EAI Endorsed Transactions
on Smart Cities

Research Article EAI.EU

Securing Data using Audio Steganography for the Internet of Things

Anju Gera[1,*] and Vaibhav Vyas[2]

[1]Banasthali University, GLBITM, Greater Noida, India.
[2]Banasthali University, Jaipur, India.

Abstract

The Internet of Things (IoT) is prevalent in today's world and is part of our everyday life. While the residential district gains in several respects, numerous problems are developed, such as data confidentiality and privacy. The community is worried, in reality, about what information might leak through IoT. Therefore, the need for a protected environment is necessary if data transmission from devices across the network is to be protected. As a consequence, this paper proposes a secure scheme for using audio steganography to secure data from Laptop, which is distributed as an IoT device to other devices, or on LAN or WAN networks, as an alternative protection strategy along with a home server. The outcome of the developed system shows that the amount of distortion exposed by the Signal to Noise Ratio (SNR) is low.

Keywords: IoT, IoT protection, disclosure of details, Audio steganography.

Received on 04 July 2022, accepted on 14 November 2022, published on 04 January 2023

doi: 10.4108/eetsc.v6i4.1775

*Corresponding author. Email: anju.gera@gmail.com

1. Introduction

The Internet of Things (IoT) is one of the most emerging innovations to transform the modern world. IoT has traditional computing machines but of household devices and several other sensors for data collection. Also, hackers could be targets primarily on IoT devices with a weak protection level and computing capacities, such as IP cameras, smart TVs and other home appliances with little secrecy. For example, attackers are more likely to intercept continuous data transmission among IoT devices because it involves extensive network delivery, typically involving the Internet. The intruder can enter or manipulate such IoT devices by using the knowledge that he has been obtained for further use by accessing authentication information or by intercepting the link [3, 4]. To solve the confidentiality problem in the IoT network, we propose a security scheme involving web access. The use of audio steganography in the LAN is based on transmitting confidential audio information between the Desktop and home server. In contrast, data distribution between home servers and other computers would be encrypted from a LAN (Internet). Therefore, the paper provides the following efficiency metrics as a steganographic scheme for IoT implementation using a robust and lightweight algorithm: computational time, compression ratio, and signal-to-noise ratio, which can accommodate mass deployment [7]. The remainder of the document is arranged accordingly. IoT steganography is shown in Sec. II. Sec. III surveys the latest literature on IoT steganography. The scheme suggested is defined in Sec. IV. Sec. V describes modelling tests and outcomes of associated success evaluations. Sec. VI ends the paper with future works.2.

2. Problems in IoT Security

Safety in IoT networks entails challenges. These challenges, summarised below, must first be solved before implementing these networks.

- IoT networks need to protect a wide range of products, including laptops, cameras etc. The suggested protection strategies should handle the whole range of heterogeneous systems without compromising their functionality.
- Devices Capacity: Because of the heterogeneity of IoT architecture connected devices, multiple nodes are available, which include IoT networks with limited storage capacity and communication capacities.
- Data transmission rate: Protection schemes should also be able to have high payloads for secured data transfer.

3. Related Works

Three essential techniques give Security and privacy: cryptography and steganography. Encryption turns natural text into an unknown person in an unreadable form. Watermarking hides data in a digital medium and sends covers, including ownership and copyright, where the hidden message can be visible or invisible. The unique features, problems and peculiarities of running IoT security systems are addressed in an essential work by F. Djebbar [1]. The distributed implementation infrastructure, interoperability and heterogeneity of devices and the high traffic amount of IoT components are some of these peculiarities. The authors of [2] note that these unique features of IoT play an essential role in raising the risk of security attacks in IoT compared with other systems with clearly defined security policy and resources in a managed environment.

The study [5,6] aims to create an IoT security architecture consisting of two algorithms, the AES and the steganography of photography. Lightweight encryption is a sophisticated approach for limited conditions, such as RFID tags, cameras, contactless smart cars and medical equipment. In programme deployment, smaller code and RAM size implementations which do not always take advantage of the security-performance trade-offs are favoured. If the WSN is built into IoT devices to gather adjacent tools and boost the IoT device output on the network, self-jamming can be used as a protection mechanism to protect data from disclosure. Indeed, self-jamming is a tactic that avoids passive attacks by intentionally jamming the messages obtained by eavesdropper [9,10] and corrupting them. It can be achieved by noise when transmitting data. El Gamal Encryption is the encryption process used in their analysis. The encrypted message is integrated into the homogenous mp3 audio file frames. The encrypted message is improved with the spread spectrum approach and XOR modulation to improve randomness before embedding the register's message.

4. Proposed Scheme

In the real scenario, the Mic using desktop allows this opportunity to authenticate customer speech to open doors. In that case, the Desktop will receive and transmit users' voices to authentication servers or other computers (Ex. cloud storage) outside the LAN network for storage, The secrecy of the transmitted data is compromised by every eavesdropping attack, particularly on the LAN network. E.g., the voice intercepted is shown as sensitive information in Figure 1, and the authentication server [1] would authenticate any intruder who succeeds in getting it through an eavesdropping attack.

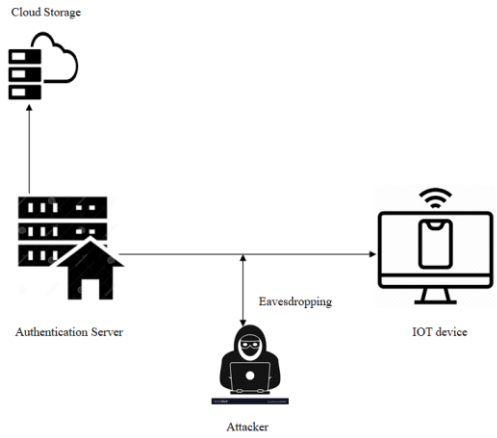

Figure 1. Real scheme

Figure 2 illustrates the proposed scheme for securing a transmitted voice using an IoT device. In this case, audio steganography is used to secure sensitive information, such as user voice, which is sent from an IP desktop (IoT device) on the LAN network. In addition, a home server can be used as a centralised device on the LAN network to receive a voice that is already shielded using audio steganography to encrypt it to the computers that are stored on the Internet (cloud storage).

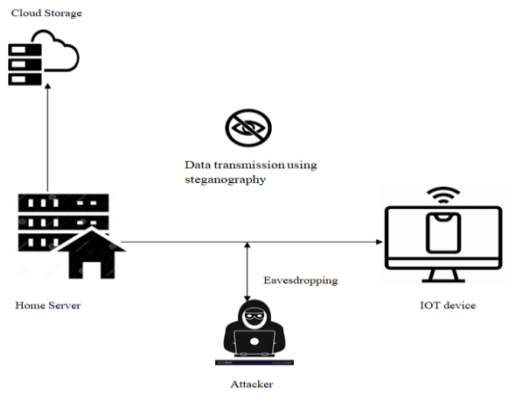

Figure 2. Proposed Approach

As a result, the Steganography technique can be used as an alternative authentication method for transmitting data in a protected manner. We are implementing Audio Steganography to Protected Audio, which is expected to be transferred from an IP desktop to a home server. In order to make the scheme simple, we consider that Bob, who owns a home, is entering the Desktop with Mic to load Audio. After the mic has successfully loaded Bob's Audio, it stores it as audio and loads another audio called the cover audio. Instead of transmitting the audio directly to the home server, the audio is covered (embedded) in the chosen audio (cover audio) with a steganography technique to generate another audio (stego audio) that includes the original audio. Later, the Stego audio can be sent to the home server to recover the original audio from the Stego audio using the same steganography method, albeit in a reverse manner. In the other hand, Eve, the eavesdropper, has successfully attacked Bob 's network to intercept data transfer between the laptop and the home server for any classified information. He realised that a laptop with a microphone would serve as an audio authenticator for Bob's front door home. As a result, the user loaded all audios, including stego audio, but does not doubt the audio as it seems to be identical to other audios loaded. Steganography is a way of rendering sensitive information and communications undetectable and stopping hackers from identifying them [10].

In the following, the Spread Spectrum technique was used to conceal encrypted text in the optical audio signal. Cast spectrum is a process by which the energy produced in particular by the wavelength is purposefully cast to the frequency domain , resulting in a signal with a broader wavelength.

Spread spectrum systems encode data as a binary series that sounds like noise but can be understood by a receiver with the right key. There are two types of spectrum spread techniques: the Direct Sequence Spread Spectrum (DSSS) and the Frequency Hopping Spread Spectrum (FHSS). In the Direct Sequence Spread Range, the data to be transmitted is split into small sections and each piece is assigned to a frequency channel throughout the range. Frequency Hopping Spread Spectrum is used in this research work. In Frequency-Hopping Spread Spectrum, the frequency spectrum of the audio file is modified such that it jumps easily between frequencies. The explanation for this is that it would be easier to decompose the digital audio signal into an analogue signal using the One Dimensional Discrete Cosine Transform (DCT).

The DCT is one of the strong compact transformations. The bulk of the signal energy is transmitted to the first transition coefficients, the lower energy or information is transmitted to other (i.e. high-frequency) coefficients.

$$f_{dct}(x) = \sum_{U=1}^{N-1} \alpha(u) c\ (u) \cos\left[\frac{\pi(2x+1)u}{2N}\right]$$

for x = 0,1,……..N-1,

Where $$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}}\ for\ u = 0 \\ \sqrt{\frac{2}{N}}\ for\ u \neq 0 \end{cases},$$

Where $f_{dct}(x)$ represents the initial sequence of the audio, N denotes the last frames in the audio file, and X denotes the number of frames in the audio file, and u denotes the height of the frame.

The Spread spectrum combined the compressed text file with the low frequencies of the audio signal using Eq.1:

$$S_{Sprect} = f_{dct}(low) \qquad \text{Eq.(1)}$$

The embedded signal is applied to the other high-frequency frames using Eq.2:

$$f_{frame}(t) = S_{Sprect} + f_{dct}(High) \qquad \text{Eq.(2)}$$

The analogue signal generated is then transformed to a digital signal using the Inverse Discrete Cosine Transform (IDCT) as shown below:

$$C_{dct}(u) = \alpha(u) \sum_{X=1}^{N-1} f_{frame}(t) \cos\left[\frac{\pi(x+1)u}{2N}\right] \qquad \text{Eq.(3)}$$

where the latest audio signal (stego file) is $C_{dct}(u)$ .The research work was analysed using the following efficiency metrics: computational time, bit per character, compression ratio and signal-to - noise ratio.

5. Result and Discussion

The system was implemented using MATLAB (R2017a version) programming language on Windows 8.1 Operating System platform. The research work was evaluated using the following performance metrics: computational time, compression ratio and signal to noise ratio.

5.1 Signal to Noise Ratio (SNR)

Signal to noise ratio is a parameter used to know the amount by which the signal is corrupted by the noise. It is defined as the ratio of the signal power to the noise power. Alternatively, it represents the ratio of desired signal (say a music file) to the background noise level. It is measured in decibel (db). SNR can be calculated by Eq. 4 [12] below.

$$\text{SNR (dB)} = 10log\left[\frac{\sum|S_c(n)|^2|}{\sum|S_c(n)-S_s(n)|^2|}\right] \qquad \text{Eq.(4)}$$

5.2 Computational Time

This is the time taken for the system to execute its function. From Table 1, the value of the Signal to Noise

ratio is more than 50db as the size of the text file to be inserted varies from 40 kb to 200 kb, and this means that there will be no distortion of the audio. But from 240 kb to 400 kb, the values of the Signal to Noise Ratio have started to decrease; rendering the values less than 50db and this means that there would be distortion as the value falls from 50db.

Table 1. SNR value after embedding Audio Size

Text Size(KB)	Audio File2 size(MB)	Audio length(minutes)	Compressed Size (MB)	Computational Time	Signal to Noise ratio(db)	Audio size after embedding(MB)	Extraction time
40	5	6	30923.5	7	58.4	5	4
80	5	6	72623.2	7	56.4	5	4
120	5	6	110810	7	53.4	5	4
160	5	6	141235	7	51.2	5	4
200	5	6	184365	7	50.4	5	4
240	5	6	218365	7	44.4	5	4
280	5	6	262587	7	38.5	5	4
320	5	6	305487	7	31.6	5	4
360	5	6	348655	7	17.6	5	4
400	5	6	386472	7	10.5	5	4

5. Conclusion and Recommendation

A scheme based on image steganography is proposed in this article, as the IP Desktop with microphone and memory capability is used as an IoT device to address privacy issues during transmission between smart devices and home servers. In this study, an audio steganography method for MP3 that uses DCT and spectrum spread techniques has been developed. Implementation and subjective experimentation have shown that the built audio steganography technology supports digital audio MP3 format. The device built has the ability to insert a hidden message of a size of up to 400 kb. Additionally, the system has the ability to insert a text size of 250 kb of respect to the digital audio duration or size without any distortion and has the ability to maintain the same size after embedding text into it. These findings suggest that the proposed scheme will satisfy the specifications and difficulties of IoT steganography by being able to handle a large number of devices and a large amount of IoT traffic. Further studies should be carried out to incorporate lightweight cryptography in combination with steganography (dual steganography) techniques to provide more protection for transmitted data using IoT devices across the network.

References

[1] F. Djebbar, “Lightweight Noise Resilient Steganography Scheme for Internet of Things,” 2017.

[2] U. Khadam, M. M. Iqbal, M. Alruily, M. A. Al Ghamdi, M. Ramzan, and S. H. Almotiri, “Text Data Security and Privacy in the Internet of Things : Threats , Challenges , and Future Directions,” vol. 2020, 2020.

[3] H. A.Abdullah, A. A. Abdulameer, and I. F. Hussein, “Audio Steganography and Security by using Cryptography,” i-manager’s J. Inf. Technol., vol. 4, no. 4, pp. 17–24, 2015, doi: 10.26634/jit.4.4.3644.

[4] F. Djebbar, B. Ayad, H. Hamam, and K. Abed-Meraim, “A view on latest audio steganography techniques,” 2011 Int. Conf. Innov. Inf. Technol. IIT 2011, pp. 409–414, 2011, doi: 10.1109/INNOVATIONS.2011.5893859.

[5] A. Jurcut, T. Niculcea, P. Ranaweera, N. An, and L. Khac, “Security Considerations for Internet of Things : A Survey,” SN Comput. Sci., vol. 1, no. 4, pp. 1–19, 2020, doi: 10.1007/s42979-020-00201-3.

[6] C. T. Jian, C. C. Wen, N. H. Binti Ab Rahman, and I. R. B. A. Hamid, “Audio Steganography with Embedded Text,” IOP Conf. Ser. Mater. Sci. Eng., vol. 226, no. 1, 2017, doi: 10.1088/1757-899X/226/1/012084.

[7] Mohsen Bazyar, Rubita Sudhirman, “A New Method to Increase the capacity of Audio Steganography Based on the LSB algorithm”, Journal Teknologi Science and Engineering, 74:6 (2015), 49-53.

[8] K.Sakthisudhan,P.Prabu and Dr.C.M.Marimuthu,”Dual Steganograpghy Approach for Secure Data Communication”, ELSEVIER International Conference on Modelling, Optimization and Computing,2012.

[9] Mengyu Qiao, Andrew H. Sung, Qingzhong Liu, “MP3 audio Steganalysis”, Information sciences, vol. 231, pp. 123-134, May 2013.

[10] Rostam, H. E., Motameni, H., & Enayatifar, R. (2022). Privacy-preserving in the Internet of Things based on steganography and chaotic functions. Optik, 258, 168864.

[11] Gera, A., & Vyas, V. (2022). Hiding Capacity and Audio Steganography Model Based on LSB in Temporal Domain. Recent Patents on Engineering, 16(2), 65-74.

[12] Gera, A., & Vyas, V. (2022). Message Security Enhanced By Bit Cycling Encryption and Bi-LSB Technique.