Computers, Materials & Continua
DOI:10.32604/cmc.2021.014802
Article

Tech Science Press

An Efficient Sound and Data Steganography Based Secure Authentication System

Debajit Datta[1], Lalit Garg[2,*], Kathiravan Srinivasan[3], Atsushi Inoue[4], G. Thippa Reddy[3], M. Praveen Kumar Reddy[3], K. Ramesh[5] and Nidal Nasser[6]

[1]School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore, 632014, India
[2]Faculty of Information and Communication Technology, University of Malta, Msida, MSD2080, Malta
[3]School of Information Technology and Engineering, Vellore Institute of Technology (VIT), Vellore, 632014, India
[4]Department of Information Systems & Business Analytics, Eastern Washington University, Spokane, WA99202, USA
[5]Department of Computer Science, Karnataka State Akkamahadevi Women's University, Vijayapura, India
[6]College of Engineering, Alfaisal University, Riyadh, 1153, Saudi Arabia
[*]Corresponding Author: Lalit Garg. Email: Lalit.garg@um.edu.mt
Received: 18 October 2020; Accepted: 07 November 2020

Abstract: The prodigious advancements in contemporary technologies have also brought in the situation of unprecedented cyber-attacks. Further, the pin-based security system is an inadequate mechanism for handling such a scenario. The reason is that hackers use multiple strategies for evading security systems and thereby gaining access to private data. This research proposes to deploy diverse approaches for authenticating and securing a connection amongst two devices/gadgets via sound, thereby disregarding the pins' manual verification. Further, the results demonstrate that the proposed approaches outperform conventional pin-based authentication or QR authentication approaches. Firstly, a random signal is encrypted, and then it is transformed into a wave file, after which it gets transmitted in a short burst via the device's speakers. Subsequently, the other device/gadget captures these audio bursts through its microphone and decrypts the audio signal for getting the essential data for pairing. Besides, this model requires two devices/gadgets with speakers and a microphone, and no extra hardware such as a camera, for reading the QR code is required. The first module is tested with real-time data and generates high scores for the widely accepted accuracy metrics, including precision, Recall, F1 score, entropy, and mutual information (MI). Additionally, this work also proposes a module helps in a secured transmission of sensitive data by encrypting it over images and other files. This steganographic module includes two-stage encryption with two different encryption algorithms to transmit data by embedding inside a file. Several encryption algorithms and their combinations are taken for this system to compare the

resultant file size. Both these systems engender high accuracies and provide secure connectivity, leading to a sustainable communication ecosystem.

Keywords: Cyber-attacks; signals; privacy; security; organization; encryption; decryption; authentication; effective communication; steganography

1 Introduction

In this era of scientific and technological developments, the users are exposed to large amounts of audible information from various sources such as TV, radio, online media, and music at shopping centers [1,2]. Most people carry their smartphones to these places, which are also exposed to these sounds in the surroundings [3,4]. It is possible to add confidential information to these sound channels, and it is even more secured than the standard data encryption techniques for smaller distances. Over the years, the use of sound as communication channels for facilitating device-to-device communication has drastically increased. This practice has been portrayed as a cheap and easy to use alternative to traditional communications protocols such as Wi-Fi, Bluetooth, and Zigbee [5,6]. Since this technology is relatively new, it lacks several standardizations, protocols, implementations, and varying security levels, which means that as this technology will gain more momentum, there are likely to be several security questions raised and assurances sought. Advancements in technologies and the development of several security measures and protocols have not stopped cyberattacks, but rather the attackers' end up coming with better-advanced processes for attacks on the systems [7]. The attacks are also performed on several Internet of Things (IoT) technologies and protocols like Radio Frequency Identification (RFID), Zigbee [6,8], Message Queuing Telemetry (MQTT), Advanced Messaging Queuing Protocol (AMQP) [9], and even IoT devices. The attackers also succeed in faking someone's identity belonging to the network [10,11]. However, this work provides an alternative solution to securing communication over a network by using sound-based authentication. Sound waves of particular interest are the use of ultrasound (20 kHz+) or near-ultrasound (16 kHz–20 kHz), or even audible sounds (20 Hz–20 kHz) for device-to-device communications. The frequencies which belong to the ultrasound frequency range are outside the hearing range of most adults, and so ultrasound or near ultrasound can be used as a covert communications channel. Ultrasound has been used as an out-of-band channel for authentication of peers in wireless *ad hoc* networks [12,13]. Ultrasound can implicitly contribute to secure communication-based on inherent limitations in signal propagation and can be used by the peers to measure and verify their relative positions [14–16].

The cyber-based attacks are not just limited to authentication and eavesdropping problems, but instead, there are possible attacks on the system's data and invasion of privacy [16–19]. Several encryption systems have been developed and revised to secure data related to a system. However, the attackers still manage to break into the systems and decrypt the messages through several techniques and approaches. Encryption algorithms like the Rivest Shamir Adleman (RSA) [13,20], Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), Data Encryption Standard (DES) have been developed. However, these also have vulnerabilities as encryption keys can be leaked through scan structure by violating confidentiality policies [21–23]. Moreover, the attackers can estimate the channel for transmission of confidential messages since the secret messages or sensitive data transmitted by an organization are not transmitted publicly, in general [24]. The latter problem, which consists of prediction of the transmission channel by an attacker, can be solved if a secured message is transmitted publicly [25,26] with some encryption, as attackers will less likely be suspicious of the data that is accessible to a wide range of people. This system

provides a sound authentication system that converts data as mathematical functions into a wave file that can be recorded by the destination; then, the similarity can be checked within the peaks of the audio signals and the width around the peaks within the waves that are formed. Based on the similarity, authenticated communication can be provided [27–29]. This system also provides a secured transmission of an encrypted message multiple times using different encryption algorithms into an audio file that is transmitted over the public platform, which will be accessible to a wide range of people. Nevertheless, the attackers will be unable to identify the data—given the encryption techniques are changed every time a transmission is made under proper information exchange along both ends.

Precisely, this work proposes a unique method for secure authentication system by combining two broad domains of cybersecurity—A sound-based authentication system and data steganography based secure data communication aided with a two-staged encryption system. The sound-based authentication uses peak-width and the peak-height to generate an angle that can be calculated using the equations and procedures discussed in other sections. The sound is generated randomly, and it changes before the central initiator node initiates every conversation. For the data steganography module, two-staged encryption is carried out using various file features—be its length, content, size, number of vowels, starting index from the beginning, etc. Once these attributes are chosen, the encryption occurs one after another and is appended to the transmission file. Like the sound-based authentication system, this also provides dynamic fixation of transmission files. Before every communication is initiated, the initiator node distributes the file to every other node within the network and parameters needed for the encryption systems. These two features of the system will be able to secure authentication and provide secure transmission of data. This system proposes a reduction in the overheads of the traditional approaches by systematically utilizing them. The main advantage of this work is that it can be used to provide secure data communication and authentication and protect the system from outside cyber-attacks. This work proposes a method that is dynamic and changes with every new transaction. The transactions in this system can be either a communication transaction or an authentication transaction, depending on the scenario. However, the limitation includes central node dependency for managing and initiating the communication, which can be addressed in future work. The rest of the paper is organized as follows: Section two of this paper deals with a literature review of the previous works. Further sections deal with the implementation of the system. Section three provides detailed information about the proposed system. Section four discusses the implementation and the required hardware and software configuration and the media used. Next, section five shows the results and visualization of data. Finally, the entire work based on the results achieved is concluded in the sixth section, along with the possible prospect of work that can be extended from this piece of work.

2 Related Work

Reference [30] established a sound encryption system that is based on fractional-order chaotic systems. The speech encryption system was provided with substitution boxes and other blocks like XOR, etc. required for generating the encryption. Several analyses for checking the security were made considering the sensitivity, statistical analysis, and several other parameters. According to [31], audio file steganography can be secured with AES encryption techniques and hashing functions like MD5, and used the AES algorithm for encrypting the data with MD5 for scrambling passwords. Also, the mp3 file was encoded. At the other end, decoding is carried out by the extraction of the sensitive private message and decrypted to recover the original data.

This technique's shortcoming is that it can only be carried out on the mp3 files based on a homogeneous frame. While [32] encrypted mp3 data within an image, and the steganographic method included a Cuckoo search followed by other optimization approaches. The result of their system was quite impressive, as the overall system produced good accuracy. Although several images were used, however, the steganographic system was limited to only audio files. Reference [33] proposed a three-dimensional chaotic system with the points of equilibrium presented in a close curve, which appeared similar to a boomerang shape, and was claimed to be feasible under several conditions. Also, Nasution et al. [34] dealt with steganography of images used to secure the audio files via several encryption algorithms. The audio and image files were fed into the system to perform a read operation; next, the audio was encrypted after proper compression on the system and inserted into the image. After that, the Peak Signal to Noise Ratio (PSNR) value was calculated, and the steganographic image was formed. However, the inserted data did not have any additional noise; thus, it is more vulnerable to be extracted by the attackers. Reference [35] provided security over communication that dealt with publicly transmitted data through various sources like loudspeakers, vibration motors, microphones, etc. The transmitter and receiver were designed such that the data was encrypted using AES techniques. Then the modulated data was transmitted, while the receiver was able to synchronize the data for performing the demodulation and later decrypt the message. Reference [36] developed an encryption system that used music to encrypt—Called MUSICYPHER. With the system, the message was encrypted with the Guyot system, and further, the message was decrypted. Further, this Android application was used for sending messages through sound or via the coded music message. Reference [37] investigated a three-dimensional chaotic system with a pattern of equilibrium points that form a shape of a cloud. Further, this work dealt with generating a sequence of random bits used to perform the National Institute of Standards and Technology (NIST) tests. References [38,39] proposed symbolic encryption through pseudorandom keys and FGPA-based chaotic cryptosystem, respectively. Moreover, the system's computational model dealt with cryptographic primitive, including encryption and decryption algorithms that offered efficient results. Reference [40] discussed the aspects of privacy and security provided over encryption and surveillance. It also highlighted the contrasts between the complaints of agencies that were based on Law Enforcement (LE). The knowledge of unacceptable risks provided by the security experts who force the Law Enforcement Access (LEA) features. Reference [41] described the methodology to synchronize a wide range of hyperchaotic systems having several characteristics, including noise, sensitivity, unpredictability, etc. It provided an implementation of a Cellular Neural Network (CNN) and synchronization over several dimensions Lorenz system. A chaotic simulation was carried out, and the design was prepared to develop an algorithm that facilitates the encryption of audio. Reference [42] analyzed the system's performance over different simulated spectrums analysis, correlation analysis, noise-based attacks, and the overall system sensitivity analysis. References [43,44] discussed the steganography on audio and image files, respectively, carried out via extra channels. In this system, the audio file was fed into the system to read the content. Further, this content was quantized, and then the sign bits' distinction was performed for building an extra sample. Reference [45,46] showed new methods to use steganography for secure data communications. These works perform a comparative study of various data hiding techniques. Besides, this system does not affect the quality of the audio after the recovery of embedded data. Reference [47,48] provided a different approach to steganography of audio files inside image carriers, and provide a secure video streaming system that is lightweight. Reference [49] discussed digital audio steganography after a critical review of several related works. Further, it provided information about echo hiding techniques, mp3

data hiding techniques, phase data hiding techniques, and many other steganographic techniques. Reference [12] proposed a system based on direct-sequence spread-spectrum modulation (DSSS) and real-time data that was obtained while working with the main application. The model used was broadly divided into several parts, encoding using an N-periodic pseudorandom sequence of $+1$ and -1 values, decoding using a raw complex-valued baseband signal. Local means of pointwise square $c(t)^2$ is equal to one approximately. Synchronization should also be considered. The main advantage of their system was that the protocol shows good overall robustness to noise.

Reference [14] used Pulse Code Modulation (PCM), Frequency-Shift Keying Modulation (FSK) algorithms. Further, no external dataset was used; the whole project was based on live data. The system was built using the GNU Radio; they established a TCP link over ultrasound between two laptops. Moreover, 23 kHz was used as a carrier wave. The mini modem program helped in a more formalized testing method to determine the best frequency, baud rate, and framing protocol suited to ultrasonic data transmission. The main parameters that influenced the system's performance were different baud rates, and framing protocols were required to check the system's overall accuracy. Baudot character map was used for the transmission of generally lowercase characters. Merit can be considered because the frequency generated using the FSK modulation was inaudible by most human beings. The transmission was reliable in the frequency generated by FSK modulation. However, there were drawbacks to this system like the frequencies higher than the FSK modulation generated frequency were unreliable, whereas the ones below them were audible to some human beings. Reference [15] portrayed a set of software-defined multi-layer functions used on general-purpose processing units and used live data to test their algorithm. It was based on a project called U-wear, an ultrasonic waves based software-defined networking. U-Wear runs on a processing unit which accesses an analog-to-digital converter and a digital-to-analog converter through the hardware-specific system APIs. The transmitted chain collects and converts U-Wear's output, and the received chain converts and passes the signal as waveforms to the U-Wear. A narrowband was used GMSK as the continuous-phase modulation. Wideband OFDM was extensively used in underwater acoustic communications. The system's main advantage was that the power consumption was low, and the design of the wuMote, which could be reduced further. The accuracy of data processing performance was pretty high. Nevertheless, the system's drawback was that the accuracy could be increased using different bandwidths and frequencies. Reference [50] developed a prototype for Sonic Data that comprised an encoder and a decoder and used Frequency-Shift Keying (FSK) modulation and did not use any external dataset, but the data was embedded in Kelly Clarkson's "Stronger" song. SonicData algorithm received an ASCII message from the user; then, it translated the same into a stream of binary data, which was later encapsulated into 8 ITA2 characters packets. Subsequently, the message was transformed into a decimal, further mapped with the message to frequencies ranging from 18 to 19.8 kHz. The parameters that influenced their system's performance include smartphone usage conditions, first one in the user's pant pocket, next held across the user's chest in a position similar to texting, and the last one against the user's ear. The system was a simple communication technique. The merit could be that SonicData entertains flexibility. It does not require some high configuration hardware or software infrastructure.

3 Proposed Work

Authentication of users over a network needs to be secured, but the measures taken using a certificate transmission or exchange of encrypted codes with encryption algorithms are vulnerable to attacks. Attacks made on authentication systems mostly deal with attackers who pretend to be

someone authorized within the network. Finding an attacker who has broken into the network with an authorized identity is a challenging task. This work provides a different approach to authenticate users or devices over a network—An authentication system using audio data in wave format transmitted over devices in a network. The communication amongst big organizations over sensitive data is more likely to be targeted by the attackers since they can estimate the location or mode of correspondence and even decode the entire conversation. The data transmitted over secret networks are vulnerable to attacks compared to those transmitted over public platforms like social networks, websites, messaging applications, etc. However, the confidential data that is transmitted publicly has to be carefully and adequately encoded or encrypted to trick the attackers by pretending that the file that has been transmitted has no sensitive data inside it. This work also deals with a system that provides steganography to transmit various files encrypted within other files; that need not be of the same format. The system is very advantageous for communication or authentication, where there is a transfer of sensitive information that is not supposed to leak in public. The system described in this work helps cater to secure communication and authentication of data. It also secures the system from outside cyber-attacks by its dynamic nature. The parameters and data—The sound data for a sound-based authentication system and the transmission file for data communication—Are a particular communication specific, and they change for every new communication transaction and authentication transaction, depending on the scenario. This system's limitation includes the fact that this system is based on a central initiator node and depends entirely on it. In future work, the distributive approach can be implemented. Further, the system implementation is carried out and tested on a laptop only; other platforms can be used in future work.

3.1 Sound Based Authentication System

Typically, this system module provides an authentication system based on verification of similarity of audio amongst the devices within a communication network. This sound-based authentication system can be installed into the nodes of a network of IoT devices, with enabled recorder and speaker functionalities. When the devices try to communicate with one another, authentication is carried out where the device that wants to communicate plays the wave file, and the device to which it wants to communicate to, record the audio. It compares the similarity amongst the transmitted data and the original wave file; based on similarity, the connection is granted for communication. The illustration of a scenario is shown in Fig. 1. Here two systems *A* and *B* in a network are considered—Given audio in wave file format is transmitted throughout every node within a network, say, *system A* wants to initiate a conversation with the *system B*, authentication has to be carried out between them. In the authentication process, *system A* will be playing the audio wave file for *system B*, and *system B* will be recording it using the recorder feature that it has already been facilitated. On completion of recording, the already recorded audio wave file has to be compared with the original one already been sent to all the network nodes. For a successful communication setup, both the systems must be equipped with a speaker and a microphone to generate the sound, that is, the audio file and a receiver that will record the sound for analyzing it later. The system is inspired by the three-way handshaking protocol exhibited by the Transmission Control Protocol (TCP). Instead of having data packets over a channel, this system transmits audio. The similarity is calculated by considering the peak values of audio files and the width associated with those peaks by taking the inverse of the tangent of the rate of change; if found to be greater than the fixed threshold, the connection must be authenticated, and thus, the conversation facility will be given. However, the authentication must be rejected if the similarity value is less than the threshold. A valid user *system A* (not an attacker) can

replay the authentication audio until *system B* recognizes it, and similarity becomes more than the threshold value.

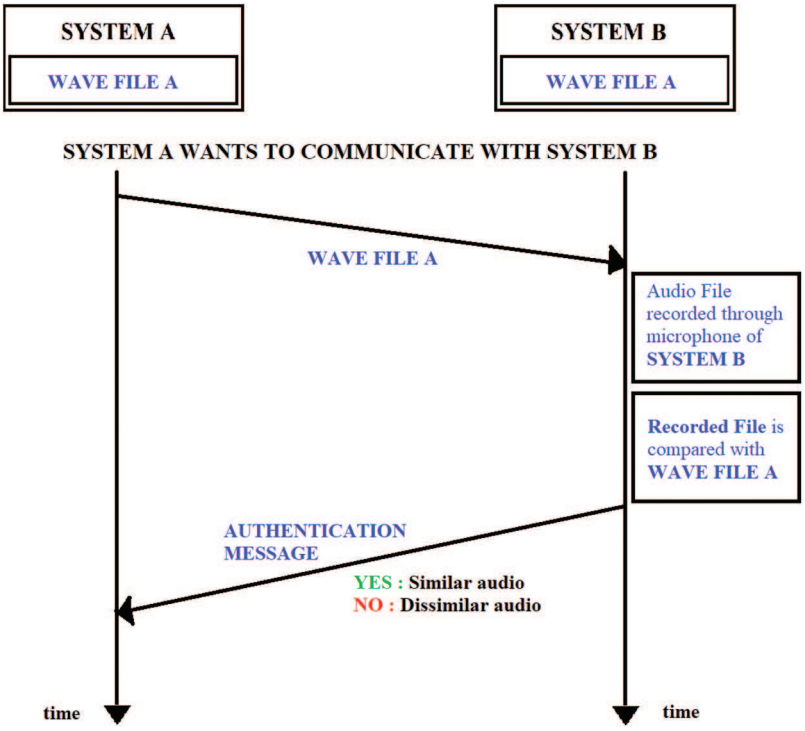

Figure 1: Illustration of the authentication system

The audio file, which is communicated over all the nodes, needs to be changed frequently in lesser time intervals to improve the network's security. One should select a threshold value such that the normalized audio similarities are between 0 and 1 but never equal to or very close to 1 or 0. Several dry runs should be carried out before ideally choosing a threshold value since a wide range can be vulnerable to attacks, but a narrow range can reject a genuine request. The system automates the threshold value to its optimal. The system also incorporates a technique that can select an optimum threshold that reduces the False Rejection Rate (FRR). The system is proposed keeping in mind the vastness of the environment that the system can be designed. There can be environmental interference like background noises, but there are chances that the sound sources can also have improper orientation like fewer loudspeakers, etc. The system has been ideally tested over several distinct environments to check the versatility of the proposed system. The ideal environment is taken earlier, where the background noises are absent, and the source has a distinctive loudspeaker. However, the system has also been tested over an environment with noisy background—where (i) It includes traffic noises and noises of loud music, (ii) An environment where the speaker is not loud, and (iii) A noisy environment where the speaker is not loud enough to check the system performance.

3.2 Data Steganography

This system module provides a different method of transferring encrypted data or file embedded into another file with steganography [51,52]. The communications dealing with sensitive

information facilitated between organizations are vulnerable to capture the attackers' unwanted attention. Often, the attackers are successful in tracing the location and mode or predicting communication channels since these conversations are done over dedicated systems and not publicly. However, publicly transmitted information is less vulnerable to the attackers' attention [53–56]. Further, this system comes up with a prototype of data transmission that has been encrypted with several algorithms over systems in a network, publicly.

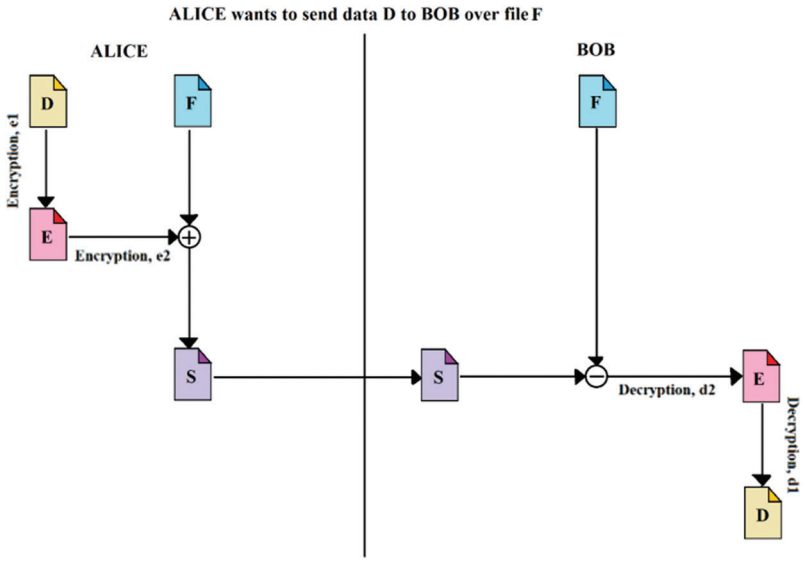

Figure 2: Illustration of steganography used in the data transmission system

The system is based on the transmission of encrypted data or files over ordinary files like mp3 files, image files, etc. The system provides a two-stage encryption process with two different encryption algorithms, e1 and e2; in this case, e1 is primarily the Fernet algorithm, and e2 is mainly the RSA algorithm, which should be different for strengthening the security of the system. The illustration of the system where communication takes place between two users or nodes, Alice and Bob, is shown in Fig. 2, where—Alice wants to send data or file *D* to Bob, and *F* is the source file used for steganography is. There is a communication initiator in this system that distributes a randomly generated file to every network node using security protocols before initiating a communication. The files are randomly generated and are renewed and redistributed after a particular amount of time. After the time passes, the file expires and no longer can be used for validation. This reduces the chances of attacks since the fields are dynamically changed. There is a data *D* that is needed to be transmitted. The source file that acts as a medium of transmission is file *F*. There are also the encryption algorithms *e1* and *e2* along with their decryption algorithms d1 and d2, respectively. The steps for communication are stated as follows:

- The communication initiator sends File *F* to the nodes before communication.
- The data *D* is encrypted by Alice using *e1* to form encrypted file *E*.
- File *E* is further encrypted using *e2* (second stage encryption).
- The resultant is then merged with file *F* to form an intermediate file, *S*.
- File *S* is sent to Bob.
- Bob removes File, *F* from File, *S*.

- The resultant is decrypted using *d2* to fetch File, *E*.
- File *E* is, further, decrypted using *d1* to fetch the data, *D*.

This system uses a two-step encryption system. The encryptions are implemented on different aspects of data—For this work, the content and the length of the data are the chosen encryption aspects. The encryption algorithms can be random for a particular transmission; thus, this can reduce the risks and vulnerability to different system attacks. The algorithms like AES, DES, ECC, RSA, and Fernet are treated as the information security backbone; hence, their security needs will not be analyzed separately.

4 Implementation

4.1 Hardware Requirement

The system modules are implemented on an HP Spectre x360 Convertible 15-ch0xx, with x64-based Intel® Core™ i7-8550U processor, a 16 GB RAM, a 64-bit operating system, and touch and pen support. HP manufactures the system and also contains a GPU. However, the system can be implemented on other workstations, IoT devices, and other devices. Precisely the authentication system, a device facilitated with a speaker, and a recorder is required that will be used for verification.

4.2 Software Requirement

The proposed systems have been built using python. For the system's authentication module, the libraries used include math, NumPy, wave, struct, matplotlib.pyplot, simpleaudio, time, sounddevice, soundfile scipy.io.wavfile, and scipy.signal. For the system's steganography module, the libraries that used are cryptography.fernet, eciespy, Crypto.Cipher, Crypto.PublicKey, time, os, random, and base64.

4.3 Methodology

The system is broadly classified into two modules that are independent of each other—The inputs and outputs of both modules are not based on each other, and they do not alter the results.

4.3.1 Methodology Adopted in the Authentication System

The authentication system is further divided into three coarse grain sub-modules—Generation of audio, recording of sound, and analysis of the recorded audio. The audio files generated are based on mathematical functions; for this system, the mathematical functions include sine and cosine functions over a given frequency. The functions that are used include:

- $\sin\left(\frac{2*\pi*x}{48000}\right), \quad where\ x \epsilon [1, 48000]$
- $\cos\left(\frac{2*\pi*x}{48000}\right), \quad where\ x \epsilon [1, 48000]$
- $\sin\left(\frac{2*\pi*x}{48000}\right) + \cos\left(\frac{2*\pi*x}{48000}\right), \quad where\ x \epsilon [1, 48000]$
- $\sin\left(\frac{8*\pi*x}{48000}\right), \quad where\ x \epsilon [1, 48000]$
- $\sin\left(\frac{0.5*\pi*x}{48000}\right), \quad where\ x \epsilon [1, 48000]$

After the audios are generated as wave files, all the systems are provided with the functions for future references. The second part of the authentication system includes recording the audio for further verifications. Using the functions provided by the various python libraries, the audio is recorded and fed into the third sub-module where analysis of the given audio is taken place. In the authentication system analysis section, the audio wave's peak values and width are retrieved for both the recorded audio and the reference audio. As shown in Fig. 3, the vertical height marked with purple gives the peak value, and the horizontal lines characterize the width, where the green line denotes half-width, and the red line denotes full-width. The similarity is measured based on a threshold angle θ_{min}, which is decided beforehand. In Eq. (1), the θ_{1_i} for the recorded audio is the inverse of the tangent of the change in peak altitude corresponding to the change in peak half-width. Similarly, in Eq. (2), the θ_{2_i} for the actual audio is the inverse of the tangent of the change in peak altitude corresponding to the change in peak half-width. The P in Eqs. (1) and (2) denotes the altitude of peaks, and W represents the value of half-width.

$$\theta_{1_i} = \tan^{-1}\left(\frac{P_{1_{i+1}} - P_{1_i}}{W_{1_{i+1}} - W_{1_i}}\right) \tag{1}$$

$$\theta_{2_i} = \tan^{-1}\left(\frac{P_{2_{i+1}} - P_{2_i}}{W_{2_{i+1}} - W_{2_i}}\right) \tag{2}$$

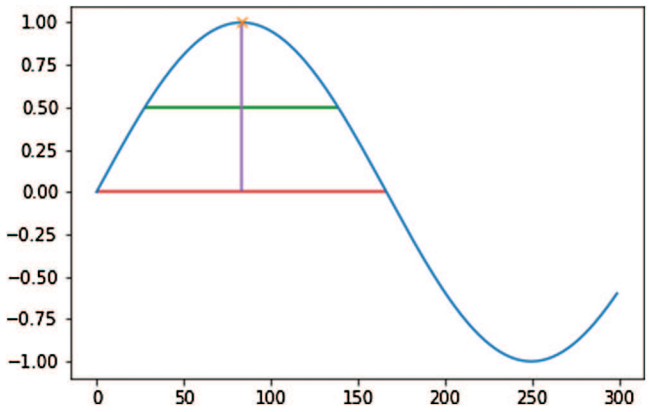

Figure 3: General plot to show peak altitude, half-width, and full-width in a graph

The value of θ is calculated as the absolute difference between the angles θ_{1_i} and θ_{2_i}, which are obtained from Eqs. (1) and (2), as shown in Eq. (3).

$$\theta = |\theta_{1_i} - \theta_{2_i}| \tag{3}$$

If the value of θ is less than that of the threshold angle θ_{min}, the point is considered true value; else, it is considered false. The optimal selection of θ_{min} is essential to ensure a broad range of θ facilitating system's testing in a noisy background—Including traffic noises and loud music. Another threshold, p, is decided, which denotes the minimum required fraction of positive results for authenticating the system. The value of the threshold fraction p is also chosen optimally such that it is often close to 1. The value is automatically chosen so that it is not vulnerable to external attacks and simultaneously does not reject genuine sources' communication requests due to background noises or faint audio sources. The optimal threshold that is generated considers

several dry runs, considering a method that can minimize the False Rejection Rate (FRR) of the system. The False Rejection Rate is undefined until there are no rejections. It becomes 0 when it starts rejecting the True Negative values. It starts rejecting the True Positive value; that is when the False Rejection Rate increases from 0. The threshold is chosen to be the last value until the False Rejection rate is 0. The threshold theta is chosen such that its tangent gives a value equal to or around 0.4. Thus, in degrees, the value is around 20°. The threshold fraction p is chosen around one so that the closely similar waves are only accepted for granting communication requests. It is not equal to 1 since there are background noises too. Further, the sound wave received is normalized concerning the minimum and maximum value of the waves. Thus, the intensity or loudness of the sound does not play an essential factor in authentication. Therefore, the devices can have any orientation, but the authentication system can authenticate until even the slightest of audio is audible. Precision, Recall, F1-Score, Entropy, and Mutual Information (MI) are calculated to evaluate the system's performance and efficiency. The system can tackle attacks that are remotely made, where the attackers guess the sound in the victim's environment at the time of the attack. Each communication is maintained by a central communication provider that creates different mathematical functions that generates the associated audio file. There can be infinitely many mathematical functions that can be made, including trigonometric, logarithmic, linear, square, cubic, nth power, or nth root and combinations of all of these. Thus, guessing a randomly generated function for a particular communication has a significantly less probability. The functions generated are also confidential and generated by the central communication provider; thus, it is hard for attackers to execute a co-located attack since even the victim is unaware of the random function [16] generated on their system.

4.3.2 Methodology Adopted in Steganography

The data steganography module is further divided into two sub-modules—The encryption module and the decryption module. In this system, two encryption algorithms are primarily used, Fernet encryption algorithm and Rivest Shamir Adleman (RSA) encryption algorithm. Further, several other AES, DES, ECC, Fernet, and RSA combinations are used to compare the time taken and the output file size. The two-step encryption system with different encryption algorithms decreases the chances of stage attacks.

As stated in the previous sections, this system consists of a communication initiator that distributes file F to all the network nodes using security protocols. File F is dynamically generated and has a timestamp and validity. After the validity period, it expires, and no one can use it further. This reduces the chances of external attacks. Fig. 4 shows the flowchart of the encryption and decryption modules that is proposed by this system. In the encryption process, the data or file transmitted securely is first encrypted with the Fernet algorithm with key $KEY(f)$ to produce data E. A length-function is applied to E to find its length $L(E)$. Using the RSA encryption technique, $L(E)$ is further encrypted using a large number N, a product of two large random prime numbers belonging to the RSA algorithm, and using the public key e, forming E'. Now, both E and E' are added to the file F (used as a medium of transmission) and results in file S. The RSA decryption algorithm is used to decrypt the encrypted file S using the private key d and the number N. $L(E)$ *is* the resulted decripted file in the decryption process. After the encrypted data's length is found, the original medium file F and the encrypted data E are retrieved.

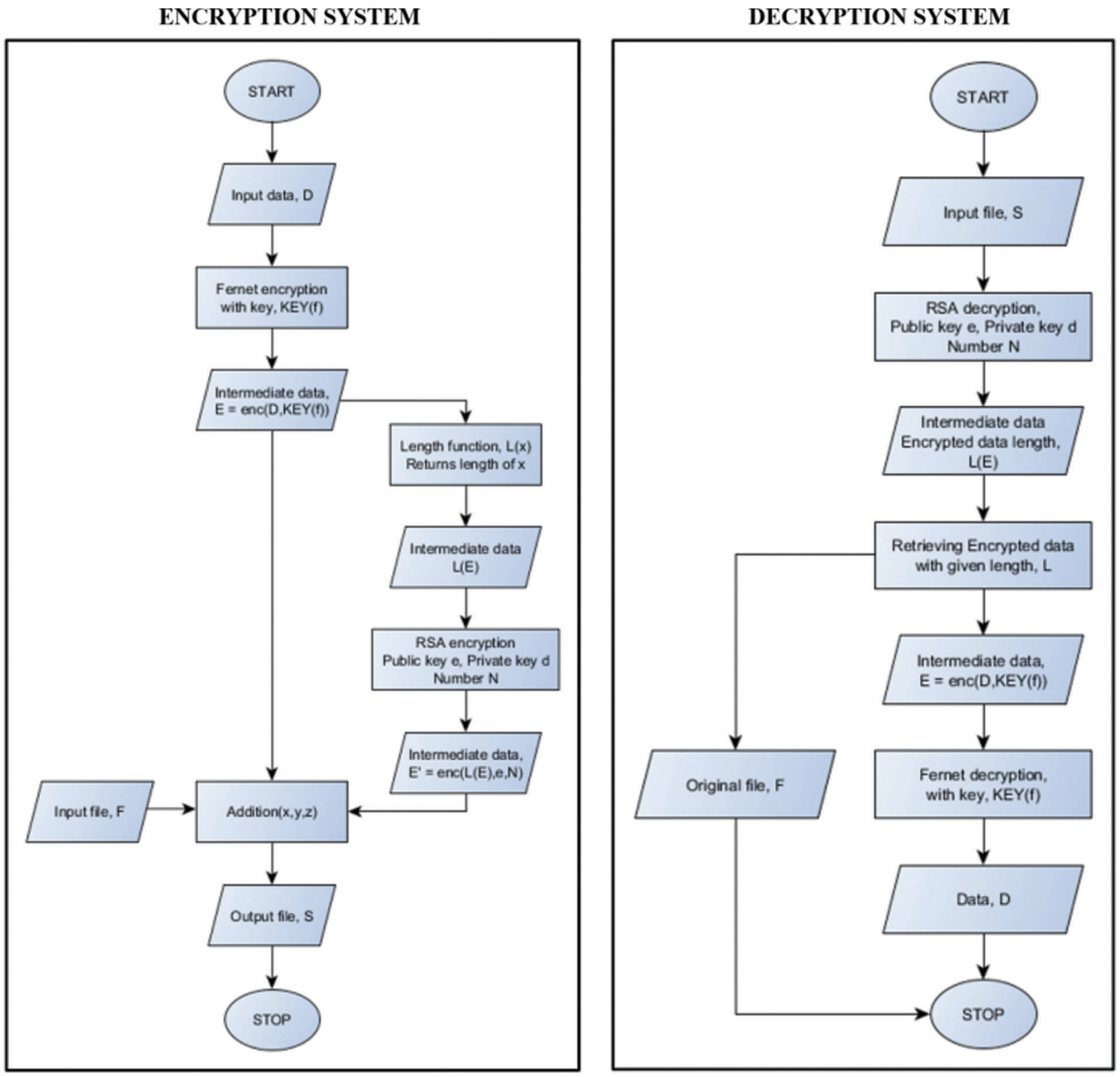

Figure 4: Flowchart showing the encryption and decryption modules of the system

Further, the decryption algorithm of Fernet is used along with the key, $KEY(f)$, to retrieve the transmitted data D. The Fernet key is updated after every successful transmission, and the random number N is also generated randomly every time. Further, this makes it very challenging for the attackers to track every detail; moreover, since N is a very large number, finding its prime factors is also problematic. However, since the file is used as a medium for transmission, it is less likely for an attacker to figure out that the file can have sensitive data encoded within it, making the system more secure. Various files are taken as the medium for transmission and as the data to be transmitted to compare the system's performance over different types of files—Audio files, video files, image files, and document files. However, no fixed file size can be embedded in another

file. It can be very large or tiny. Ideally, it should not exceed one-third of the actual file size into which it is embedded—since, otherwise, the resultant encoded file will be abnormally large. Although primarily, only the Fernet algorithm and RSA algorithm are used, later, the comparison based on the time taken as well as the percentage increase in encrypted file size, is carried out amongst all the possible combinations among AES, DES, ECC, Fernet, and RSA. In all possible combinations, two algorithms are chosen to compare the output file size, and the overall time is taken. Since these algorithms are widely known and accepted for the security they provide, no separate comparison on security area are carried out or analyzed for these algorithms. It will be challenging for the attackers to perform steganalysis [57] since the encryption algorithm is not fixed. Further, the steganography is independent of the file; thus, any file can be encoded. The comparison and visualization help in understanding the coverage of this system over various encryption algorithms.

5 Results and Analysis

The authentication system results are tabulated and visualized using python library matplotlib for better comparative study and more in-depth insight into the observations. The different wave functions that are used are plotted using the matplotlib library of python. The plots of functions 1 to 5 are shown in Fig. 5, where different trigonometric functions are used, the function 1 is $\sin((2 \times \pi \times x)/48000)$, the function 2 is $\cos((2 \times \pi \times x)/48000)$, the function 3 is $\sin((2 \times \pi \times x)/48000) + \cos((2 \times \pi \times x)/48000)$, the function 4 is $\sin((8 \times \pi \times x)/48000)$, and the function 5 is $\sin((0.5 * \pi * x)/48000)$. Tabulations of different observations with varying parameters are shown in Tabs. 1–5. The data shown in Tabs. 1–5 correspond to threshold value $\theta_{min} = \pi/4$, $\theta_{min} = \pi/8$, $\theta_{min} = \pi/9$, $\theta_{min} = \pi/10$ and $\theta_{min} = \pi/16$ respectively.

From the tables (Tabs. 1–5), it can be observed that as the θ_{min} value decreases, the accuracy measure, i.e., the ratio of true values to total values, decreases, and after a specific value of θ_{min}, it decreases drastically. Tab. 1 shows that when the θ_{min} value is $\pi/4$, all the values are considered to be true values, while Tab. 5 shows that almost half of the values are considered to be true, and half are considered to be false when the θ_{min} value is $\pi/16$. Tab. 2 shows that almost all the values are considered to be true values, and very few values are considered as false when θ_{min} is $\pi/8$. However, the optimal value of θ_{min} can be chosen between $\pi/9$ and $\pi/10$ since the accuracy falls from around 75% to 90%.

The plots of accuracy *vs.* θ_{min} for different functions are shown in Fig. 6 and have been plotted using python's matplotlib library. The curves in the plot in Fig. 6 are almost identical. From the plots, it is clear that irrespective of the functions, the accuracy measure starts decreasing around $\pi/9$ and $\pi/10$, decreasing a lot after $\pi/10$. In Eq. (3), f_x is the probability density function of X, $E[.]$ is the expected value functional, and $H(X, Y)$ is the total entropy of the joint variable (X, Y). $I(X; Y)$ is the mutual information of variables X and Y. The closer the value of $H(X)$ is towards 0, the less impure is the entire system, hence a better overall system concerning performance. Tab. 6 shows that the precision increases from $\pi/4$ to somewhere between $\pi/9$ and $\pi/10$ and reaches a saturation point, and then it decreases. Recall and F1 score, on the other hand, keeps increasing. Entropy decreases until somewhere between $\pi/9$ and $\pi/10$ and then again increases. However, the value of Mutual Information keeps decreasing. The associated plot for comparison can be seen in Fig. 7. As shown in Fig. 7, the recall score increases with a decrease in θ_{min} value, and similarly, the mutual information score decreases with a decrease in θ_{min}. It can also be seen that precision score and F1 score increase and reach a max value and decrease, and contrastingly, entropy decreases until a minimum value and then again increases. Higher values

for precision, recall, and F1 score are considered virtuous, whereas a lower value for Entropy and MI is considered good. Thus, from the comparison, the ideal value of θ_{min} is considered to be around $\pi/9$ and $\pi/10$.

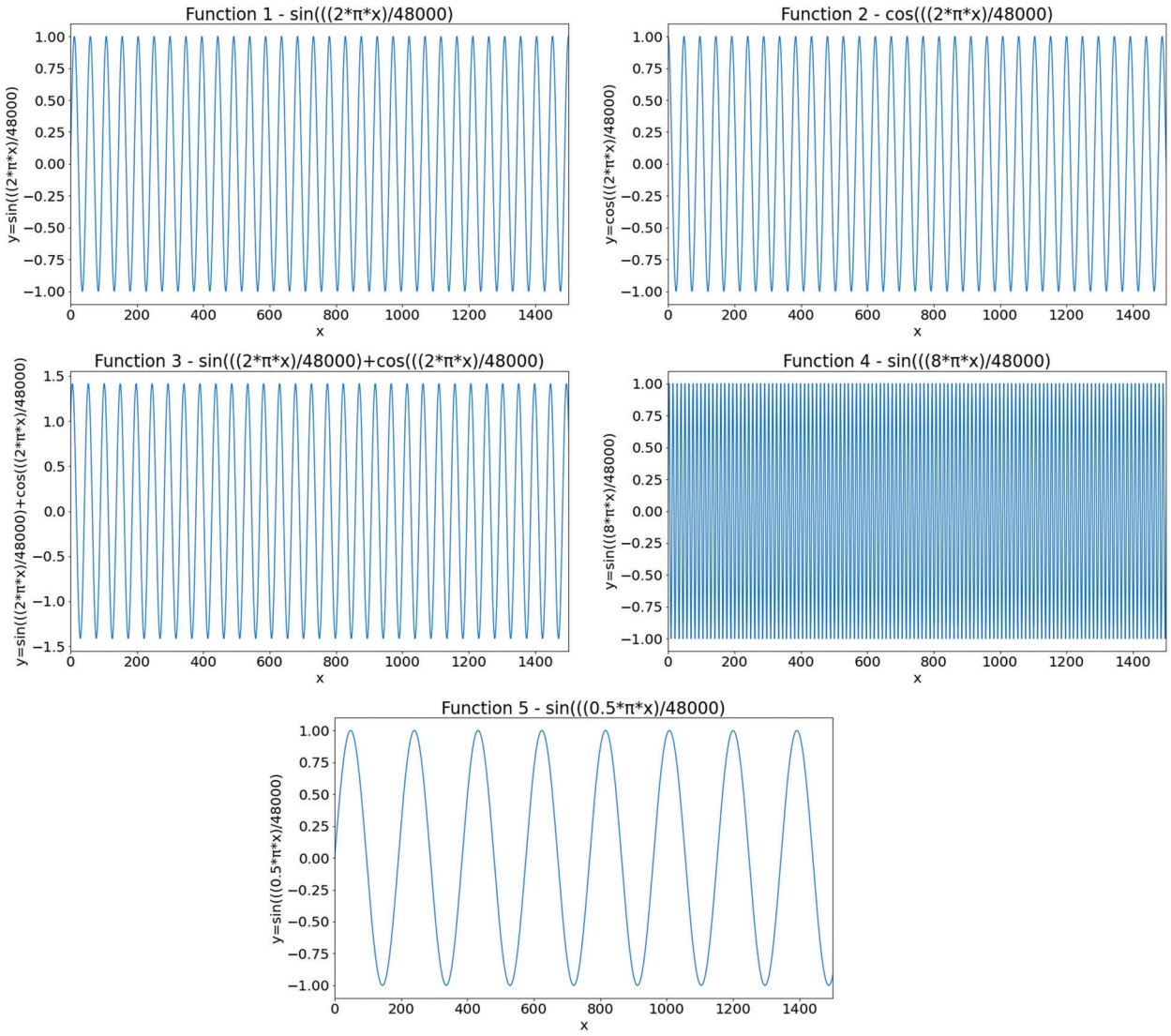

Figure 5: The wave plots—(top, left) function 1 (top, right) function 2 (top, right) function 3 (bottom, left) function 4 and (bottom, middle) function 5

The Precision, Recall, F1 Score, Entropy, and Mutual Information (MI) are calculated and compared in Tab. 6. The precision is the ratio of true positive values to the sum of true positive and false positive values; whereas, the Recall is the ratio of true positive values to the sum of true positive and false negative values [58]. The F1 score is calculated as the harmonic mean of

the values obtained from precision and Recall [59]. Entropy is obtained from Eq. (4) [60], and mutual information is calculated by Eq. (5) [53].

$$H(X) = -E[\log(f_x(X))] \tag{4}$$

$$I(X;Y) = H(X) + H(Y) - H(X,Y) \tag{5}$$

Table 1: Tabulation of data for different functions concerning threshold $\theta_{min} = \pi/4$

Function	True values	False values	Total	True/Total
1	999	0	999	1
2	998	0	998	1
3	999	0	999	1
4	3999	0	3999	1
5	249	0	249	1

Table 2: Tabulation of data for different functions concerning threshold $\theta_{min} = \pi/8$

Function	True values	False values	Total	True/Total
1	947	52	999	0.947948
2	946	52	998	0.947896
3	948	51	999	0.948949
4	3797	202	3999	0.949487
5	234	15	249	0.939759

Table 3: Tabulation of data for different functions concerning threshold $\theta_{min} = \pi/9$

Function	True values	False values	Total	True/Total
1	905	94	999	0.905906
2	903	95	998	0.90481
3	904	95	999	0.904905
4	3627	372	3999	0.906977
5	221	28	249	0.88755

Table 4: Tabulation of data for different functions concerning threshold $\theta_{min} = \pi/10$

Function	True values	False values	Total	True/Total
1	769	230	999	0.769769
2	768	230	998	0.769539
3	752	247	999	0.752752
4	3052	947	3999	0.763191
5	181	68	249	0.726907

Table 5: Tabulation of data for different functions concerning threshold $\theta_{min} = \pi/16$

Function	True values	False values	Total	True/Total
1	514	485	999	0.514514
2	514	484	998	0.51503
3	513	486	999	0.513513
4	2048	1951	3999	0.512128
5	117	132	249	0.469879

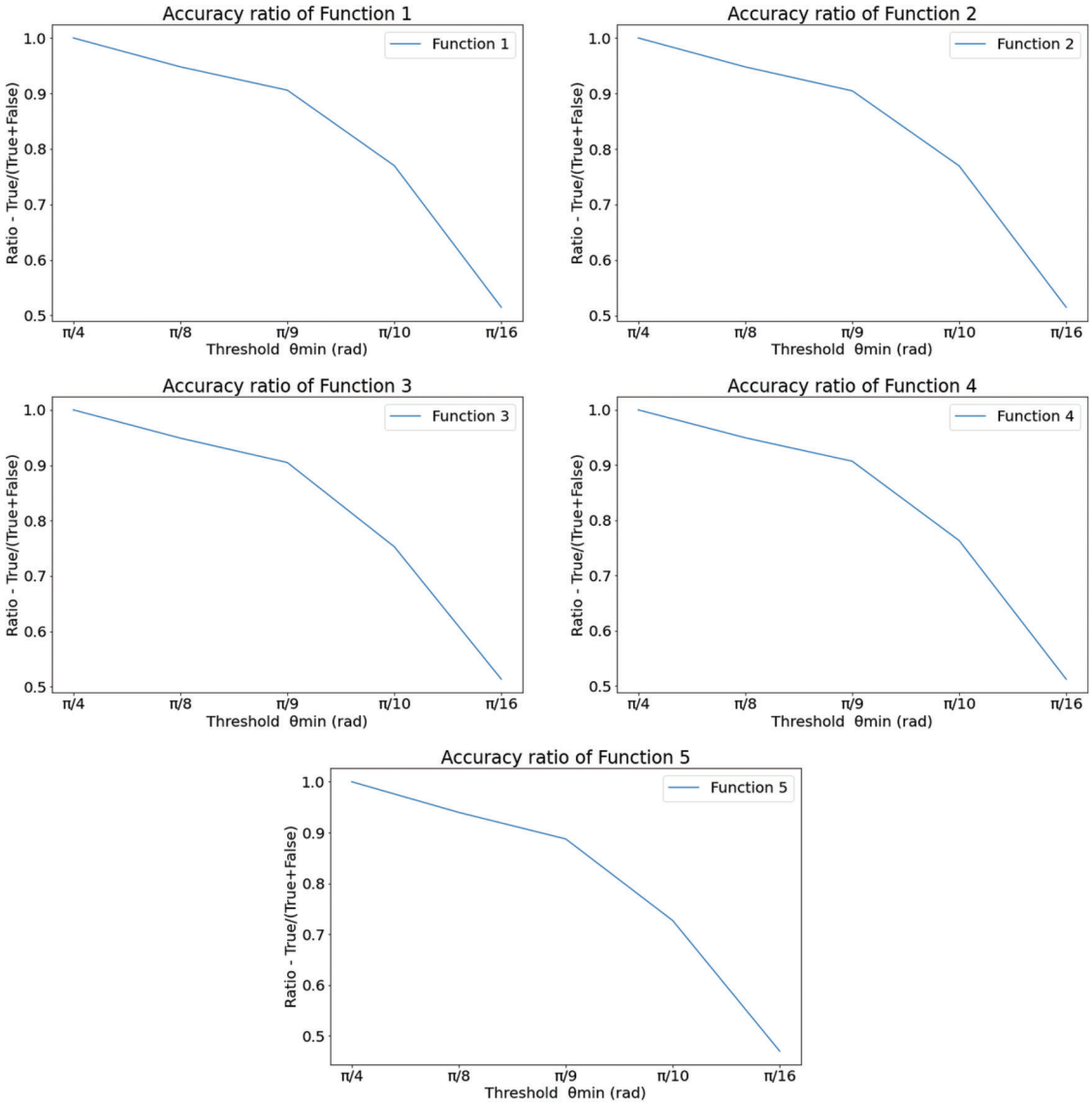

Figure 6: Accuracy *vs.* θ_{min} plots for the functions—(top, left) function 1 (top, right) function 2 (top, right) function 3 (bottom, left) function 4 and (bottom, middle) function 5

Table 6: Tabulation of precision, recall, F1 score, entropy, and mutual information (MI)

θ_{min} value	Function	Precision	Recall	F1 score	Entropy	MI
$\pi/4$	1	0.6667	0.6667	0.6667	0.3180	0.4440
	2	0.6667	0.6667	0.6667	0.3180	0.4440
	3	0.6667	0.6667	0.6667	0.3180	0.4440
	4	0.6667	0.6667	0.6667	0.3180	0.4440
	5	0.6667	0.6667	0.6667	0.3180	0.4440
$\pi/8$	1	0.7032	0.6784	0.6906	0.3130	0.4093
	2	0.7033	0.6784	0.6906	0.3130	0.4093
	3	0.7025	0.6782	0.6902	0.3131	0.4099
	4	0.7021	0.6781	0.6899	0.3132	0.4103
	5	0.7094	0.6803	0.6946	0.3118	0.4041
$\pi/9$	1	0.7359	0.6882	0.7113	0.3056	0.3834
	2	0.7368	0.6885	0.7118	0.3054	0.3828
	3	0.7367	0.6885	0.7118	0.3054	0.3828
	4	0.7350	0.688	0.7107	0.3058	0.3841
	5	0.7511	0.6926	0.7207	0.3013	0.3728
$\pi/10$	1	0.8660	0.7221	0.7875	0.2533	0.3169
	2	0.8663	0.7221	0.7877	0.2531	0.3168
	3	0.8856	0.7265	0.7982	0.2423	0.3111
	4	0.8735	0.7238	0.7916	0.2492	0.3145
	5	0.9171	0.7334	0.8151	0.2226	0.3040
$\pi/16$	1	0.8141	0.7954	0.8047	0.2557	0.2372
	2	0.8146	0.7952	0.8048	0.2556	0.2373
	3	0.8131	0.7957	0.8043	0.2560	0.2370
	4	0.8118	0.7961	0.8039	0.2563	0.2368
	5	0.7720	0.8098	0.7905	0.2650	0.2309

The data steganography system that is proposed is entirely independent of the previous system that involves an authentication system using audio verification. This steganography system includes the data's involvement, D, that needs to be encrypted and transmitted over the network and the file, F, which is used as a medium of transmission. The data, D can be a simple text or a string, or it can be any other file—like, an image file, video file, audio file, word file, excel file, etc. In the same way, file F can also be any file. The audio files that are used are—"Demi Lovato—I Love Me.mp3," "Taylor Swift—Cruel Summer.wav," "Iggy Azalea—Lola.m4a" and "Little Mix—Break Up Song.wma." The image files that are used are—"Patagonia-01.jpg," "Patagonia-02.jfif," "Patagonia-03.png" and "Patagonia-04.gif." The documents that are used are—"Doc1.docx," "Doc2.docx," "Doc3.doc" and "Doc4.doc." The video files that are used include "vid-01.mp4," "vid-02.avi," "vid-03.wmv" and "vid-04.mov." The same files are enlisted and can be seen in Tab. 7. The combination of D and F used is shown in Tab. 7; it also has the number of bytes before encryption and after decryption to check the success and accuracy of transmission over the network. The combinations that are worked on concerning the type of files used include (i) F as an audio file, D as an image file; (ii) F as an audio file, D as a video file; (iii) F as an audio file, D as a word document file; (iv) F as an audio file, D as audio file; (v) F as an image file, D as audio file; (vi) F as an image file, D as an image file; (vii) F as an image file, D as word

document file; (viii) F as an image file, D as a video file; (ix) F as a word document file, D as an image file; (x) F as a word document file, D as a video file; (xi) F as a word document file, D as word document file; (xii) F as a word document file, D as audio file; (xiii) F as a video file, D as an image file; (xiv) F as a video file, D as a video file; (xv) F as a video file, D as word document file; (xvi) F as a video file, D as an audio file. Tab. 7 demonstrates that this system works fine with any data file D and any medium file F. There is no data loss in encryption or decryption that is taken place. The total file size of the data file remains constant.

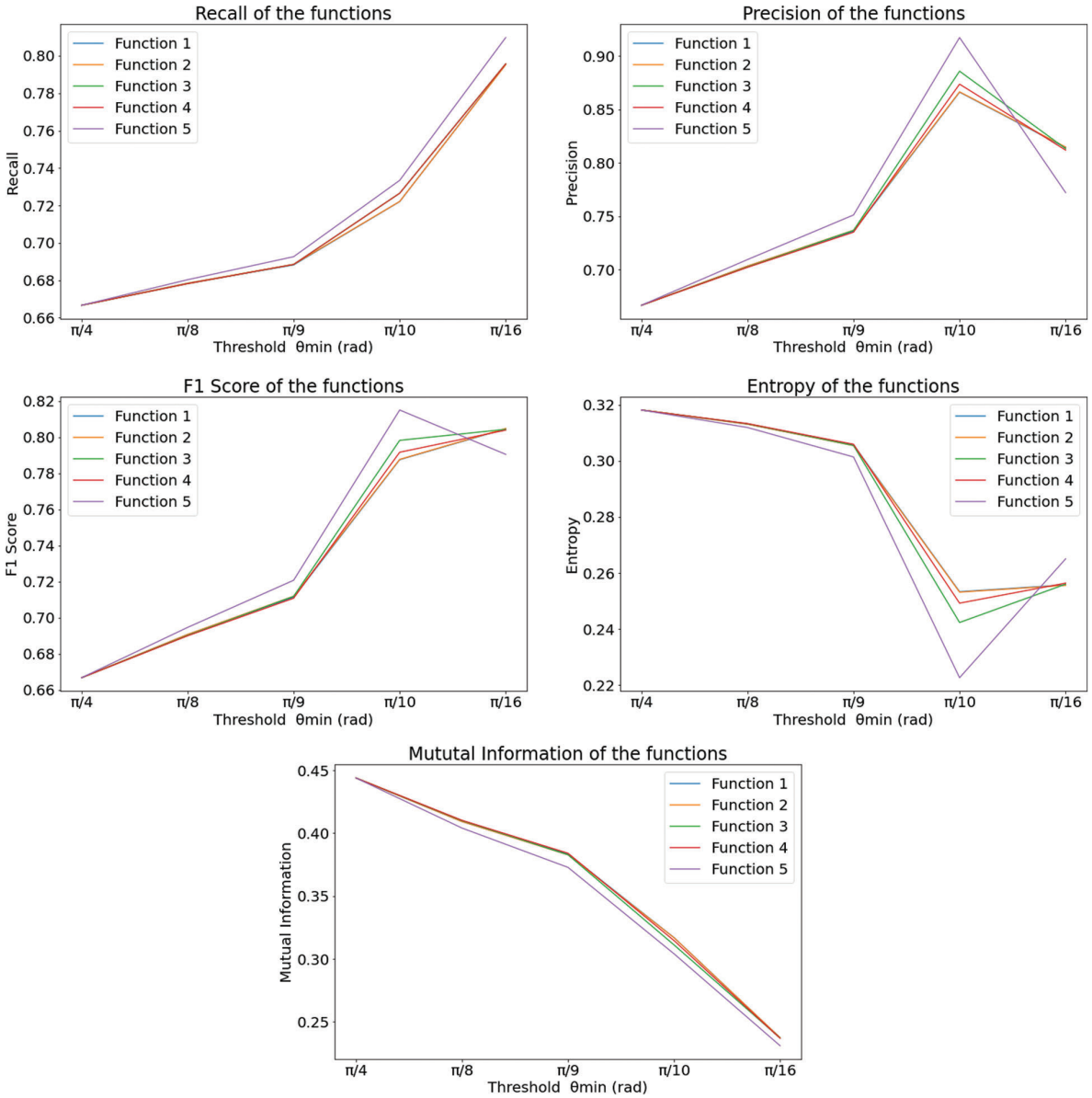

Figure 7: The plot of metrics for different functions with respect to θ_{min}-(top, left) recall (top, middle) precision (top, right) F1 score (bottom, left) entropy and (bottom, middle) mutual information encrypted data

Table 7: Tabulation of files to be transmitted, D, and data used as the medium, F

File F type	File F name	Data D type	Data D name	Bytes of D (before encryption)	Bytes of D (after decryption)
Audio	Demi Lovato—I Love Me.mp3	Image	Patagonia-01.jpg	150644	150644
Audio	Taylor Swift—Cruel Summer.wav	Video	vid-01.mp4	5848767	5848767
Audio	Iggy Azalea—Lola.m4a	Document	Doc1.docx	198999	198999
Audio	Little Mix—Break Up Song.wma	Audio	Demi Lovato—I Love Me.mp3	4892767	4892767
Image	Patagonia-01.jpg	Image	Patagonia-02.jfif	319911	319911
Image	Patagonia-02.jfif	Video	vid-02.avi	4330616	4330616
Image	Patagonia-03.png	Document	Doc2.docx	714442	714442
Image	Patagonia-04.gif	Audio	Taylor Swift—Cruel Summer.wav	7178414	7178414
Document	Doc1.docx	Image	Patagonia-03.png	2083964	2083964
Document	Doc2.docx	Video	vid-03.wmv	2184767	2184767
Document	Doc3.doc	Document	Doc3.doc	719360	719360
Document	Doc4.doc	Audio	Iggy Azalea—Lola.m4a	9501952	9501952
Video	vid-01.mp4	Image	Patagonia-04.gif	1898615	1898615
Video	vid-02.avi	Video	vid-05.mpeg	828561	828561
Video	vid-03.wmv	Document	Doc4.doc	1565696	1565696
Video	vid-04.mov	Audio	Little Mix—Break Up Song.wma	8015423	8015423

As shown in Fig. 8, there is no visible change in the visible data within the medium file *F* as the left column of images looks identical to that of the right column. Although the top row includes original images, they are identical in human vision, whereas the bottom row includes encrypted images. Thus, it is very challenging for anyone to identify the encrypted data within files for a human being. Moreover, the data *D* remains intact without any loss, as can be inferred from Tab. 7. The authentication methods and the steganography method proposed and implemented in this system work properly with high accuracy. The authentication technique can be implemented within IoT devices, too, to facilitate short-range authentication for secured communication. In the steganography method proposed, the data loss on encryption and decryption techniques is also none, and due to double encryption, the overall system is very much secured. Once the file is successfully decrypted, the system applies several combinations of encryption algorithms on a single file as the medium F, and the file to be transmitted *D*. As shown in Tab. 8, the encryption algorithms *E1* and *E2*, include AES, DES, ECC, Fernet, and RSA. The possible combinations that are considered include—(AES, DES), (AES, ECC), (AES, Fernet). (AES, RSA), (DES, AES), (DES, ECC), (DES, Fernet), (DES, RSA), (ECC, AES), (ECC, DES), (ECC, Fernet), (ECC, RSA), (Fernet, AES), (Fernet, DES), (Fernet, ECC), (Fernet, RSA), (RSA, AES), (RSA, DES), (RSA,ECC) and (RSA, Fernet). The file used as the medium, *F* is "Demi Lovato—I Love Me.mp3" and the file to be transmitted, *D* is "Patagonia-01.jpg."

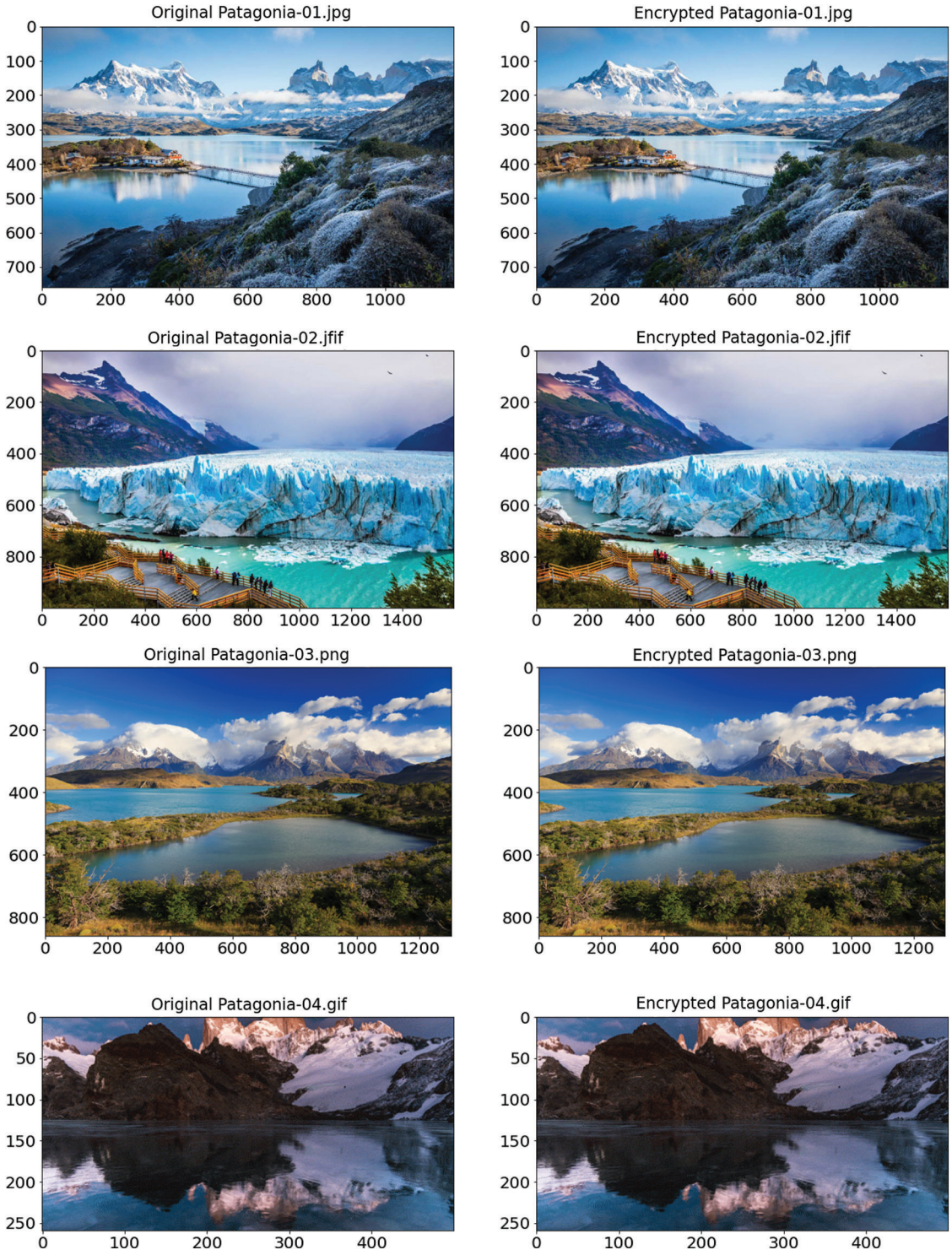

Figure 8: The picture files before and after steganography-(left) original pictures (right) picture with

Table 8: Tabulation of time taken, size of the encrypted file, and increase % of different combinations of encryption algorithms E1 and E2

E1	E2	Time taken [s]	Output file size [Bytes]	Increase (%)
AES	DES	0.328797	5167689	2.464165621
AES	ECC	0.233156	5167960	2.469538969
AES	Fernet	0.281201	5167753	2.465434604
AES	RSA	0.374403	5167657	2.46353113
DES	AES	0.325068	5477395	8.60496993
DES	ECC	0.284929	5478006	8.617084747
DES	Fernet	0.263685	5477190	8.600905221
DES	RSA	0.454135	5477997	8.616906296
ECC	AES	0.317834	5483647	8.728933652
ECC	DES	0.311475	5485241	8.760539246
ECC	Fernet	0.306823	5485013	8.756018496
ECC	RSA	0.341841	5485827	8.772158367
Fernet	AES	0.369618	5164210	2.395184529
Fernet	DES	0.307615	5164224	2.395462119
Fernet	ECC	0.339359	5164501	2.400954433
Fernet	RSA	0.226198	5164193	2.394847455
RSA	AES	1.090621	5120121	1.520994422
RSA	DES	1.405099	5120179	1.522144438
RSA	ECC	1.252591	5121518	1.54869393
RSA	Fernet	1.250054	5121519	1.548713757

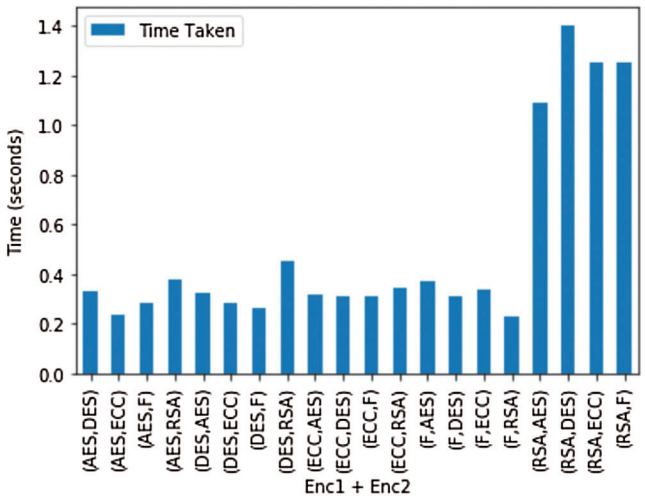

Figure 9: Plot for the time taken by the combination of different encryption algorithms

From Tab. 8 and Fig. 9, it can be observed that the time taken is the most for the systems where RSA is used as the first encryption algorithm, but the percentage increase in output file size is minimum for RSA. However, the output file size increase is very high for the systems

where DES and ECC are used as encryption for the first part. The F in Figs. 9–13 denotes the Fernet algorithm. Fig. 9 shows the time of execution for different combinations of encryption algorithms. The least time is taken for execution of the whole system, according to Fig. 9, is the system where Fernet is used as the first encryption algorithm, and RSA is used as the second encryption algorithm.

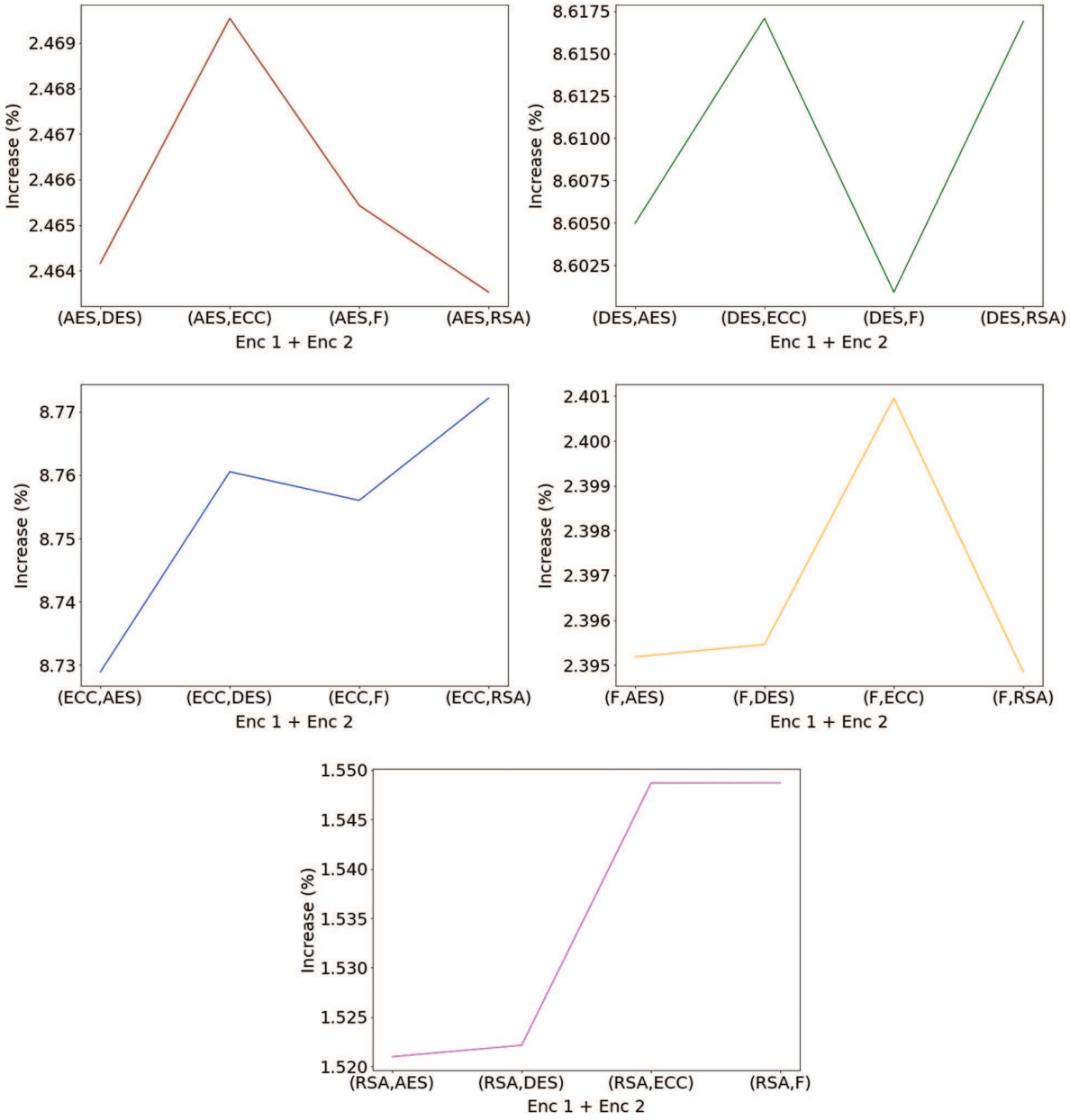

Figure 10: Plot for percentage increase in file size when the first encryption algorithm is-(top, left) AES (top, right) DES (middle, left) ECC (middle, right) Fernet and (bottom, middle) RSA

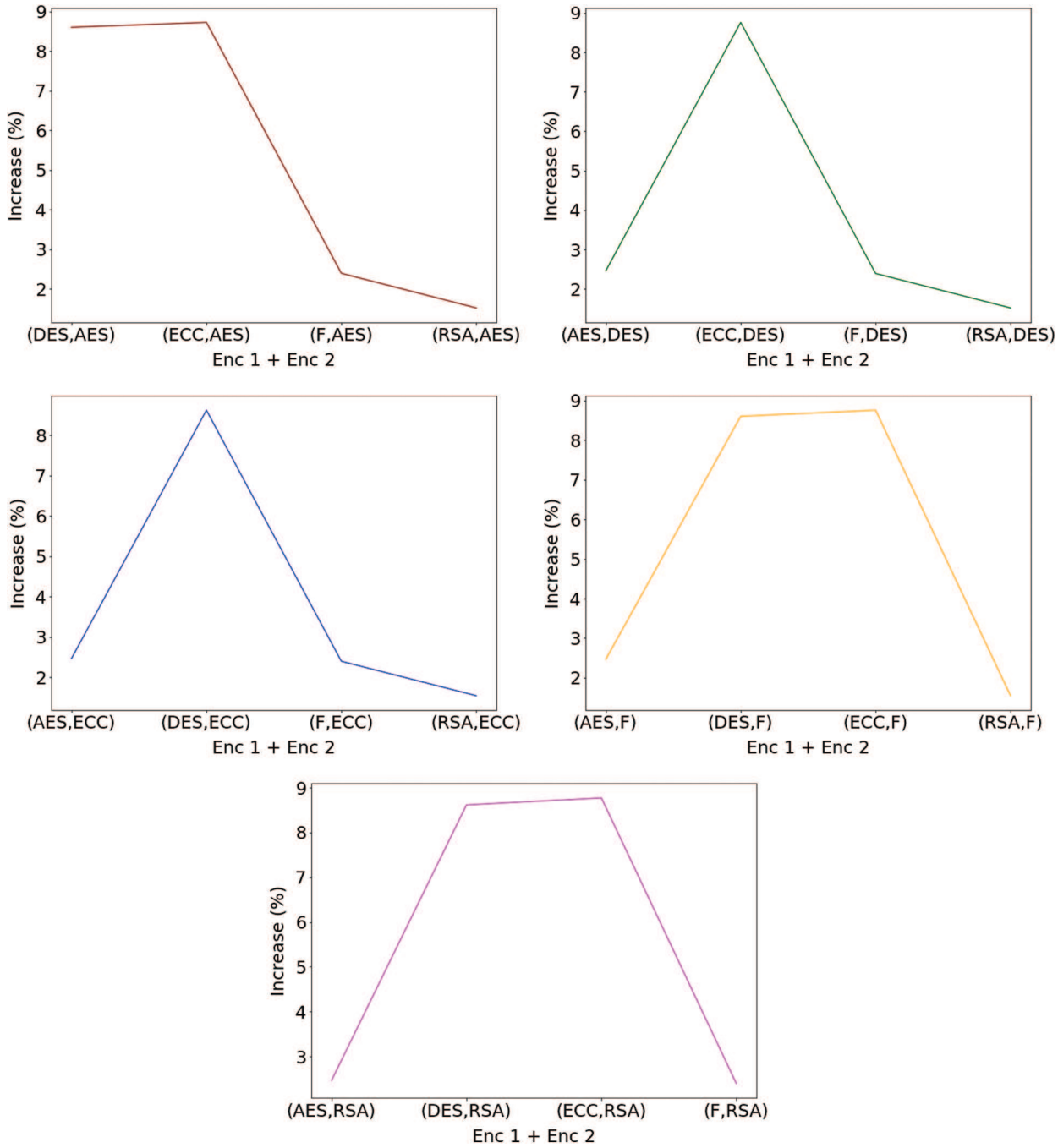

Figure 11: Plot for percentage increase in file size when the second encryption algorithm is-(top, left) AES (top, right) DES (middle, left) ECC (middle, right) Fernet and (bottom, middle) RSA

Figs. 10 and 11 show the comparison between the second encryption algorithms used and the first encryption algorithms used, respectively, when the first encryption algorithm and second encryption algorithm are fixed. From Fig. 10, it can be observed that the increase in the size of the file is comparatively high when the second algorithm is ECC, whereas, from Fig. 11, it can

be observed that the increase in the size of the file is comparatively low when the first algorithm is AES.

Fig. 12 shows the plot where the percentage increase of files can be observed concerning the different combinations of encryption algorithms. Similarly, in the bar plot in Fig. 13, the red portion shows the increase in size compared to the original file size shown with green color. Similarities between the curves can be observed in Figs. 12 and 13. The different plots help in proper visualization of the data, which helps analyze the entire system. The various encryption algorithms used in the system provide proper data transmission over the medium's files, with no data loss and the right consistency within the file information. When used as the first encryption algorithm, the RSA algorithm becomes time-consuming, but the overall increase in file size is the least irrespective of the second algorithm used. However, the file size obtained when either the DES algorithm or the ECC algorithm is pretty high.

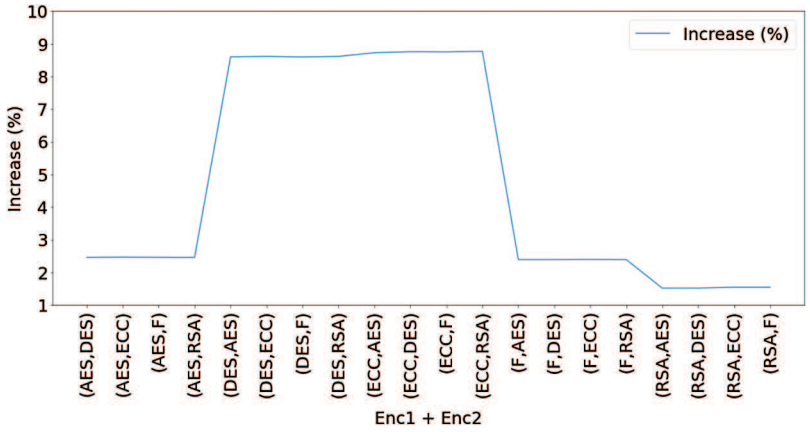

Figure 12: Plot for percentage increase in file size for all the combinations

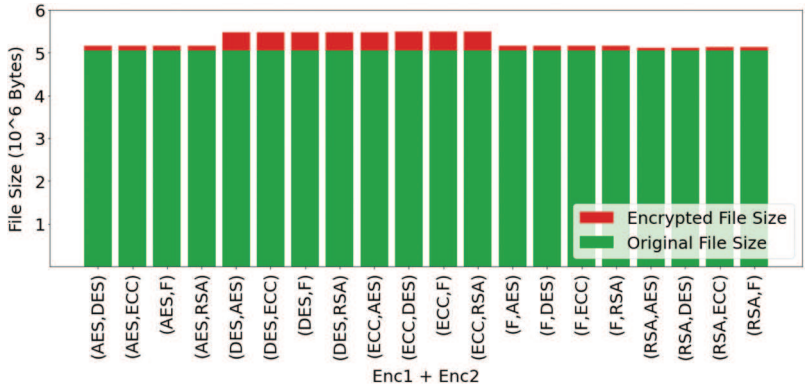

Figure 13: Plot for original file size and encrypted file size for all the combinations

6 Conclusion

The system is divided into two broad sections—one deals with authentication and the other one with steganography. The authentication is provided by validating a sound file that is generated

from a mathematical function. The similarities between the recorded wave to that of the original wave are taken with respect to a threshold angle and a threshold fraction of positive to total ratio. The threshold values for angle are optimally considered between $\pi/9$ and $\pi/10$, and the threshold fraction is chosen close to 1. The accuracy obtained within the optimal range of threshold angle is close to 1, resulting to secure authentication. The steganography module that provides secured data transmission is secured with two different encryption algorithms. The parameters associated with the encryption system like a chosen number, public key, etc. are also renewed after every successful transmission so that the attackers are unable to decode them. The system works fine with any file; either the file is used as a transmission medium or it is transmitted. There is no loss of data either the file is used as a transmission medium or transmitted, and the data is secure. The comparisons over different pairs of the algorithm used show that using the RSA algorithm as the first encryption can be time-consuming, while the increase in file size is least for it. However, the use of the ECC or the DES algorithm as the first encryption algorithm can lead to a more significant increase in file size. The first proposed system, which includes a random mathematical function generator for a given communication, is entirely dependent on the central communication initiator.

The systems perform well, and it generates decent scores for several accuracy metrics that include the precision score, the recall score, the F1 score, the entropy score, and the MI score. The first module is tested under a quiet background, a one where the source sound was kept faint and background with different noise levels—That includes traffic noises and loud music noises; however, the system performed the same for all. After the optimal threshold is chosen, the precision scores lie around 0.7–0.9, depending on the function, the Recall and F1 score is around 0.6–0.8, the entropy and MI scores are low, as expected from a good system. The second module includes two-stage encryption with two different encryption algorithms to transmit data by embedding inside a file. All the various combinations of the algorithms—AES, DES, ECC, Fernet, and RSA—are taken to compare the time taken and an increase in file size. The increase of file size ranges from around one to as high as eight times. Also, the taken time ranges from 0.2 s to 1.4 s. The time taken is less only when the first encryption is not RSA, which takes the most time to complete. However, the increase in file size is the least when RSA is the first encryption algorithm, and it is very high if the first encryption algorithm is DES or ECC. However, there is no loss in communication data, and the system performs well for every type of files.

The central communication facilitator role can be distributed to overcome the central node dependency factor in the future. Future work may also include considering other sound parameters like intensity, pitch, etc. for authenticating the system. This system can also be implemented with actual IoT devices for better authentication in the future. This work of a secured authentication system is supported only for short-range communication, which can be improved in the future and extended to more comprehensive ranges and implement ultrasound as well. The steganography system is stable and provides secure transmission, but the compression of the file treated as the medium is less and can be improved in the future. Also, the increased percentage in the size of the file can be brought to negative values.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Z. Li, V. Sharma, C. Ma, C. Ge, W. Susilo *et al.,* "Ciphertext-policy attribute-based proxy re-encryption via constrained PRFs," *Science China Information Sciences*, vol. 64, no. 6, pp. 1–2, 2020.

[2] D. Patel, K. Srinivasan, C. Y. Chang, T. Gupta and A. Kataria, "Network anomaly detection inside consumer networks: A hybrid approach," *Electronics*, vol. 9, no. 6, pp. 923, 2020.

[3] R. B. Melo, F. Carvalho and R. Assunção, "How accurate is it to measure noise with smart mobile devices?," in P. Arezes R. Boring (eds.), *Advances in Safety Management and Human Performance, AHFE 2020, Advances in Intelligent Systems and Computing*, vol. 1204, Cham: Springer, pp. 241–248, 2020.

[4] J. Guan, X. Liu, S. Yao and Z. Jiang, "Design and implementation of a central-controllable and secure multicast system based on universal identifier network," *Sensors*, vol. 18, no. 7, pp. 2135, 2018.

[5] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd and T. Hayajneh, "Security vulnerabilities in bluetooth technology as used in IoT," *Journal of Sensor and Actuator Networks*, vol. 7, no. 3, pp. 28, 2018.

[6] E. E. G. Guerrero, E. I. González, O. R. L. Bonilla, J. R. C. Valdez and E. T. Cuautle, "Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels," *Chaos, Solitons & Fractals*, vol. 133, 109646, 2020.

[7] M. Noura, M. Atiquzzaman and M. Gaedke, "Interoperability in Internet of Things: Taxonomies and open challenges," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, 2019.

[8] Y. Wang, C. Chen and Q. Jiang, "Security algorithm of internet of things based on ZigBee protocol," *Cluster Computing*, vol. 22, no. 6, pp. 14759–14766, 2019.

[9] N. Naik, "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP," in *Proc. 2017 IEEE Int. Systems Engineering Sym. (ISSE)*, Veinna, Austria, Piscataway: IEEE, pp. 1–7, 2017.

[10] K. A. Shim, "Universal forgery attacks on remote authentication schemes for wireless body area networks based on Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9211–9212, 2019.

[11] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *Proc. 2017 Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 10–11 February, Palladam, Tamil Nadu, India, Piscataway: IEEE, pp. 32–37, 2017.

[12] P. Getreuer, C. Gnegy, R. F. Lyon and R. A. Saurous, "Ultrasonic communication using consumer hardware," *IEEE Transactions on Multimedia*, vol. 20, no. 6, pp. 1277–1290, 2017.

[13] M. A. Ferrag, L. Maglaras, S. Moschoyiannis and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, 102419, 2020.

[14] H. Young, "Ultrasonic data transmission and steganography," *Honors College Capstones and Theses, 6*, 2016. [Online]. Available: http://digitalcommons.kennesaw.edu/honors_etd/6.

[15] G. E. Santagati and T. Melodia, "U-wear: Software-defined ultrasonic networking for wearable devices," in *Proc. 13th Annual Int. Conf. on Mobile Systems, Applications, and Services*, Florence, Italy, pp. 241–256, 2015.

[16] D. Datta and J. Dheeba, "Exploration of various attacks and security measures related to the Internet of Things," *International Journal of Recent Technology and Engineering*, vol. 9, no. 2, pp. 175–184, 2020.

[17] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2016.

[18] A. Oracevic, S. Dilek and S. Ozdemir, "Security in Internet of Things: A survey," in *Proc. 2017 Int. Sym. on Networks, Computers and Communications*, Marrakech, Morocco, Piscataway: IEEE, pp. 1–6, 2017.

[19] T. Nandy, M. Y. I. B. Idris, R. M. Noor, L. M. Kiah, L. S. Lun *et al.,* "Review on security of Internet of Things authentication mechanism," *IEEE Access*, vol. 7, pp. 151054–151089, 2019.

[20] Y. Chahid, M. Benabdellah and A. Azizi, "Internet of Things security," in *Proc. 2017 Int. Conf. on Wireless Technologies, Embedded and Intelligent Systems (WITS)*, Fez, Morocco, Piscataway: IEEE, pp. 1–6, 2017.

[21] G. K. Contreras, A. Nahiyan, S. Bhunia, D. Forte and M. Tehranipoor, "Security vulnerability analysis of design-for-test exploits for asset protection in SoCs," in *Proc. 2017 22nd Asia and South Pacific Design Automation Conf. (ASP-DAC)*, Chiba, Japan, Piscataway: IEEE, pp. 617–622, 2017.

[22] I. Ali, S. Sabir and Z. Ullah, "Internet of Things security, device authentication and access control: A review," *International Journal of Computer Science and Information Security*, vol. 14, no. 8, pp. 455–466, 2016.

[23] D. P. David, M. M. Keupp and A. Mermoud, "Knowledge absorption for cyber-security: The role of human beliefs," *Computers in Human Behavior*, vol. 106, pp. 106255, 2020.

[24] S. Shah, S. S. A. Simnani and M. T. Banday, "A study of security attacks on Internet of Things and its possible solutions," in *Proc. 2018 Int. Con. on Automation and Computational Engineering (ICACE)*, Greater Noida, India, Piscataway: IEEE, pp. 203–209, 2018.

[25] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou *et al.,* "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," 2020. [Online]. Available: https://arxiv.org/pdf/2006.11929.pdf.

[26] J. Valente, M. A. Wynn and A. A. Cardenas, "Stealing, spying, and abusing: Consequences of attacks on Internet of Things devices," *IEEE Security & Privacy*, vol. 17, no. 5, pp. 10–21, 2019.

[27] Y. Cao, Z. Zhou, C. N. Yang and X. Sun, "Dynamic content selection framework applied to coverless information hiding," *Journal of Internet Technology*, vol. 19, no. 4, pp. 1179–1186, 2018.

[28] Y. Cao, Z. Zhou, Q. J. Wu, C. Yuan and X. Sun, "Coverless information hiding based on the generation of anime characters," *EURASIP Journal on Image and Video Processing*, vol. 2020, no. 1, pp. 1–15, 2020.

[29] Y. Cao, Z. Zhou, X. Sun and C. Gao, "Coverless information hiding based on the molecular structure images of material," *Computers, Materials & Continua*, vol. 54, no. 2, pp. 197–207, 2018.

[30] A. J. A. El-Maksoud, A. A. A. El-Kader, B. G. Hassan, N. G. Rihan, M. F. Tolba *et al.,* "FPGA implementation of sound encryption system based on fractional-order chaotic systems," *Microelectronics Journal*, vol. 90, pp. 323–335, 2019.

[31] R. Indrayani, H. A. Nugroho, R. Hidayat and I. Pratama, "Increasing the security of MP3 steganography using AES encryption and MD5 hash function," in *Proc. 2016 2nd Int. Conf. on Science and Technology-Computer (ICST)*, Yogyakarta, Indonesia, Piscataway: IEEE, pp. 129–132, 2016.

[32] A. Gupta and A. Chaudhary, "A metaheuristic method to hide MP3 sound in JPEG image," *Neural Computing and Applications*, vol. 30, no. 5, pp. 1611–1618, 2018.

[33] S. Mobayen, S. Vaidyanathan, A. Sambas, S. Kacar and Ü. Çavuşoğlu, "A novel chaotic system with boomerang-shaped equilibrium, its circuit implementation and application to sound encryption," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, no. 1, pp. 1–12, 2019.

[34] A. B. Nasution, S. Efendi and S. Suwilo, "Image steganography in securing sound file using arithmetic coding algorithm, triple data encryption standard (3DES) and modified least significant bit (MLSB)," in *Proc. Journal of Physics: Conf. Series, Int. Conf. on Mechanical, Electronics, Computer, and Industrial Technology*, Prima, Indonesia, vol. 1007, pp. 1–6, 2018.

[35] S. Nishihara, N. Shinmen, T. Ebibhara, K. Mizutani and N. Wakatsuki, "Design of secure near-field communication for smartphones using sound and vibration," in *Proc. 2017 IEEE 6th Global Conf. on Consumer Electronics (GCCE)*, Nagoya, Japan, Piscataway: IEEE, pp. 1–4, 2017.

[36] V. Jaime and A. Peinado, "Musicypher: Music for message encryption," 2019. [Online]. Available: http://smc2019.uma.es/articles/D1/D1_06_SMC2019_paper.pdf.

[37] S. Vaidyanathan, A. Sambas, S. Kacar and Ü. Çavuşoğlu, "A new three-dimensional chaotic system with a cloud-shaped curve of equilibrium points, its circuit implementation and sound encryption," *International Journal of Modelling, Identification and Control*, vol. 30, no. 3, pp. 184–196, 2018.

[38] D. Micciancio, "Symbolic encryption with pseudorandom keys," in *Proc. Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Darmstadt, Germany; In: Y. Ishai, V. Rijmen (Eds.), Advances in Cryptology—EUROCRYPT 2019. EUROCRYPT 2019. Lecture Notes in Computer Science, Cham: Springer, vol. 11478, pp. 64–93, 2019.

[39] E. R. Orozco, E. E. G. Guerrero, E. I. Gonzalez, O. R. L. Bonilla, A. F. Vergara *et al.,* "FPGA-based chaotic cryptosystem by using voice recognition as access key," *Electronics*, vol. 7, no. 12, pp. 414, 2018.

[40] J. Feigenbaum, "Encryption and surveillance," *Communications of the ACM*, vol. 62, no. 5, pp. 27–29, 2019.

[41] G. Li, Y. Pu, B. Yang and J. Zhao, "Synchronization between different hyper chaotic systems and dimensions of cellular neural network and its design in audio encryption," *Cluster Computing*, vol. 22, no. 3, pp. 7423–7434, 2019.

[42] D. Datta, D. Mittal, N. P. Mathew and J. Sairabanu, "Comparison of performance of parallel computation of CPU cores on CNN model," in *Proc. 2020 Int. Conf. on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, Vellore, India, Piscataway: IEEE, pp. 1–8, 2020.

[43] S. Zhang, I. Khan and Y. Ullah, "Audio steganography by additional channel, " in *Recent Developments in Intelligent Computing, Communication and Devices*. Singapore: Springer, pp. 633–642, 2019.

[44] S. F. Yousif, A. J. Abboud and H. Y. Radhi, "Robust image encryption with scanning technology, the El-Gamal algorithm and chaos theory," *IEEE Access*, vol. 8, pp. 155184–155209, 2020.

[45] A. A. Alfa, K. B. Ahmed, S. Misra, A. Adewumi, R. Ahuja *et al.,* "A comparative study of methods for hiding large size audio file in smaller image carriers," in *Emerging Technologies in Computer Engineering: Microservices in Big Data Analytics. ICETCE 2019.* A. Somani, S. Ramakrishna, A. Chaudhary, C. Choudhary, B. Agarwal (Eds.), Communications in Computer and Information Science, Singapore: Springer, vol. 985, pp. 179–191, 2019.

[46] A. Venčkauskas, N. Morkevicius, K. Bagdonas, R. Damaševičius and R. Maskeliūnas, "A lightweight protocol for secure video streaming," *Sensors*, vol. 18, no. 5, pp. 1554, 2018.

[47] X. Duan, L. Nao, G. Mengxiao, D. Yue, Z. Xie *et al.,* "High-capacity image steganography based on improved FC-DenseNet," *IEEE Access*, vol. 8, pp. 170174–170182, 2020.

[48] L. Xiang, S. Yang, Y. Liu, Q. Li and C. Zhu, "Novel linguistic steganography based on character-level text generation," *Mathematics*, vol. 8, no. 9, pp. 1558, 2020.

[49] H. Dutta, R. K. Das, S. Nandi and S. M. Prasanna, "An overview of digital audio steganography," *IETE Technical Review*, vol. 2, no. 1, pp. 1–19, 2019.

[50] A. S. Nittala, X. D. Yang, E. Sharlin, S. Bateman and S. Greenberg, *SonicData: Broadcasting data via sound for smartphones*. Research Report 2014-1064-15: Calgary, AB, Canada T2N 1N4: Department of Computer Science, University of Calgary, 2014. [Online]. Available: https://utouch.cpsc.ucalgary.ca/docs/2014-SonicData.Report2014-1064-15.pdf.

[51] G. Raja, S. Anbalagan, G. Vijayaraghavan, P. Dhanasekaran, Y. D. Al-Otaibi *et al.,* "Energy-efficient end-to-end security for software defined vehicular networks," *IEEE Transactions on Industrial Informatics*, 2020, In Press.

[52] A. A. A. El-Latif, B. A. El-Atty, S. E. V. Andraca, H. Elwahsh, M. J. Piran *et al.,* "Providing end-to-end security using quantum walks in IoT networks," *IEEE Access*, vol. 8, pp. 92687–92696, 2020.

[53] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari *et al.,* "A survey of security and privacy issues in the Internet of Things from the layered context," *Transactions on Emerging Telecommunications Technologies, Wiley*, 2020, In Press.

[54] M. Numan, F. Subhan, W. Z. Khan, S. Hakak, S. Haider *et al.,* "A systematic review on clone node detection in static wireless sensor networks," *IEEE Access*, vol. 8, pp. 65450–65461, 2020.

[55] C. Iwendi, Z. Jalil, A. R. Javed, T. Reddy, R. Kaluri *et al.,* "KeySplitWatermark: Zero watermarking algorithm for software protection against cyber-attacks," *IEEE Access*, vol. 8, pp. 72650–72660, 2020.

[56] R. Ch, T. R. Gadekallu, M. H. Abidi and A. Al-Ahmari, "Computational system to classify cyber crime offenses using machine learning," *Sustainability*, vol. 12, no. 10, pp. 4087, 2020.

[57] M. Chaumont, "Deep learning in steganography and steganalysis," in *Digital Media Steganography: Principles, Algorithms, Advances*, M. Hassaballah (Eds.), Academic Press, pp. 321–349, 2020.

[58] N. Tatbul, T. J. Lee, S. Zdonik, M. Alam and J. Gottschlich, "Precision and recall for time series," in *Proc. of the 32nd Int. Conf. on Neural Information Processing Systems*, 2–8 December, Montréal, Canada, pp. 1924–1934, 2018.

[59] J. Jeong, H. S. Kim and S. J. Kim, "Reconsideration of F1 score as a performance measure in mass spectrometry-based metabolomics," *Journal of the Chosun Natural Science*, vol. 11, no. 3, pp. 161–164, 2018.

[60] W. M. Lord, J. Sun and E. M. Bollt, "Geometric k-nearest neighbor estimation of entropy and mutual information," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 28, no. 3, pp. 33114, 2018.