International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(2) 2026 pp. 1649-1657
https://doi.org/10.70917/ijcisim-2026-4723
Article

An IoT-Oriented Secure Audio Communication Framework Using LSB Steganography, RSA, and MQTT

LAKSHITHA H S Murthy[1]
Research Scholar, Presidency University
lakshithahsmurthy@gmail.com

Dr. Ramesh Sengodan[2]
Professor in PSAIAC
ramesh.sengodan@presidencyuniversity.in

Abstract: The effectiveness of the data hiding techniques has been the subject of a large amount of research. One of the most secure ways of transmitting data in the digital era is the use of audio steganography whereby a secret message is hidden in an audio file without any modification of the audio file. In this paper, I am going to propose a steganography technique that has a high carrying capacity with the Least Significant Bit (LSB) substitution technique. Also, the RSA cryptosystem is secured on the inability to solve the factoring problem easily. The private and the public keys are mathematically connected to each other that the extraction of the private key out of the public key can only be impossible or computationally infeasible. This design guarantees the security and strength in two levels. There is high similarity between the original signal and the stego-audio signal that reduce the possibility of finding the stego secret message in the stego-audio signal. The proposed algorithm is implemented using MATLAB and the results are given. The parameters of the system are assessed based on a transparent gateway TCP network, and mathematical model of retransmission-based mutant Quality of Service (QoS-0) is created. Probability model is tested on a real physical network and experimented with repeatability of content delivery using VM based MQTT, a local network server, and remote server. The findings show that retransmission of the content by the sender leads to improvement of the probability of content delivery most particularly in the unreliable MQTT-based Internet of Things (IoT) environment, which is part of the development of smart city applications.

Keywords: Cryptography, Steganography, LSB, RSA, Stego-Audio

1. INTRODUCTION

In the modern technological world, information security is an important aspect in internet communication and has turned out to be among the most difficult to address. The content of the transfer is usually susceptible since, it may be easily tapped and abused by an intruder. The risk of unauthorized access to classified information is an increasing concern of the data communication professionals. To curb this problem, it is imperative that the transfer of information should be covert and confidential. One of such techniques is reversible data hiding which allows lossless data hiding, i.e., one is able to recover the original cover data fully, with the slightest possible distortion, once the hidden data has been recovered [1].

Steganography is also commonly used to protect data and reduce the risk of it being accessed by unauthorized parties, as is cryptography. Audiosteganography, specifically, applies audio files as objects of cover to hide the initial message. Steganography refers to the art and science of sending hidden messages in a manner that only the sender and their intended recipient would be aware of the presence of the message. Historically, there were methods of steganography as the text on the tablets with the wax covering, the null cipher, or the text tattooed on the head of the messenger [2].

Instead, cryptography involves the process of converting data to a series of bits that cannot be understood by an external or an attacker. Cryptography has been given the name after the Greek words crypto (secret) and graphy (writing). Coming out of the Greek noun steganos (covered) and graphy (writing), steganography is the concealment of information through the means of attaching messages to other otherwise innocent items, including text, picture or sound.

Steganography and cryptography are however susceptible to attacks when used independently. Steganography attacks are directed at identifying the presence of alterations in the cover message employed to transmit the secret information; cryptography attacks are directed at decrypting the secret message. Security breach can be overcome by integrating the strengths of the two methods. Combination of steganography and cryptography will provide a more secure and robust system. The main aim of integrating these two methods is to take advantage of the two and come up with a system that is robust and immune to attacks [3].

Literature survey was carried out and the works and studies related to the topic [4-11] were ended. Although most researchers have concentrated on the individual techniques, little has been done in the examination of the application of both cryptography and steganography. Therefore, the purpose of this project is to establish a method of combining cryptography and steganography in order to improve security.

2. RELATED WORKS

Steganography is a scientific method to encrypt secret messages in a manner that neither one nor the target party will raise a question whether the message exists or not [1][12]. Traditionally steganography has been applied in images [2-3], however, with increasing sophistication of digital tools and techniques audio and other media is being utilized more to hide messages [15-19]. Under the audio steganography technique, coded messages are hidden into digital sound files through minor adjustments to the digital audio sample sequence [6]. In this method, secret messages can be coded in the WAV, the AU and even MP3 files which are referred to as stego files once the message is coded in them [4, 5, 18].

Secret messages written in audio files are usually more complicated to embed in them than in pictures [2, 7, 11] since human auditory system is very sensitive to sound and can absorb more information of the media data than the human visual system [12]. In steganography, the sender and receiver can only know the presence of the hidden message, whereas in cryptography [14, 17], the presence of the encrypted message is apparent to the world [5, 16]. This increases the success of steganography when it comes to avoiding the unwanted attention on the hidden message. The cryptographic techniques [14] tend to secure the message content [3], whereas the steganography techniques conceal a message and a message content [11].

Despite the fact that steganography and cryptography are not new terms, using the two techniques in tandem to achieve better security is not well studied, and research on the composite method remains at its infancy. There is also a new challenge of using audio files to carry out steganography. This work is aimed at applying a cryptography technique to an audio stego file that has become a handy technique in recent years [15, 16, 19]. Recent research [18] has investigated the use of RSA (Prime) based encryption method and a Genetic Algorithm (GA) in audio steganography. RSA is known to be one of the most successful asymmetric key cryptographic systems that have been invented so far. Nonetheless, it is difficult to apply the RSA cryptography to play the role of wrapping an audio stego file. In [15], a similar study was presented with a smaller scope and assessment, as well as some convincing evidence. The current article is more detailed than the ones made in the past. The rest of the paper will be designed in the following way: the following section will describe the design methodology of the proposed technique designed to improve security.

3. PROBLEM STATEMENT

There is enhanced use of internet which has resulted into sharing and distribution of large quantities of information. Unless such information is secured in the right way it can be easily intercepted and abused by those who bear ill intentions. In order to secure this information, different strong algorithms are used. Cryptography combined with Steganography is one of the effective ways. The cryptography is a process that alters information in a way that it cannot be intelligible to unwanted outgoing parties whereby the Steganography is one that is determined to hide the presence of the message as well as the fact that there is a message that is being passed. The two have been extensively used as a measure of safeguarding against unauthorized accesses and assaults by un-intended users. The purpose of the paper is to make security better by offering a multilayered solution to security that incorporates both Cryptography and Steganography.

4. PROPOSED SYSTEM

This section is a review of the proposed system and how it works. The system can be split into three major stages, where the message is first encrypted with a cryptographic algorithm and the RSA algorithm is selected. Then, the ciphertext is steganographically concealed in an audio file with a steganographic method, the LSB substitution algorithm. Lastly, steganalysis is carried out and the hidden message is removed out of the stego-audio and then decrypted to give the original message. The flowchart of our suggested system is shown in Figure 1.

MQTT (Message Queuing Telemetry Transport) is a simple messaging protocol, which is based on a publish/subscribe model and runs over TCP/IP. It involves a central broker to handle messages between resource constrained devices (publishers and subscribers) within the Internet of things (IoT). MQTT has such main characteristics as topics (string hierarchy to filter messages), Quality of Service (QoS) levels to ensure message delivery, and a broker that acts as an intermediate, ensuring time and space decoupling, making it suited to low-bandwidth settings. Although MQTT specifies the communication architecture, scientists tend to create algorithms (e.g. artificial intelligence based intrusion detection or efficient back-off mechanisms) that can run on or improve MQTT networks.

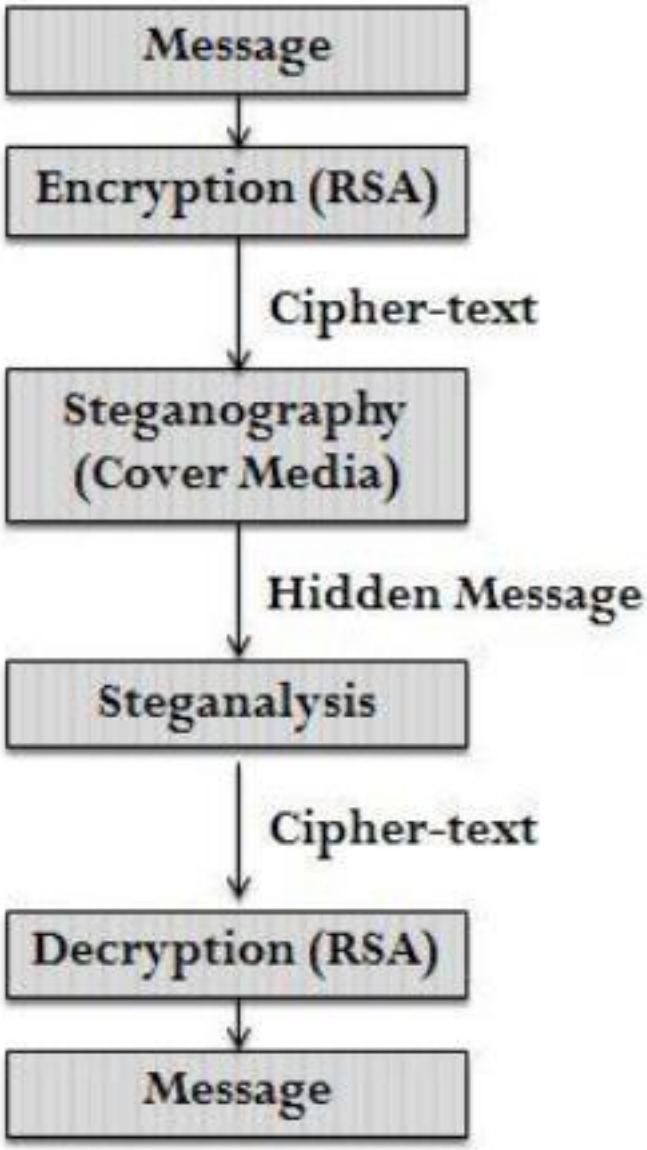

Figure 1F: lowchartofProposedSystem

A. Terminologies

Encryption: Refers to the transformation of plain text (message) into a form that cannot be deciphered, which is called cipher-text.

Cover-Media: This is the medium through which the message has been covered.

Steganalysis: The art of retrieving the coded message of the cover-media.

Decryption: This is the process of changing cipher-text to plain text (message) again.

B. Working

Step 1: Data is an input to the proposed system in the form of a secret message.

Step 2: The RSA algorithm is used to encrypt the message creating the cipher-text.

Step 3: The cipher-text is implanted in the cover-media in the form of the LSB substitution method, and it forms a stego-audio.

Step 4: Steganalysis is carried out on the stego-audio in order to decipher the encrypted message.

Step 5: The encrypted message is then decrypted to get the original message.

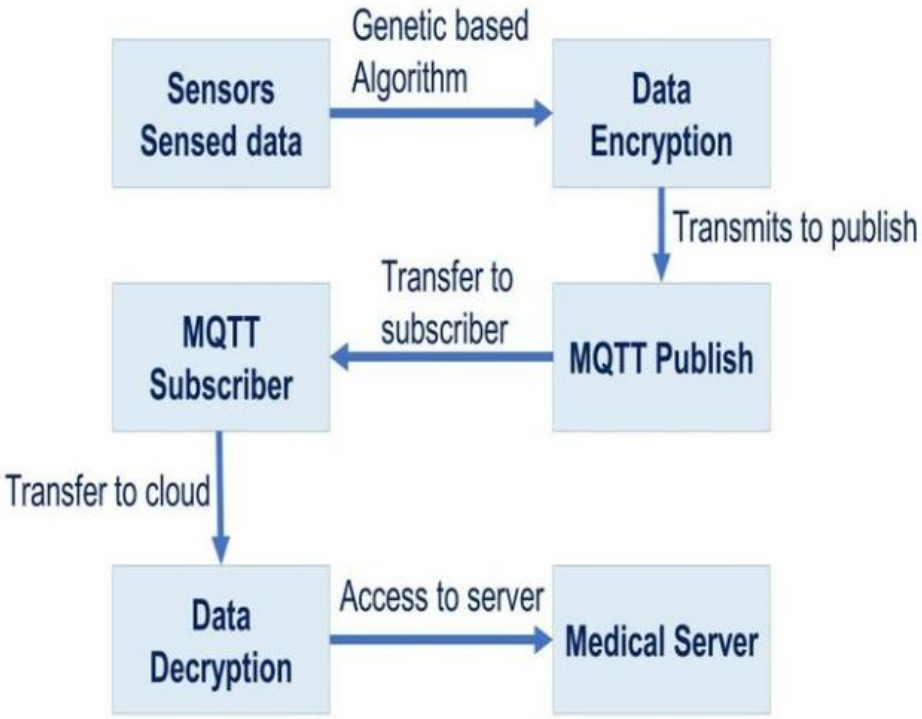

Figure 2: Block Diagram

5. ALGORITHMIC VIEW

There are several techniques used to conceal messages in the audio files, which has been referred to as Audio Steganography. Simple Least Significant Bit (LSB) techniques were applied at first and then the modified LSB method was [11]. Other investigators have attempted to make many LSB layers to improve resistance to attacks, but this can tend to cause greater distortion of the host audio. This paper will encrypt the message with the RSA algorithm and then randomly place the bits of the encrypted message in upper LSB layers of the host audio. This is used to enhance strength and minimize distortion.

The algorithm is comprised of four major steps:

A. Alteration

The initial stage is change, in which the message bits are substituted with target bits of the audio samples. Target bits are the ones that are located in the layers of which we want to change. This is obtained by mere substitution which does not entail adjustment and results are easily measurable [12].

B. Modification

This is the most essential stage in the algorithm. The success or failures of all the expected outcomes and results are dependent on the effectiveness of this step. The purpose of the algorithm used in this stage is to reduce errors and increase transparency. Transparency is described as the audible distortion that is produced by changes, i.e. by embedding messages, or by attack. Whereas simple methods can be applied, more effective methods alter the bits of samples with a higher precision. Because transparency is the difference between the original and modified samples, it is possible to perform bit and sample modifications with a smarter algorithm and transparency can be improved by introducing less differences.

C. Verification

This phase will be the quality control phase. When the algorithm has carried out the changes, the result has to be checked. In this case, the variation of the original sample with the modified sample is verified so that the integrity of the process is upheld.

D. Reconstruction

The last process is the creation of the new audio file, or the stego-file. The stego-file will be stored as a file named after its file name like as file-stego.wav and it will be stored in the same location as the original audio file.

MQTT Algorithm:

Core MQTT Logic (Pub/Sub Pattern)

Connect: Clients (devices) establish a TCP/IP connection to the MQTT Broker.

2. Subscribe/Publish:

Publishers send messages to the broker, tagging them with a

specific Topic (e.g., home/livingroom/temperature).

Subscribers tell the broker which Topics they are interested in.

Broker's Role: The broker receives messages and forwards them only to subscribers who have registered interest in that topic.

Key Features & Algorithms

Lightweight: Minimal header size, perfect for constrained devices.

QoS Levels (Delivery Algorithms): Define reliability.

QoS 0 (At Most Once): Fire and forget (no ack).

QoS 1 (At Least Once): Ensures delivery with acknowledgment (duplicates possible).

QoS 2 (Exactly Once): Guarantees delivery with a four-way handshake (highest overhead).

Last Will and Testament (LWT): A "will" message set by a client, sent by the broker if the client disconnects unexpectedly, notifying others.

Security Algorithms: Often uses TLS/SSL for encryption (port 8883) and HMAC for message integrity.

Advanced Algorithms: Researchers add custom algorithms for things like intrusion detection (using AI/ML like KNN, CNN) or backoff strategies to manage traffic.

RSA Algorithm:

Key Generation Algorithm

The primal key generation algorithm is as follows:

Take two big random prime numbers p and q, which are roughly equal, where their product is

n=pq is the desired bit length (eg. 1024 bits). [See note 1].

Compute n=pq and φ=(p−1)(q−1). [See note 6].

Select an integer e that satisfies the following conditions: 1<e<phi and gcd(e,phi) =1. [See note 2].

Calculate the secret exponent d, 1< d <1/4phi, which satisfies ed=1(mod 1/4phi). [See note 3].

The private key is (d,p,q), and public key is (n,e). Keep d, p, q, and φ secret. In other instances, the private key is in the form of. (n,d), as n is required in case d is being used. In other cases, the key pair would be represented as ((n,e),d)].

n is the modulus.

e is the public exponent (which is also referred to as encryption exponent).

d is the secret exponent (also referred to as the decryption exponent).

6. RESULTSANDDISCUSSIONS

The proposed system can be represented by the GUI as shown in the following figure, Fig. 2. Fig. 3 and Fig. 4 present the waveforms of the audio prior to and following data embedding and it is seen that the waveforms have practically no difference. The gap between the two signals is very small and it is barely noticeable.

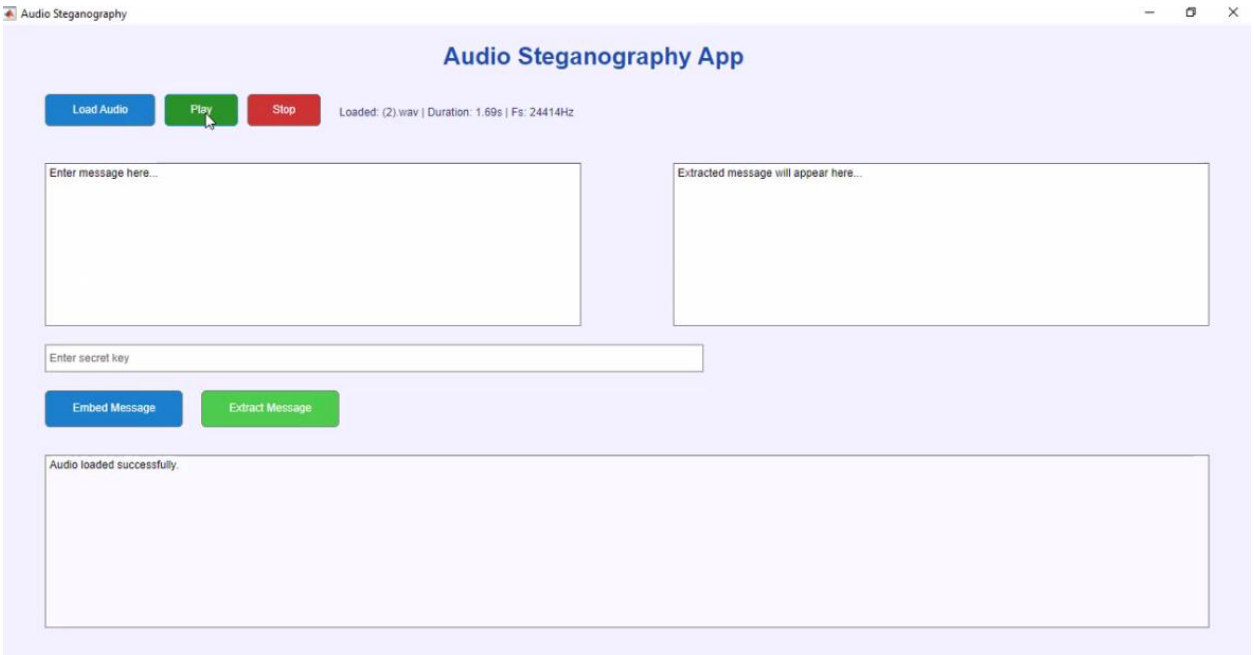

Figure 3: GUI for the Proposed System

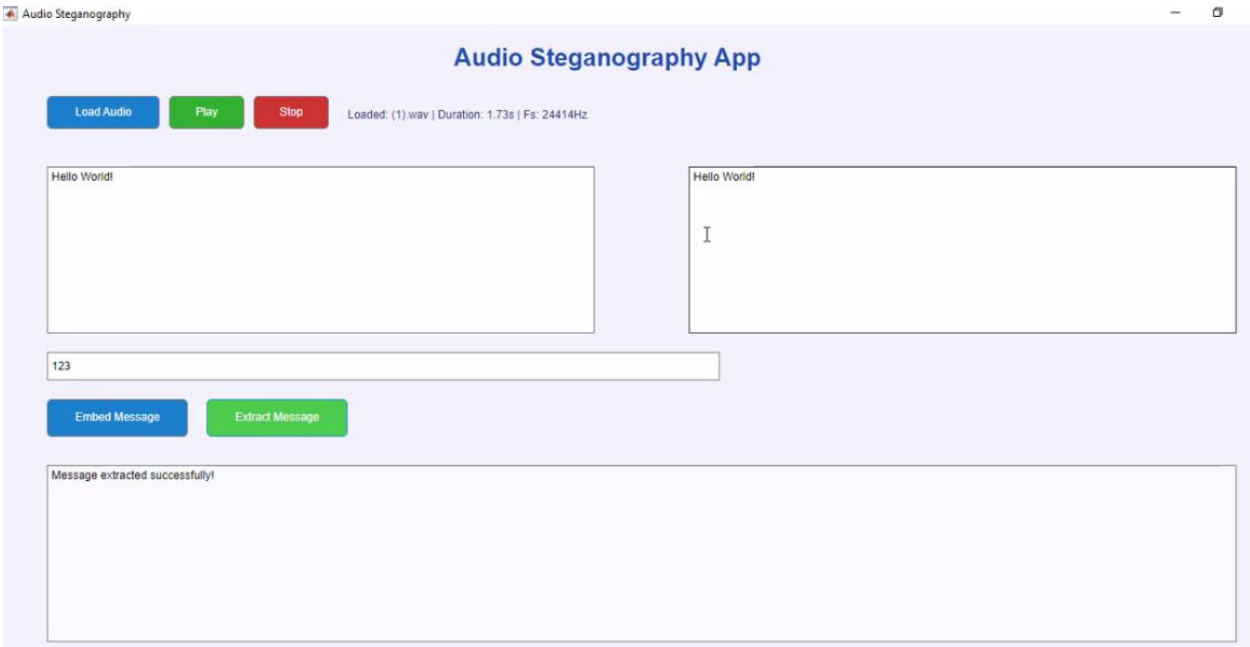

Figure 4: GUI for the Result System

7. CONCLUSION

The given work describes the process of encrypting textual information into an audio file (.wav) with the help of the LSB modification technique. WAV files are almost never used in audio transfer in recent times, however, they can easily be translated to compressed music files such as MP3. The repercussions that come with compression of stego-audio files are not discussed in this research, but this may be investigated later in the research. Although the synergistic approach of steganography and cryptography might appear rather simple, the greater innovation in the suggested approach is the development of a new level of security through the asymmetric integration of these two entirely different methods. In order to increase the security, a more common cryptography system RSA is used as a shield. Since the RSA implementation has been successful, it is proposed that other cryptography techniques can also be examined in the existing cryptostego framework. Even though cryptography and steganography possess their own advantages and disadvantages, the combination of both offers a better degree of security as is shown by the experiment outcomes.

Lakshitha H. S. Murthy is an Assistant Professor and Research Scholar in the School of Information Science and Engineering at Presidency University. She has over 7 years of teaching experience and specializes in Cryptography, Computer Networks, and Machine Learning. She is currently serving as an Assistant Professor at M. S. Ramaiah College of Arts, Science and Commerce (Autonomous), Bengaluru. Her research interests include network security, secure computing, and machine learning–based solutions.

Email:lakshithahsmurthy@gmail.com

Dr. Ramesh Sengodan, Professor, PhD in Computer Science and Engineering at Anna University Chennai, 30 years of experience, expert in Network Security, loT, AI. Presently Working in Presidency University, Bangalore. In School of Computer Science.

Email: ramesh.sengodan@presidencyuniversity.in

Reference

1. Gopalan, K. "Audio Steganography by Bit Modification. IEEE International Conference on Acoustics, Speech and Signal Processing, 2003, Vol. 2, pp 421-424.
2. Nazari, S., Eftekhary-Moghadam, A. M., and Moin, M. S. . A Novel Image Steganography Scheme based on relation of Morphological Associative memory and Permutation schema. Early view Security and Communication Networks, 2014. DOI: 10.1002/sec.962
3. Chang, C. C., Chen, T. S., & Hsia, H. S. An Effective Image Steganographic Scheme Based on Wavelet Transform and Pattern-Based Modification. IEEE 2003 International Conference on Computer Networks and Mobile Computing, 2003.
4. Chen, B., and Womell, G. W., p. 4 Quantization Index Modulation: A Provably Good Digital Watermarking and Information Embedding Method. IEEE Transactions on Information Theory, 2001, vol. 47, no. 4, pp. 1423-1443.
5. Chen, B., 2004, p.91. Design and Analysis of Digital Watermarking, Information Embedding, and Data Hiding Systems. Doctoral thesis, MIT, Cambridge, MA, 2000.
6. Amin, M., Salleh, M., Ibrahim, S., Katmin, R. M., and Shamsuddin, M. Z. I. Information Hiding Using Steganography. 4th IEEE National Conference on Telecommunication Technology, Shah Alam, Malaysia, 2003.
7. Zollner, J., Federrath, H., Klimant, H., et al. "Security in Steganography Systems Modeling." 2nd Information Hiding Workshop, Portland, April 1998, pp.345-355.
8. Anitha Devi, M. D., and ShivaKumar, K. B. "Novel Audio Steganography Technique of Ecg Signals in point of care systems (NASTPOCS). International Conference on Cloud Computing in Emerging Markets, 2016.
9. Gambhir, A., & Khara, S. "Audio Steganography + RSA Cryptography." International Conference on Computing, Communication and Automation (ICCCA), 2016.
10. Lemos, N., Sonawane, K., and Roy, B. “Secure Data Transmission With Video. IEEE, 2015.
11. Anitha Devi, M. D. and ShivaKumar, K. B. Novel Audio Steganography Technique in ECG Signals in Point of Care Systems (NASTPOCS). IEEE International Conference on Cloud computing in emerging markets, 2016.
12. Arora, A., Singh, M. P., Thakral, P., and Jarwal, N. Image Steganography based on Enhanced LSB Substitution Technique. 4th International Conference on Parallel, Distributed and grid Computing (PDGC), 2016.
13. Lamba, J. S., Sachdeva, K., Sinha, V. and Singh, N. 2008. "Differential Pulse Code Modulation in Audio Steganography." International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), 2016.
14. Singh, K. U. "LSB Audio Steganography Approach." ISSN 2250-2459 ISO 9001:2008 Certified Journal, Vol. 4, Issue 4, April 2014, International Journal of Emerging Technology and Advanced Engineering.
15. RSA Encryption - Keeping the Internet Safe, AMS Grad Blog. Available: https://blogs.ams.org/mathgradblog/2014/03/30/rsa/
16. Bazyar, M., & Sudirman, R. "A New Method to Capacitate the Capacity of Audio Steganography using LSB Algorithm. University Teknologi Malaysia, 81310 UTM Johor Bahru, Malaysia.
17. Jayaram, P., Ranganatha, H. R., and Anupama, H. S., "Information Hiding Using Audio Steganography - A Survey. International Journal of Multimedia and its Applications (IJMA), vol. 3, No.3, August, 2011.
18. Bhowal, K., Pal, A. J., Tomar, G. S., and Sarkar, P. P. "Audio Steganography with the use of GA. IEEE Proceedings, 2010.
19. Zamani, M., Taherdoost, H., Manaf, A. A., Ahmad, R. B., and Zeki, A. M. "Strong Audio Steganography through Genetic Algorithm." IEEE, 2009.