security is required for the businessmen, the military users, the home users and the computer professionals. Often the data is transmitted over Internet. As the number of Internet users rises, the concept of Internet security has also gained importance. There are many ways to transfer data to a destination like e-mails, social sites, etc. At the same time, it has become easier to modify and misuse the valuable information. The Steganography and Cryptography are the two techniques that are being considered for secure transmission of data.

Steganography is derived from the Greek word “Steganos” which means secret or covered and graphy‟ means drawing or writing. Steganography is the science and art of information embedding so that its existence could not be revealed. Secret data is embedded in such a manner that the information presence is obscured. Steganography is used to bring out embedded exchanges pairing with existing communication methods. Steganography helps not only to keep others from understanding that the secret data exists but also to bypass drawing suspicion to hide the information.

Steganography received less attention recently from the community of research and from industries. However this situation is changing rapidly. For two main reasons there has been a fast advancement of interest in Steganography:

(i) The broadcasting and the publishing industries have become interested to hide serial numbers and encrypted copyright marks in books, multimedia products, audio recordings, and digital films.

(ii) To decrease the availability of encryption amenities various governments have motivated crowd to study the techniques of which seemingly harmless information can be hidden.

Steganography software is becoming effective to hide the information in various multimedia files such as audio, audio, video or text files.

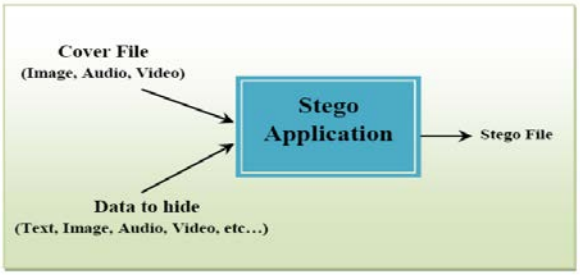


Figure 1.1 A Steganography Application System.

Within a cover file the Steganography system embeds various types of information. The resulting stego file contains hidden information.

Steganography utilizes medium, for example, audio, sound, video, or text file to cover any data in it, so that does not draw any interest and resembles a harmless medium. Cover medium, for example, digital audio, video and photograph turned into the undeniable decision. Stego media are the media, which contain the secret data while cover media are the plain file. As of late, the audios have been a prominent decision as a way to cover essentially in view of its excess in the portrayal and the capacity to

infiltrate applications in everyday life. Throughout the years, numerous algorithms have been proposed to hide data in audios and growing new algorithms are a point of ebb and flow investigate. In this postulation, probably the most famous and powerful among audio Steganography algorithms are broke down for their instruments, focal points and drawbacks, which could be a profitable guide for future research scope openings.

The three significant classifications of steganographic techniques are: spatial domain strategy, frequency domain strategy and adaptive methods. The last one can be utilized both in past two cases, as it is considered as extraordinary cases. Once more, spatial domain and frequency domain are two expansive orders in audio steganography. In spatial domain, the hidden data is embedded legitimately in the intensity of the pixels i.e in spatial area technique, a steganographer made an alteration of the hidden message and the cover file, which suggests change at the phase of the least noteworthy bit. This technique is less muddled and has more powerful than the other two kinds of strategies, while in the event of frequency domain, first audio is transformed to frequency domain or transform domain and after that, the hidden data is embedded in the transform coefficients.

II. RSA ENCRYPTION ALGORITHM

The rising growth of data communication technique and electronic transactions over the web has made system security to become the most important issue over the network. To provide modern security features, public-private key cryptosystems are used. One of such cryptosystem is RSA algorithm. Though computation in RSA takes more time by if the message to be encrypted is generated randomly then RSA will prove to be good cryptography algorithm for system security [7].

For the better working of RSA based cryptosystem the system has the public key for decryption and the user will have the device containing the private key assigned to the user. And instead of entering the password the user will just have to insert the device to the system and the system will do the cross checking of the password for that particular user and allow access accordingly [8].

1. Public-key encryption

In RSA, encryption keys are made public while the decryption keys are kept private, so only the person with the correct decryption key can decipher an encrypted message. Everyone has their own encryption and corresponding decryption keys. The keys are made in such a way that the decryption key cannot be easily deduced from the public encryption key.

2. Digital signatures

The receiver may need to verify that a transmitted message is actually originated from the sender, and didn't just come from authentication. This is done with the help of the sender's decryption key, and later the signature can be verified by anyone, using the corresponding public encryption key. Signatures therefore cannot be copied. Also, no signer can later deny having signed the message.

The various steps involved in RSA algorithm are :

A. Finding large prime numbers

Finding ‘n’ is the first step of the algorithm, where ‘n’ is the product of two prime numbers ‘p’ & ‘q’. The number ‘n’ will be revealed in the encryption and decryption keys, but the numbers ‘p’ and ‘q’ will not be explicitly shown. The prime numbers ‘p’ and ‘q’ should be large such that it will be very difficult to derive from ‘n’.

$$n = p \times q \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Eq.1$$

B. Finding the public key (e)

Choose a number ‘e’ such that ‘e’ is co-prime to $\varphi(n)$, where $\varphi(n)$ is the Euler’s totient function that counts the number of positive integers less than or equal to ‘n’ that are relatively prime to ‘n’ i.e.

$$\varphi(n) = (p-1)(q-1) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Eq.2$$

$$Gcd\big(e, \varphi(n)\big) = 1 \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Eq.3$$

where, $1 < e < \varphi(n)$

C. Determine the private key (d)

Determine the private key ‘d such that‘d’ is the multiplicative inverse of the public

key ‘e’ i.e.

$$d^{-1} = e\left(mod\big(\varphi(n)\big)\right) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Eq.4$$

C. Encryption

Let ‘m’ be the message (integer type) that is to be encrypted using public key ‘e’ to give the encrypted message as ‘c’ where ‘c’ is calculated as

$$c = m^e\big(mod(n)\big) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Eq.5$$

D. Decryption

The decrypted message ‘m’ is found out using the private key‘d’ and is calculated

as:

$$m = c^d\big(mod(n)\big) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Eq.6$$

III. PROPOSED METHODOLOGY

In this proposed work, first, encode secret message utilizing RSA encryption algorithm. And after that applying proposed Substitution algorithm, implant

message bits to the sound piece stream (16 bit test) in arbitrary and higher layer positions (increment the robustness) to get a gathering of chromosomes. Presently RSA Algorithm administrators are utilized to get the cutting edge chromosomes.

In this work, an intelligent RSA algorithm is utilized to install the message bits in the more profound layers of tests and modify different bits to diminish the mistake and if modification isn't feasible for any example it will disregard them, which aides in accomplishing higher limit which alludes to the measure of data that an information concealing plan can effectively insert without presenting perceptual contortion in the stamped media and robustness which estimates the capacity of implanted information or watermark to withstand against purposeful and unexpected attacks.

As a performance measure for audio twisting due to hiding of message, the outstanding peak signal-to noise ratio (PSNR), which is arranged under distinction mutilation measurements, can be connected to stego sounds execution advancement of proposed work has been done dependent on PSNR execution of proposed methodology.

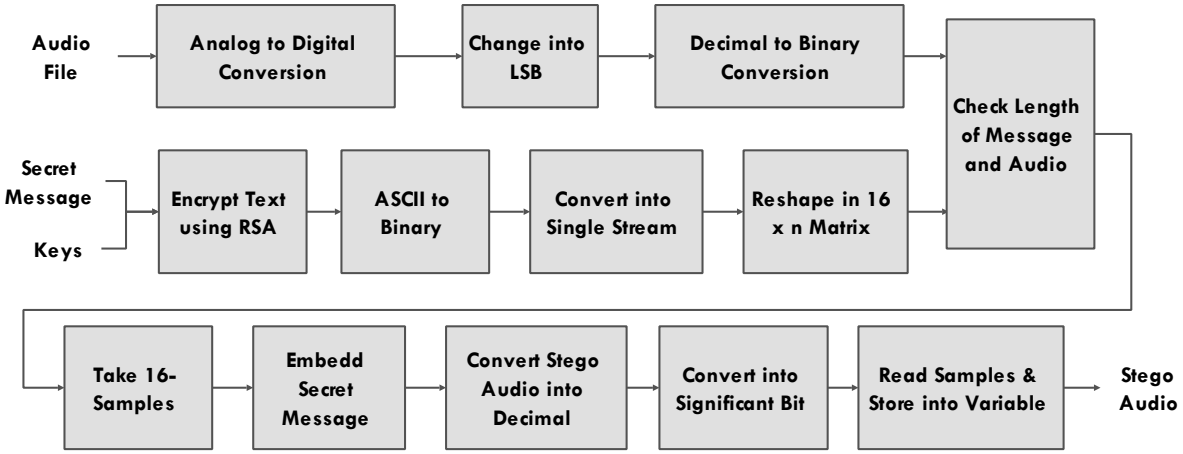


Fig. 3.1 Block Diagram of Embedding Process

a. Embedding Process

In audio steganography procedure the spread audio tests are divided to get guess and definite coefficients. The secret message is encoded powerfully utilizing the measurements of the message. The duration of the secret message is used for encryption in the suggested approach. The scrambled secret message is covered up in the point by point coefficients of the spread. In the extraction stage, the stego audio tests are changed utilizing reversible methodology. The encoded secret message is recovered from the point by point coefficients of the spread. At that point it is unscrambled utilizing the equivalent factual data. Fig. 3.1 demonstrates the square graph of proposed algorithm. and Fig. 3.2 demonstrates the progression of procedure of extraction process. The embedding procedure is as following.

First the audio record is handled in MATLAB condition the audio documents is sectioned and phase contrasts are determined and dependent on phase distinction computation a grid of phase is made and a secret data which is to be insert in audio are changed over into its identical binary structure and included audio document. The audio document is remade again an embedded stego audio is acquired as an output of embedded square.

The point of Extraction RSA is to implant the secret back rub into the multi-media content audio in proposed work. The presentation of reversible steganography is assessed in the capacity to distinguish the of alteration. Fundamentally the misfortune less compression technique is utilized to embed. The proposed work process flow has been provided in Fig. 3.4.

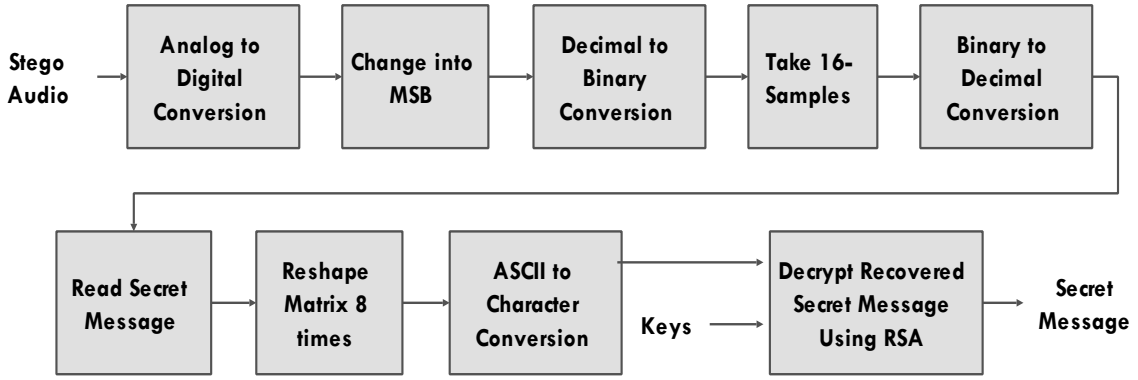


Fig. 3.2 Block Diagram of Extraction Process

Fig. 3.3 Flow Chart of Embedding Process

b. Extraction Algorithm

At the receiver end will be removed from the embedded audio file. If the audio extracted matches with the stego text, the audio will be recognized at the end of the receiver. Fig. 3.2 Shows the block representation of the proposed algorithm for extraction.

IV. SIMULATION OUTCOMES

In this examination Implementation and simulation of proposed audio steganography utilizing RSA plot with higher length of secret message has finished in MATLAB Simulation condition. The led work in this exploration intends to structure a successful audio steganography technique to discover an answer for the security issue past techniques. Likewise, it offers an effective strategy to shroud audio data in more protected manner with the utilization of the MATLAB program. The Secret information is encrypted using an audio steganography strategy that increases safety and decreases the technique's complexity.

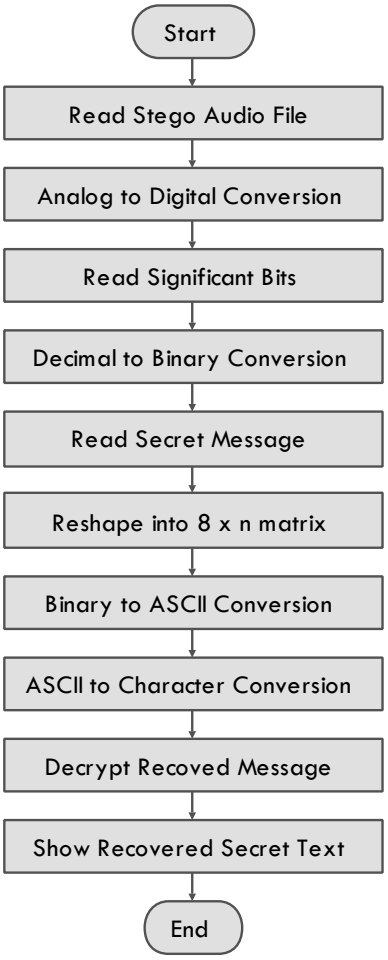


Fig. 3.4 Flow Chart of Extraction Process

Results are provided for various audio files with varying amounts of concealed information. Stego audio quality is evaluated with PSNR.

The execution of this technique is assessed with three sorts of payload limit: enormous, medium, and little. The spread audio sign is a music file and the secret file is a content file, both having fixed piece tests.

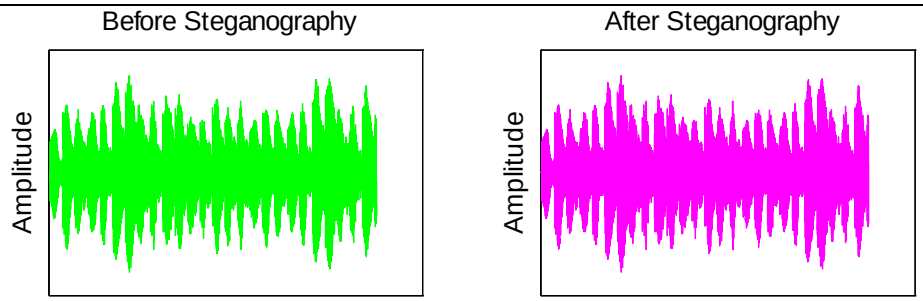
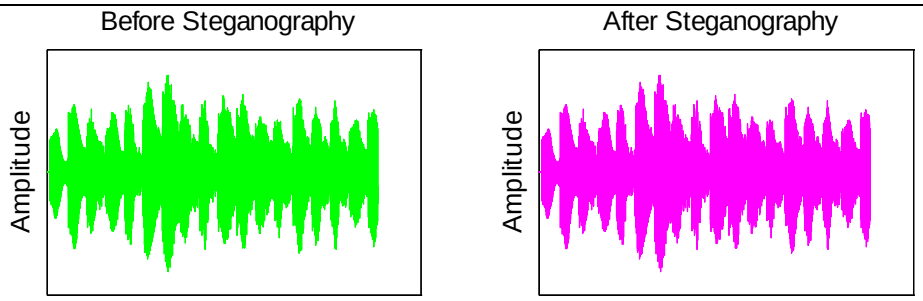
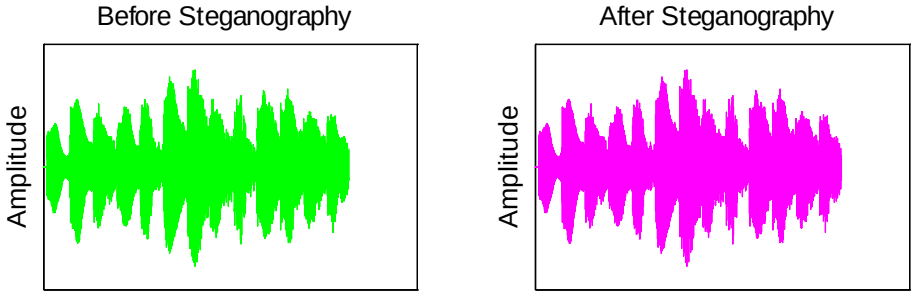
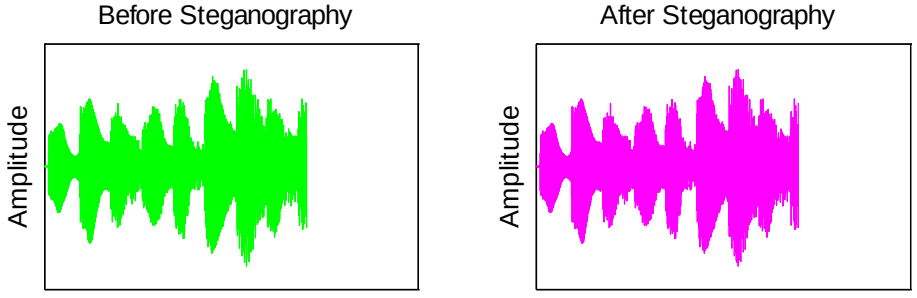
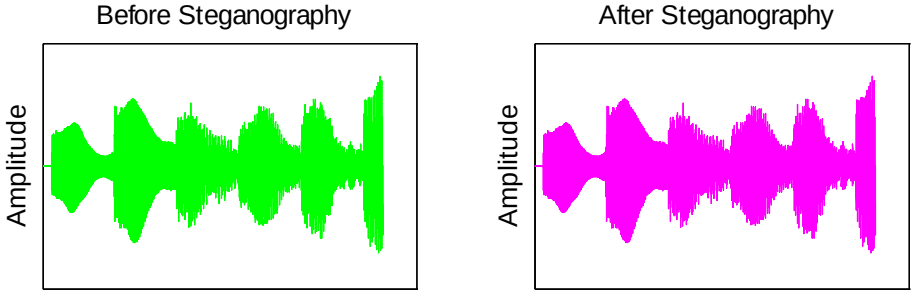
Keeping spread audio tests steady, the secret content examples sizes are fluctuated to survey the presentation of the technique and in this manner the variety of the security with limit is contemplated. Enough number of tests is considered for spread audio, and the secret content examples are taken as half, same, and twofold that of the spread audio. The secret content file is compacted and by implication encoded by reversible algorithm. The whole procedure has finished in MATLAB recreation.

The relative examination of proposed work with existing base work has given in Table 1 where past work from base paper [1] has taken as reference and proposed fill in as augmentation of base work. The correlation has analyzed

as far as PSNR value in dB for different secret message size and audio file size.

For audio file size 254945, secret message of length 100 byte has past PSNR 50.67 has reached out in proposed work to 547 chomp of secret content size for filed audio file size accomplished PSNR 106.04 dB.

Table 1 Comparison of Performance between Previous [1] and Proposed Work (Our)

Size of Audio	***Before and After Waveforms***	***PSNR***
254945		106.04 dB
172616		104.32 dB
128985		103.01 dB
82756		101.09 dB
54026		98.58 dB

The above assessment dependent on reenactment has done for various audio tests, for example, 172616, 128985, 82756, and 54026. The relating PSNR for all examples for fixed message 547 byte has accomplished better performance against past base work.

Table 2 shows the comparative analysis of proposed work with respect to previous base work in terms of secret message size and corresponding PSNR value recorded for a fixed audio file size.

Table 2: Comparison of Performance between Previous [1] and Proposed Work (Our)

File Size	*Previous [1]*		*Proposed(Our)*	
	Secret Message Size (bytes)	*PSNR (dB)*	*Secret Message Size (bytes)*	*PSNR (dB)*
254945	100	50.67	547	106.04
172616	100	39.43	547	104.32
128985	100	68.25	547	103.01
82756	100	40.31	547	101.09
54026	100	42.60	547	98.58

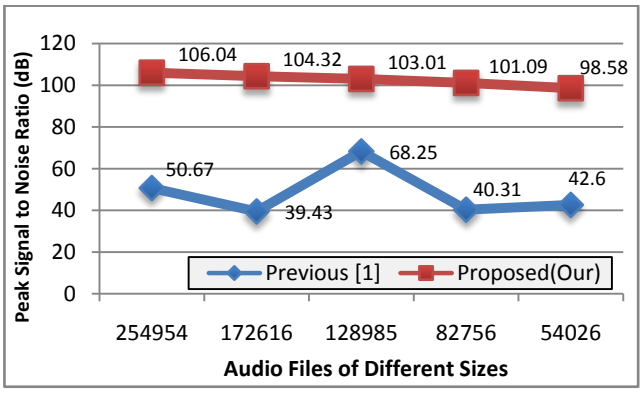


Fig. 4.1 Side by Side Comparison of PSNR with Previous [1] Work

The graphical representation of comparative analysis of proposed work and previous base work has shown in Fig. 4.1 in terms of PSNR in dB. It can be concluded to analyze bar chart that proposed work has better performance against existing work.

V. CONCLUSION AND FUTURE SCOPE

In this examination, presently multi day, and turns into a dynamic theme in both private and government areas. In our proposed work researches that audio steganography improvement by joining audio and picture through RSA falls into a few classes viz. For example, the exacting method for selecting the secret message, audio information to be incorporated into the media content. The suggested framework uses the RSA method used to embed data, which changes the content of the media marginally. At that point the RSA algorithms have been additionally considered in order to play out the extraction without data to proposed higher PSNR incentive to the past work to various secret message sizes.

The work presented in this Study is, hopefully, appreciated inside the characterized degree, yet look into never closes, along these lines, future research is relied upon to investigate skylines past the extent of this work. It is trusted that the impediments of this work would be considered as the start for the examination in the future. The viability and effectiveness of the proposed framework can be improved and upgraded in the method for limit, Security and robustness of audio steganography.

REFERENCES

[1] R. Indrayani, H. A. Nugroho and R. Hidayat, "An evaluation of MP3 steganography based on modified LSB method," 2017 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, 2017, pp. 257-260

[2] S. P. Rajput, K. P. Adhiya and G. K. Patnaik, "An Efficient Audio Steganography Technique to Hide Text in Audio," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, 2017, pp. 1-6.

[3] Z. Sultana, F. Jannat, S. S. Saumik, N. Roy, N. K. Datta and M. N. Islam, "A new approach to hide data in color image using LSB steganography technique," 2017 3rd International Conference on Electrical Information and Communication Technology (EICT), Khulna, 2017, pp. 1-6

[4] M. Tayel, A. Gamal and H. Shawky, "A proposed implementation method of an audio steganography technique," 2016 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, 2016, pp. 180-184

[5] P. Johri, A. Mishra, S. Das and A. Kumar, "Survey on steganography methods (text, image, audio, video, protocol and network steganography)," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 2906-2909

[6] M. M. Salih and M. S. Atoum, "Applying AWGN MP3 Steganography Attack in BiLSB and SLSB Techniques," 2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Kuala Lumpur, 2015, pp. 62-67

[7] Yakun Dong, Ru Zhang, Jianyi Liu, Chenlei Cao and Di Xiao, "The MP3 steganography algorithm based on

linbits," ICINS 2014 - 2014 International Conference on Information and Network Security, Beijing, 2014, pp. 134-151

[8] H. B. Kekre, A. Athawale, B. S. Rao, and U. Athawale, "Increasing the capacity of the cover audio signal by using multiple LSBs for information hiding," in 2010 3rd International Conference on Emerging Trends in Engineering and Technology (ICETET), 2010, pp. 196-201

[9] R. Sridevi, A. Damodaram, and S. Narasimham, "Efficient Method Of Audio Steganography By Modified Lsb Algorithm And Strong Encryption Key With Enhanced Security," Journal of Theoretical & Applied Information Technology, vol. 5, 2009

[10] M. S. Atoum, M. Suleiman, A. Rababaa, S. Ibrahim, and A. Ahmed, "A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III," Journal of Computer Science, vol. 11, pp. 184-188, 2011

[11] B. Datta, P. Pal, and S. K. Bandyopadhyay, "Robust multi layer audio steganography," in 2015 Annual IEEE India Conference (INDICON), 2015, pp. 1-6

[12] K. Srinivasan, V. Ramamurthi, and K. S. Chatha, "A technique for energy versus quality of service trade-off for MPEG-2 decoder," in IEEE Computer society Annual Symposium on VLSI, 2004, 2004, pp. 313-316