IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124125

Analysis of Audio Steganography combined with Cryptography for RC4 and 3DES Encryption

Namitha M V[1], Anusha Y[2], Chaitra P R[3], Deekshitha K[4], Druva D[5]

Research Scholar, Department of Computer Science and Engineering, JNNCE, Shimoga, India[2,3,4,5]

Assistant Prof., Department of Computer Science and Engineering, JNNCE, Shimoga, India[1]

Abstract: Digital data security is of utmost importance in today's world, both cryptography and steganography are important tools to ensure the confidentiality and integrity of the data. Cryptography involves transforming the plaintext into ciphertext using encryption techniques and then decrypting it back into plaintext using decryption techniques and steganography involves hiding data in plain sight by embedding it in cover media such as images, audio, or video. Both cryptography and steganography have their own strengths and weaknesses, they can be combined to provide even better protection for digital data. By encrypting the data before embedding it in cover media using steganography, we can ensure that even if the cover media is intercepted, the data remains secure as it is encrypted. Regarding audio steganography, the techniques you mentioned, such as LSB, Echo hiding, Phase coding, and Tone insertion, are commonly used. For example, LSB is a simple technique that involves replacing the least significant bits of audio samples with data bits, while Echo hiding involves modifying the echo of an audio signal to hide the data. The combination of cryptography and steganography can provide better protection for digital data. Audio steganography techniques such as LSB, Echo hiding, Phase coding, and Tone insertion can be used depending on the specific requirements of the application.

Keywords: Human auditory system, least significant bit, Peak signal-to-noise ratio, Rivest Cipher4, 3Data Encryption Algorithm.

I. INTRODUCTION

Steganography and cryptography are two important techniques used in information security. Steganography involves hiding information within a cover object, while cryptography involves encrypting information to protect it from unauthorized access, and combining them can provide additional security. Steganography can be applied to various types of media, such as text, images, audio, and video. For example, steganography in images takes advantage of the limitations of the human visual system, while steganography in audio relies on the imperfections of the human auditory system. While steganography can provide a layer of security, it is not a substitute for cryptography even if an introducer detects the existence of a message within a cover object. In terms of encryption algorithms, there are many different techniques available. The TTJSA and DJSA algorithms proposed by Nath et al. in their modern encryption standard version - I algorithm combine two different encryption algorithms in a randomized method to enhance security. Additionally, the random-based approach for secure communication involves encrypting secret data using the SHA-1 algorithm and embedding the encrypted data in an audio file using a random-based approach.

II. RELATED WORK

Chadha et al. [1] experimented using both DCT and DWT techniques for data hiding in audio, which can provide a higher capacity for watermarking and improve the robustness of the system. Using the LSB technique for image steganography in the audio files can also be a useful approach for hiding data in a covert manner. It would be interesting to see how their technique performs compared to other existing image steganography techniques in audio files. Nugrahaet. al. [2] sequence generated from the secret key. The noisy signal is then added to the original audio signal in order to hide the data. The proposed method uses a variable length to map the secret data to the sequence of pseudo-noise samples, which helps in achieving a higher embedding rate while maintaining the quality of the audio signal and conducted experiments to evaluate the performance of the proposed technique in terms of embedding rate, distortion and robustness against attacks. The results showed that the proposed technique achieved a high embedding rate with low distortion, and was able to resist various attacks such as noise addition, filtering, and compression. The experimental results also showed that the proposed technique outperformed existing steganography techniques based on LSB and Echo hiding.

N Rashmi et al. [3] Reversible data-hiding steganography combined with cryptography is a technique that ensures both data confidentiality and integrity. It involves embedding secret data into a cover object, such as an image or a video while maintaining the cover object's original quality. Additionally, the embedded data is encrypted to prevent unauthorized

DOI: 10.17148/IJARCCE.2023.124125

access. This improved method for reversible data hiding steganography combined with cryptography provides a higher amount of safety and privacy for sensitive data. The use of reversible data hiding ensures that the cover object remains unchanged and does not arouse suspicion. The encryption of the embedded data provides an additional layer of protection against unauthorized access in 2018. Vinothkanna et al [4] a secure steganography creation algorithm for multiple file formats can be developed that provides both confidentiality and integrity of data by file selection, encryption, password protection, testing, and validation. Gurpreet Singh et al. [5] the selection of encryption algorithms depends on the specific requirements of the application. RSA is commonly used for public-key encryption, while symmetric-key encryption algorithms such as DES, 3DES, and AES are used for securing data in transit and at rest 2013. M Asad et al [6] The least significant bit (LSB) modification technique is widely used in audio steganography for embedding secret messages within the audio signal. However, this technique suffers from some limitations such as low embedding capacity, perceptual degradation, and vulnerability to steganalysis attacks. To overcome these limitations, an enhanced LSB modification technique for audio steganography has been proposed in recent research. The proposed technique involves dividing the audio signal into small frames and modifying the LSBs of the frames based on a secret key. The key determines which frames are used for embedding and the number of bits that are modified. The proposed method also employs a scrambling process to increase security and prevent detection by steganalysis algorithms. Experimental results have shown that the proposed technique achieves higher embedding.

III. METHODOLOGY

The proposed technique provides security in two ways in which the processes involved along with the input-output entities present. The input entities include the original message and the audio samples, while the output entities include the stego audio file and the revealed original message. The encryption and decryption algorithms require the input of the selected key, and the embedding and extraction processes involve the modification and extraction of LSBs of the audio samples.

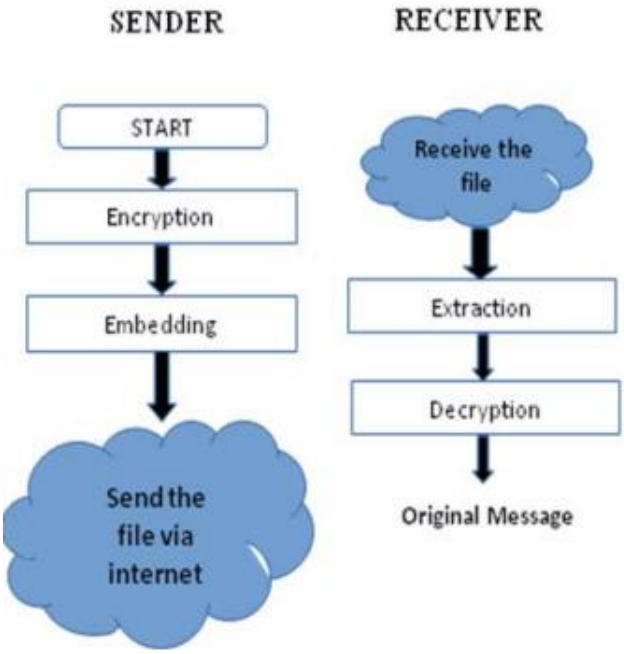

Fig. 10 System Framework

A. Encryption:

Step 1: The input text message that needs to be sent is provided.

Step 2: The original message is converted into cipher text using the selected encryption algorithm. In the proposed work, two algorithms RC4 and 3DES are used, and the performance of each algorithm is measured.

RC4 is a stream cipher algorithm that uses a variable-length key from 1 to 256 bits to initialize a 256-bit state table. The state table is then used to generate a pseudo-random stream, which is simply XOR with the data stream to produce the cipher text. The steps involved in the RC4 algorithm are illustrated in Figure 2. Overall, the RC4 algorithm is a widely used stream cipher algorithm that is known for its simplicity and fast encryption speed. However, its security has been questioned in recent years, and it is no longer recommended for use in new cryptographic applications. The entire document should be in Times New Roman. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124125

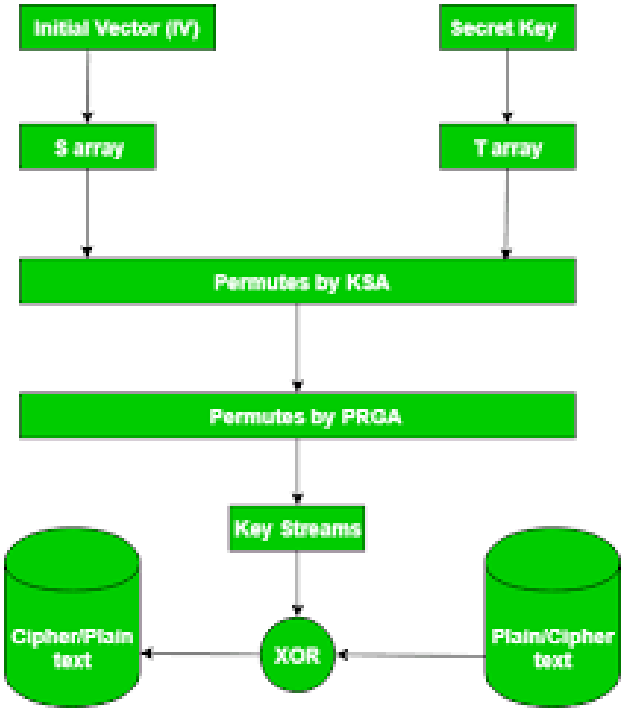

Fig. 2 RC4 Encryption

3DES is a block cipher algorithm that operates on 64-bit data blocks and can work with one, two, or three 56-bit keys. Its name is derived from the fact that it is equivalent to using DES three times on the plaintext with three different keys. Like the RC4 algorithm, 3DES also uses the Feistel structure. However, it operates using 48 rounds, compared to the 256 rounds used by RC4. Figure 3 shows the steps involved in the 3DES algorithm.

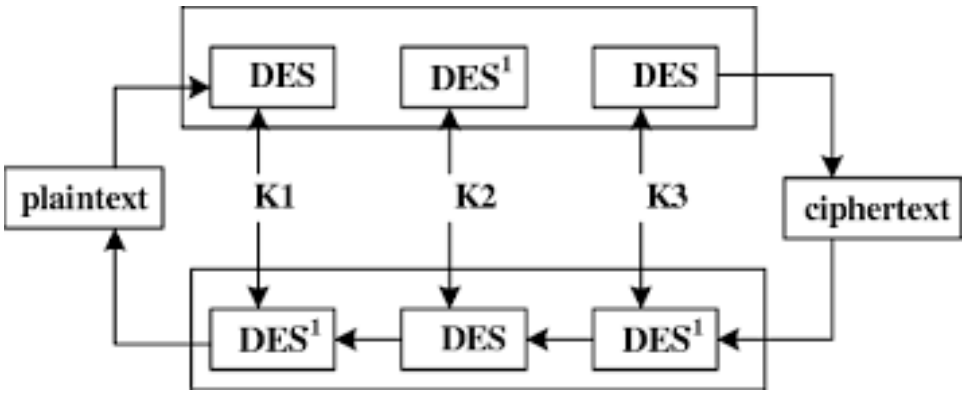

Fig. 3 3DES Encryption

B. Embedding:

In the proposed audio steganography algorithm, the audio signals are first converted from analog to digital format and represented as samples. Each sample is characterized by the sampling rate, number of channels, and number of bits per sample. For this algorithm, 16 bits per sample are used, and two channels of 8 bits each for each alternate sample are processed. The first 50 bytes of the audio file are left out, and embedding is done after performing a series of AND and OR operations on both the text and the binary value of each channel. The data embedding process starts from the 51st sample, and the least significant bit (LSB) value of alternate samples is modified accordingly. Specifically, the lower 4 bits of channel 1 contain the higher 4 bits of the text, while the lower 4 bits of channel 2 contain the lower 4 bits of the text. This embedding process ensures that the steganographic message is hidden in a way that is not easily detectable by human perception or analysis.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.124125

C. Extraction:
To extract the hidden cipher text from the stego audio created using the proposed audio steganography algorithm, a reverse embedding procedure is applied. This process involves the following steps:
1. Take the stego audio file as input and extract the audio samples.
2. For each channel of the audio, extract the LSBs of alternate samples.
3. Combine the extracted LSBs to form the embedded binary message.
4. Convert the binary message back to the original text message using the selected encryption algorithm and key.
The reverse embedding procedure effectively retrieves the hidden cipher text from the stego audio without affecting the original audio content. This process is essential for the intended recipient of the steganographic message to access the hidden information.

D. Decryption:
After extracting the hidden cipher text from the stego audio using the reverse embedding procedure, the next step is to decrypt the cipher text to reveal the original message. This process is the reverse of the encryption process, where the cipher text is transformed back into its original form using the selected decryption algorithm and the key that was used for encryption. For the proposed work, two encryption algorithms, RC4 and 3DES, were used. Therefore, the decryption process would involve using the respective decryption algorithms and the corresponding keys to obtain the original message. Overall, the process of decrypting the cipher text involves reversing the encryption process and applying the appropriate decryption algorithm and key to obtain the original message.

IV. RESULTS AND DISCUSSION

It sounds like you're describing a research proposal or paper that involves using a variable sample selection method for audio steganography with cryptography. The proposed method involves using the RC4 and 3DES algorithms to encrypt and decrypt the original text, with key lengths of 64 bits for RC4 and 112 bits for 3DES. An experiment is conducted using four audio files of different sizes to test the effectiveness of the method.

Steganography involves hiding information within other data, in this case, hiding a secret message within an audio file. The variable sample selection method likely refers to selecting specific samples or sections of the audio file to embed the hidden message in, rather than embedding it throughout the entire file. RC4 and 3DES are both encryption algorithms used to scramble data so that it is unreadable without the correct decryption key. 64-bit and 112-bit refer to the length of the encryption keys used for each algorithm. Generally, longer key lengths are more secure as they make it harder for unauthorized parties to decrypt the data. The experiment involving four audio files of different sizes is likely used to test the effectiveness and efficiency of the proposed method. The results of the experiment will provide insight into the performance of the method and whether it is viable for use in real-world applications.

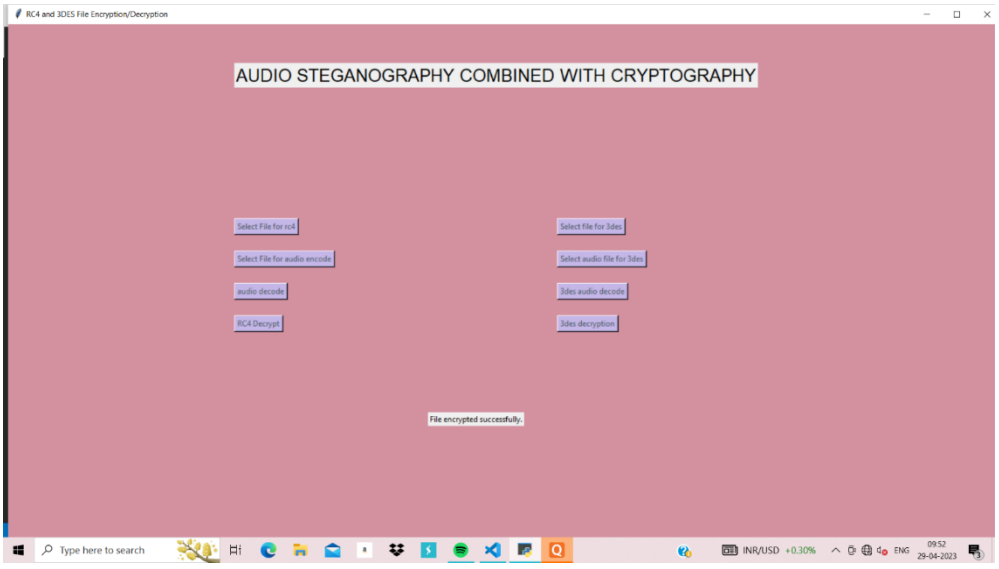

Fig. 4 RC4 Encryption result

DOI: 10.17148/IJARCCE.2023.124125

Two techniques that have been used in this are Confidentiality and PSNR by implementing RC4 and 3DES cryptography the variable sample selection method of audio steganography for hiding information within audio files, having many potential applications in the field of security.

TABLE 1 PSNR analysis

Audio	PSNR for the text size=300 characters with RC4 Encryption	PSNR for the text size=300 characters with DES Encryption
Audio 1(3 sec)	69.34	69.97
Audio 2(10 sec)	63.35	63.51

Table 1 provides valuable insights into the performance of the proposed technique using RC4 and 3DES encryption for audio steganography. It is evident from the results that the PSNR values are higher for 3DES compared to RC4, indicating the better perceptual quality of the stego audio file. This may be attributed to the fact that 3DES is a more secure and robust encryption algorithm compared to RC4. Additionally, it can be observed that the PSNR values increase as the block size and key size increase. However, this comes at the cost of larger file sizes and longer encryption and decryption times. Therefore, it is important to strike a balance between the quality of the stego audio and the practicality of the encryption parameters. The optimal values for block size and key size may vary depending on the specific requirements of the application. It is worth noting that PSNR is not the only metric for evaluating steganographic techniques, and other factors such as imperceptibility, robustness, and capacity should also be considered.

V. CONCLUSION

The proposed algorithm that combines cryptography and steganography techniques is effective in providing multilevel security to confidential data. However, it is essential to analyze and evaluate its performance. The variable sample selection techniques used in audio steganography, combined with the dual security model of RC4 and 3DES encryption algorithms, were analyzed to determine the optimal solution for securing data. The analysis revealed that the quality of the stego audio is directly proportional to the block size and key length of the encryption algorithms. In addition, the results indicated that the proposed algorithm performs better with RC4 encryption compared to 3DES encryption. It is crucial to continue evaluating and enhancing the algorithm to ensure the maximum security of digital data.

REFERENCES

[1]. doi: 10.1109/5.771065 [8] Vinothkanna, Mr. R. "A SECURE STEGANOGRAPHY CREATION ALGORITHM FOR MULTIPLE FILE FORMATS." Journal of Innovative Image Processing (JIIP) 1, no. 01 (2019): 20-30.

[2]. doi: 10.1109/ICCNIT.2011.6020921 [15] N. Rashmi and K. Jyothi, "An improved method for reversible data hiding steganography combined with cryptography, "2018 2nd IEEE International Conference on Inventive Systems and Control (ICISC), Coimbatore, 2018, pp.81-84. doi: 10.1109/ICISC.2018.8398946.

[3]. Fatiha Djebbar and Beghdad Ayad and Karim Abed Meraim and Habib Hamam - "Comparative Study of Digital Audio Steganography Techniques".

[4]. Teck Jian, Chua & Chuah, Chai Wen & Hidayah Binti Ab. Rahman, Nurul & A Hamid, isredza rahmi. (2017). "Audio Steganography with Embedded Text". IOP Conference Series: Materials Science and Engineering. 226. 012084. 10.1088/1757-899X/226/1/012084.

[5]. Praveena, A., and S. Smys. "Efficient cryptographic approach for data security in wireless sensor networks using MES VU." In 2016 10th international conference on intelligent systems and Control (ISCO), pp. 1-6. IEEE, 2016.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.124125

[6]. SiddalingeshBandi and H.S. Manjunatha Reddy, (2019) "SSAWS: Secure Scrambling and Adaptive Wavelet-based Blind Image Steganography" Journal of Advanced Research in Dynamical and Control Systems, 11(7), 60-72.
[7]. Abood, M. H. (2017). Efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms. 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT). doi:10.1109/ntict.2017.7976154.
[8]. Mohajon, J., Ahammed, Z., &Talukder, K. H. (2018, December). An Improved Approach in Audio Steganography Using Genetic Algorithm with K-Bit Symmetric Security Key. In 2018 21st International Conference of Computer and Information Technology (ICCIT) (pp. 1-6). IEEE.
[9]. Tayel, M., Gamal, A., &Shawky, H. (2016). A proposed implementation method of an audio steganography technique. 2016 18th International Conference on Advanced Communication Technology (ICACT). doi:10.1109/icact.2016.7423320.
[10]. Yang, Z., Du, X., Tan, Y., Huang, Y., & Zhang, Y. J. (2018). AAG-Stega: Automatic Audio Generation-based Steganography. arXiv preprint arXiv:1809.03463.
[11]. Mohajon, J., Ahammed, Z., & Talukder, K. H. (2018, December). An Improved Approach in Audio Steganography Using Genetic Algorithm with K-Bit Symmetric Security Key. In 2018 21st International Conference of Computer and Information Technology (ICCIT) (pp. 1-6). IEEE.