Practical Data Security by Combining Cryptography and Audio Steganography

Rajat Subhro Bose, Soumya Mukherjee

Abstract— **In the modern age where information security is paramount, it is of utmost importance to conform to the most recent advancements in security technology for data security and integrity. Steganography is a ground-breaking technique in the field of information security for the purpose of covert data transmission. The technique is used to hide high fidelity information in unsecure channels so it has to transmit and receive safely to the authority using a medium that is a carrier or a cover file. This paper attempts to highlight the novel and robust approach of combining cryptographic techniques with audio steganography to utilize the spectral spaces of the audio cover to transmit information securely.**

***Index Terms*— AES encryption, audio steganography, audio-data integrity, data encryption, hybrid cryptography, message hiding, privacy protection, secure communication**

I. INTRODUCTION

Emails, credit card details, and business data that we storeon personal computers need to be protected. To conceal crucial information, we can combine steganography and cryptographic approaches, offering the user security and trust to safeguard his data on a PC. The security provided while using steganography to conceal critical information inside a cover media requires the assurance that no one will discover that any data are buried. However, if someone notices that the cover media has changed, they can still find the sensitive information. So, rather than hiding the sensitive information in the cover material, it is preferable to encryptit using a separate technique, like cryptography. Because it is encrypted, even if the concealed text is discovered, no onewill be able to decipher its meaning. In order to ensure that the secret data are protected even in the case of a verysevere security breach, we can profit from combining the two methods for enhanced protection. In this study, we proposed a strong security solution that uses RSA-AES cryptography as an assurance layer and audio-based steganography based on the use of widely available PC files.To fully safeguard the sensitive data on a PC, two tiers of system concealment techniques are used: steganography and cryptography. Steganography, in general, is the study of concealing information using a particular technique in another type of medium, such as text, image, audio, and audio files. When the secret and cover object are combined, the resulting file is known as a stego-file. The process of hiding data begins with cryptography, in which the plaintext is converted into a cipher text. A secret key will be required for the encryption procedure. We will have two levels of security in our system. The first is the cryptographic layer, which converts the plaintext into cipher text; the second is the steganographic layer, which turns the cipher text into bitstream and conceals it with an audio file. In order to take advantage of them and offer the best security for PC applications, we proposed and implemented a flexible system employing two approaches in two layers, namely cryptography and steganography, in this study. AES-RSA hybrid cryptography is used in the first layer of encryption, and audio-based steganography is used in the second layer to hide the message in the spectral phases of the audio cover. The capacity to quickly encrypt plaintext and send it using audio covers, which can be previously accessible audio files or obtained in real time, is the main advancement in this study above earlier similar work. The human hearing sense, which is typically underutilized in security applications, is being exploited in this technique. Security and law enforcement agencies can considerably benefit from this method of secure voice channel communication because it can also covertly convey secret messages. We investigated the prior literature, encrypting data with the RSA symmetric key crypto method [2], and then we further developed utilizing the AES-RSA hybrid technique, whose advantages would be discussed later.

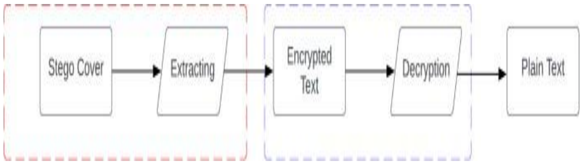

Fig. 1. Encoding and encryption

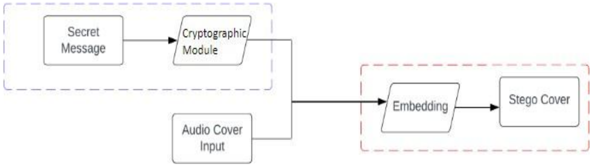

Fig. 2. Decryption and decoding

II. Background Knowledge of AES-RSA Algorithmand Phase Coding

RSA, an acronym representing its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is a well known cryptographic standard. Conceived in 1977, RSA operates on a distinctive key pair framework, consisting of a public key accessible to all and a private key accessible only to the receiver of the message. The public key serves as the gateway to encryption and digital signature verification, while the private key is used for decryption and signature creation.

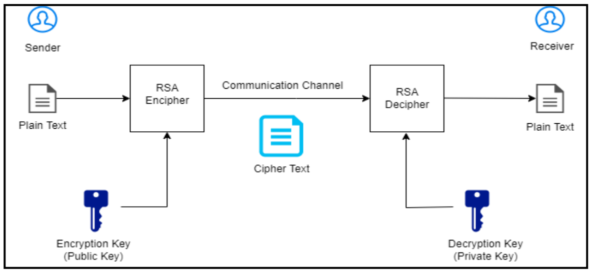

Fig. 3. RSA encryption and decryption [4]

RSA relies on the computational complexity of factoring large semi prime numbers, which are the result of multiplying two prime numbers together [9]. RSA takes into notion the fact that factorizing large semi prime numbers into their prime components is a challenging computational problem. This security parameter is inextricably linked to key length, with longer keys necessitated as computing power advances.

RSA finds applications in a diverse array of settings, securing data transmission, enabling digital signatures, and providing authentication. These applications span secure email communication, the encryption of web traffic through SSL/TLS, and secure remote access. RSA however takes a huge amount of computational resources into play for its working and hence high computational strength is required for its working.

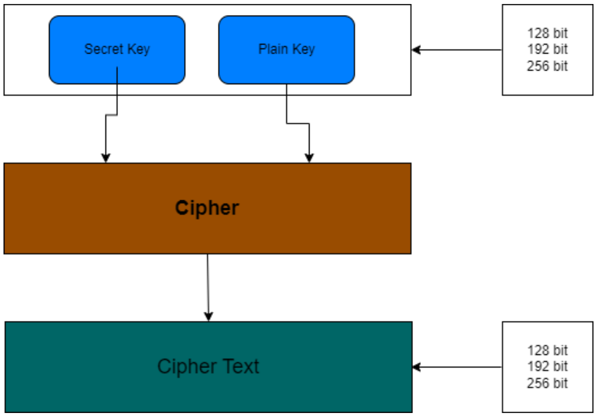

Fig. 4. AES encryption and decryption [6]

Phase coding is a key technique in the field of covert information transfer, particularly in audio steganography. While the LSB method works on the principle of hiding the secret data after the least significant bit of the audio signal, which can be functionally deciphered easily by analyzing the audio signal using specialized tools like StegExpose, Phase coding technique modifies the signal phase to hide the message into the carrier wave. Phase coding does this by introducing binary bits (0s and 1s) of hidden information into audio signals by slowly changing the phase component of the audio waves. These changes are imperceptible to the human ear, since human ears cannot detect a phase change in a wave, preserving the secrecy of any buried information. Whether employed in secure voice communication or safeguarding critical information within audio files, phase coding steganography, is a strong approach to hiding of information in a secured channel. Digital audio is represented by a series of discrete samples, each of which correlates to the amplitude of the audio waveform at a certain point in time. These samples are collected at regular intervals, often hundreds of times per second, in order to accurately capture the audio signal. When consecutively played again, these samples replicate the original audio waveform that people hear as sound. Each sample in the digital audio contains an amplitude (how loud the sound is at that precise instant) and a phase (the sample's location in relation to the waveform's cycle). Phase indicates the location during the waveform's cycle, which impacts its timbre or tonal quality, whereas amplitude controls the volume. In order to encode binary information (0s and 1s), phase coding steganography takes advantage of the fact that minor changes in the phase of audio samples are audibly unnoticeable to humans. Here's how it works: To hide a message, phase coding modifies the phase ofselected audio samples to represent binary data. Forinstance, a phase shift to the left could represent a binary"0," while a shift to the right could represent a binary "1."

It should be ensured that these phase modifications are extremely subtle. When listening to the audio, these changes should not produce audible distortions that would arouse suspicion. To extract the hidden message, the recipient applies a similar phase coding algorithm to analyze the phase differences between the samples. The resulting phase shifts are then translated back into binary data.

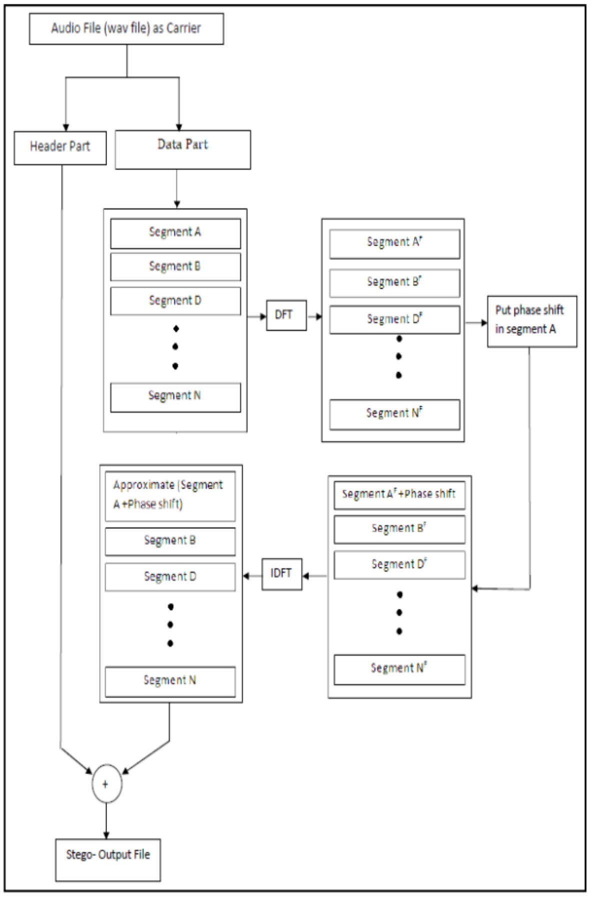

Fig. 5. Phase coding in audio steganography [7]

III. LITERATURE REVIEW

In the realm of information security, the protection of data during transmission is of paramount importance. Cryptography and steganography are two vital techniques used to safeguard data in various applications. This literature review examines recent research on these techniques, highlighting their effectiveness and areas forimprovement. In [1] Varghese and Sasikala provide an overview of the most recent and widely accepted cryptographic and steganographic standards. Their work serves as a foundational reference for understanding the contemporary landscape of secure data transmission. In [2], Mohammed et al. conducted a comprehensive comparison of cryptographic algorithms, including DES, 3DES, AES, RSA, and Blowfish, with a focus on preventing guessing attacks. Their analysis sheds light on the relative strengths and weaknesses of these algorithms, providing valuable insights for practitioners. Mohammed et al. (2018) also performed a detailed performance evaluation of the RSA- AES algorithm in comparison to other cryptographic algorithms. Their findings suggest that RSA-AES is particularly noteworthy for its efficient memory usage and speedy encryption and decryption processes, making it a compelling choice for secure data transmission. In [3] Performance Analysis of RSA and Elliptic Curve, International Journal of Network Security, Vol.20, No.4, PP.625-635, July 2018 In [4] Prof. Samir Kumar Gupta Banik, and Barnali Bandyopadhyay (2012) revisited audio steganography with a focus on mitigating the noise introduced by LSB. They introduced phase encodingtechniques to address this issue. Their work highlights the potential for making steganographic processes imperceptible to the human ear, reducing the risk of detection. A comprehensive study and understanding of audio steganographic performances reinforces our faith in our endeavour [10].

IV. METHODOLOGY

In this section, we incise the proposed architecture for our combined cryptographic-steganographic system. The systemhas two primary components along with a helper component.We elaborate the functionalities of each module hereby.

A. Cryptographic Block

This is the first layer of data protection. The cryptographic block employs the use of the AES-RSA hybrid cryptographic algorithm to encrypt the plaintext into cipher text. In our work we are employing the RSA algorithms for asymmetric key generation as concluded from our study of [9], and AES would be used to actually encrypt the data. We are primarily employing this algorithm for its security as it employs both the symmetric and asymmetric nature of the algorithms.

B. Bitstream conversion

The encrypted block of secret message can now be converted into a bitstream in correspondence to its ASCIIvalues.

C. Steganographic Block

This is the phase where we employ audio steganographic techniques to add a cover for our encrypted message. The goal is to make the hidden data imperceptible to the human ear while maintaining the audio's quality and originality. This technique leverages the fact that the human auditory system is less sensitive to certain frequency bands, allowing for the manipulation of these frequencies without causing noticeable distortion to the audio. Phase audio coding technique is robust against noise and environmental disturbances more so than amplitude modification techniques.

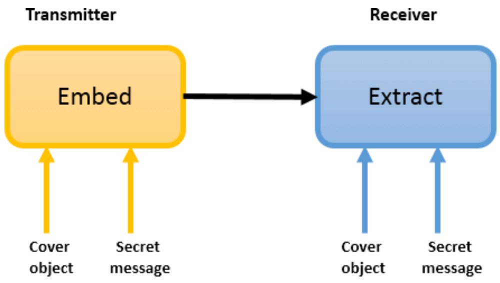

Fig. 6. Block Diagram for audio steganography [8]

To initiate this process, the first step is to create a robust RSA encryption key, chosen according to specific security needs. Following this, we encrypt the message using the AES algorithm. Using the encryption key provided before, this operation will convert our message into cipher text, a disorganized and unreadable format. This cipher text is then transformed into a binary bitstream. The cipher text's characters are represented by a string of binary numbers thatare made up of 0s and 1s. In order to facilitate seamless embedding into the audio, it's crucial to make sure that this binary bitstream has a specified, constant length or, if required, pad it with zeros to conform to certain size requirements. The stage of phase audio coding and spectral analysis is to be done next. We start by choosing a suitable audio track that will be used as our cover audio and hide ourbinary bitstream. This audio file needs to be long enough and have excellent audio quality. Next, we engage in spectral analysis of this chosen cover audio. This involves dissecting the audio signal into its constituent frequency components. Typically, this is achieved through techniques like the Short-Time Fourier Transform (STFT), which divides the audio into smaller, overlapping segments, offering valuable insights into the audio's frequency characteristics over time.

Within the spectral domain, our primary focus will be on altering the phase component of the audio signal. This is where the binary bitstream comes into play: Each binary bit in our bitstream is mapped to a specific phase modification. For instance, we could designate "0" as representing aa negative phase shift and "1" as indicating a positive phase shift. We apply these designated phase modifications to the audio within each short-time segment, ensuring that the changes are virtually imperceptible to the human ear and devoid of any audible interference.

We then use an inverse Short-Time Fourier Transform (ISTFT) to reconstruct the audio signal. The audio file has successfully incorporated our concealed binary data with nuanced phase adjustments in its spectral representation. Optionally, should the need arise, we proceed to message extraction. To do so, we employ a similar spectral analysis technique as we did during the encoding phase on the modified audio. Mapping the extracted phase information back into binary data (0s and 1s) using the predefined mapping from the encoding phase will allow us to reconstruct the binary bitstream. If required, we decrypt this extracted binary bitstream employing the private RSA key used for encryption, getting the plaintext back.

V. ALGORITHM

Algorithm 1 Hybrid encryption function

```
FUNCTION hybrid_encrypt(plaintext, public_key)
padded_plaintext <- pad(plaintext) # Apply PKCS7
paddingkey <- generate_aes_key() # Generate AES key
iv <- generate_aes_iv() # Generate AES IV
ciphertext <- encrypt_aes(padded_plaintext, key, iv) #
Encrypt with AES
cipherkey <- encrypt_key(key, public_key) # Encrypt
AESkey with recipient's public key
RETURN {'iv': iv, 'ciphertext': ciphertext}, cipherkey
```

Algorithm 2 Hybrid decryption function

```
FUNCTION hybrid_decrypt(ciphertext, cipherkey,
private_key)
    key <- decrypt_key(cipherkey, private_key) # Decrypt
    AESkey with private key
    padded_plaintext <-
    decrypt_aes(ciphertext['ciphertext'],key,
    ciphertext['iv']) # Decrypt with AES
    plaintext <- unpad(padded_plaintext) # Remove
    PKCS7padding
    RETURN plaintext
```

Algorithm 3 Steganographic module

```
# Function to hide a message in an audio file
FUNCTION hide_message(audio_path,
output_path,message)
    audio_data <- read_audio(audio_path) # Read audio
    data message_bytes  <-  message.encode('utf-8')  #
    Convert the message to bytes
    message_length <- length(message_bytes)

    IF message_length * 8 > length(audio_data)
        RAISE ValueError("Message is too large to hide
        in theaudio file.")
    END IF

    FOR i FROM 0 TO message_length
        audio_data[i] <- (audio_data[i] &
        0xFFFE) |
        ((message_bytes[i] >> 7) & 0x0001) # Hide
        message inaudio

    END FOR

    write_audio(output_path, audio_data) # Write stego
    audio
```

Algorithm 4 Extract data from waveform

```
FUNCTION extract_message(audio_path)
    audio_data <- read_audio(audio_path) # Read
    audio datamessage_bytes <- []

    FOR i FROM 0 TO length(audio_data)
        message_byte <- (audio_data[i] & 0x0001)
        << 7
        message_bytes.APPEND(message_byte)
    END FOR
    message <- decode_bytes(message_bytes, 'utf-8') #
    Decodethe hidden message
    RETURN
    message#
Main
Program
IF _name_ == "main"
    private_key <- generate_private_key() # Recipient's
    privatekey
    public_key <- generate_public_key(private_key) #
    Publickey for sender

    plaintext <- "This is a secret message."

    # Encrypt and hide the message in the audio
    ciphertext, cipherkey <-
    hybrid_encrypt(plaintext,public_key)
    hide_message("original_audio.wav",
    "stego_audio.wav",ciphertext)

    # Extract and decrypt the message from the stego
    audiorecovered_ciphertext <-
    extract_message("stego_audio.wav")
    recovered_plaintext <-
    hybrid_decrypt(recovered_ciphertext,
    cipherkey,private_key)

    IF plaintext == recovered_plaintext
        PRINT "Message successfully hidden and
        extracted."END IF
END IF
```

V. RESULT

The provided pseudo code outlines a program that combines cryptography and audio steganography to secure and conceal a message within an audio file. The program first encrypts a secret message using hybrid encryption, utilizing both AES encryption and public-key encryption. The encrypted message, along with the encrypted AES key, is then hidden within the audio file. Subsequently, the program can extract the concealed message from the audio file and decrypt it, ensuring that the recovered plaintext matches the original message. If the two messages align, the program prints "Message successfully hidden and extracted." This approach showcases a technique for both safeguarding data and covertly transmitting it within an audio medium.

VI. CONCLUSION

We have assured data integrity, confidentiality, and authentication by carefully implementing the hybrid cryptographic algorithm. The next step in the process involves converting this cipher text into a binary bitstream, which is an essential step in connecting the worlds of cryptography and audio. This binary form serves as the baseon which the stego cover is generated. Phase coding orchestrates the undetectable embedding of binary data by functioning inside the spectrum domain of audio sources. Each phase modification created by its spectrum analysis covertly holds information, creating a sequence of phase modifications. Even though they are minor, these alterations are resistant to the effects of noise, interference, and compression. Our approach offers a novel method for communicating securely across audio channels, a field frequently disregarded in the objective for data privacy.

ACKNOWLEDGMENT

I would like to extend my gratitude to my peers and all those who supported me along the way. Their encouragement and assistance were essential in making this project a reality.

REFERENCES

[1] A Detailed Review Based on Secure Data Transmission Using Cryptography and Steganography Fredy Varghese1,2 · P. Sasikala3 Accepted: 7 February 2023 / Published online: 27 March 2023 © The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023.

[2] Nazeh Abdul Wahid MD, Ali A, Esparham B, Marwan MD (2018) A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. J Comp Sci Appl Inform Technol. 3(2): 1-7. DOI: 10.15226/2474-9257/3/2/00132.

[3] Performance Analysis of RSA and Elliptic Curve, International Journal of Network Security, Vol.20, No.4, PP.625-635, July 2018

[4] LSB Modification and Phase Encoding Technique of Audio Steganography Revisited Prof. Samir Kumar, Bandyopadhyay Barnali, Gupta Banik: International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2012.

[5] Bodur, Hüseyin & Kara, Resul. (2015). Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application.

[6] Advanced Encryption Standard (AES), https://www.techtarget.com/searchsecurity/definition/Advanced- Encryption-Standard

[7] Achyuta Katta, Medium.org (2021), Audio Steganography using Phase Encoding using Python https://medium.com/@achyuta.katta/audio-steganography-using- phase-encoding-d13f100380f2

[8] Almaliki, Alaa & Din, Roshidi. (2019). Steganography analysis techniques applied to audio and image files. Bulletin of Electrical Engineering and Informatics. 8. 1297-1302. 10.11591/eei.v8i4.1626. https://www.researchgate.net/figure/Block-diagram-for-audio- steganography_fig1_336286720

[9] A Review Paper on DES, AES, RSA Encryption Standards, 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART).

[10] Recent Audio Steganography Trails and its Quality Measures, 2019 First International Conference of Computer and Applied Sciences (CAS)