A Modified Enhanced Method of Audio – Video Steganography for High Security Data Transmission

Natchiamai PL[1,*1], *Rajalakshmi* V[2] , *Indumathy* A[3] and *Sudarsanan* K[4]

[1]Assistant Professor, Department of ECE, Mookambigai College of Engineering, Pudukkottai, Tamilnadu, India

[2]Associate Professor, Department of ECE, Mookambigai College of Engineering, Pudukkottai, Tamilnadu, India

[3]Assistant Professor,Department of ECE, Mookambigai College of Engineering, Pudukkottai, Tamilnadu, India

[4]Assistant Professor, Department of ECE, Kings College of Engineering, Pudukkottai, Tamilnadu, India

Abstract. Steganography is an art of convert communication, which offers secrete and secure way of communication. It has many application areas such as audio-video synchronization,in defense forces etc… The audio data is converted into binary format and encrypted using a XOR encryption algorithm. Then the encrypted audio data converted into XL data form. The video frames are divided into non-overlapping blocks, and the difference between the adjacent pixels in each block is computed to obtain a reference matrix. Each block is then iterated through, if the difference between adjacent pixels is greater than or equal to the average difference in the reference matrix, the MPVD (Modified Pixel Value Differencing) based LSB of the pixel value is modified to embed the encrypted audio data bit. The embedded bit is then XORed with the corresponding LSB of adjacent pixel in the same block. The modified video frames can be sent over an unsecured channel without revealing the embedded encrypted audio data. To extract the encrypted audio message from the stego video, the embedded bits are XORed with the corresponding LSB of the adjacent pixel in the same block, and the modified LSBs are extracted and decrypted using the same encryption algorithm and key.

1 Introduction

Steganography is the practice of hiding secret information within an innocuous carrier message or medium, such as an image, audio file, or video, without arousing suspicion that such a message exists. The goal of steganography is to make the presence of the hidden message undetectable to anyone except the intended recipient. Steganography has been used for centuries, with ancient Greek messengers using wax-covered wooden tablets to hide secret messages, and during World War II, spies used invisible ink to hide messages on paper.

In the modern era, steganography has gained importance due to the widespread use of digital media and the need to secure sensitive information.

[*]Corresponding author: staffmceece@gmail.com

Steganography is the art of concealing information within a seemingly harmless carrier medium, such as an image, audio, or video file. One of the most popular techniques of steganography is hiding data within digital media, such as audio or video files. Steganography involves concealing information within multimedia files such as images, videos, and audio, rather than preserving it in its original form. This technique is commonly used in industries for digital watermarking and fingerprinting of audio and video, providing a means to hide and protect sensitive data during transmission and transformation. To achieve this, the information is converted into a bit stream and then embedded within altering frames of an image. Given the increasing prevalence of cybercrimes, it is crucial for steganographic methods to be highly effective and secure, aiming to minimize criminal activities. To enhance data security, it is advisable to combine cryptography with steganography.

There are two approaches to performing steganography in videos: one involves storing data from frame to frame, while the other involves converting frames into the frequency domain and storing the resulting information. The former is known as spatial domain steganography, while the latter is referred to as frequency domain steganography. Regardless of the chosen method, video steganography can be categorized into two types: lossless and lossy steganography. In lossless steganography, both the hidden information and the original video file can be retrieved without any errors or modifications. On the other hand, in lossy steganography, the hidden information can be correctly extracted, but the original video will exhibit some errors. Audio steganography involves embedding data within an audio signal, without affecting the quality of the original audio. In the case of video steganography, data is hidden within video files. One approach to this technique is to use audio data hiding in video. This involves hiding secret information within the audio track of a video file, which is then disguised by the visual content of the video. Audio data hiding in video has numerous applications, such as secure communication, copyright protection, and digital watermarking. With the increasing popularity of digital media and the ease of accessing and manipulating such files, steganography has become an important tool for securing sensitive information.

1.1 Applications of steganography process

1.1.1 Digital watermarking: Steganography can be used to embed digital watermarks into images, audio files, or videos. Watermarks are used to identify the owner of the content and protect against copyright infringement.

1.1.2 Military and intelligence operations: Steganography can be used to send secret messages between military and intelligence operatives in the field, without arousing suspicion that a message has been sent.

1.1.3 Information security: Steganography can be used to protect sensitive data, such as passwords, by hiding them within an image or other digital medium.

1.1.4 Cyber security: Steganography can be used to conceal malware or other malicious code remove within seemingly innocent files, making it more difficult for antivirus software to detect.

1.2 Previous arts

In recent years, numerous image and video encryption algorithms based on chaos have been proposed and published. While these algorithms typically undergo some level of security analysis, many of them have been successfully broken in subsequent studies. This research aims to challenge the two main reasons often cited for preferring chaos-based image encryption over classical cryptographic encryption: computational efficiency and security advantages. Through experimental evidence, it demonstrates that several commonly used statistical tests employed to evaluate the security of chaos-based encryption schemes are inadequate for thorough security analysis. The researchers construct deliberately insecure encryption schemes that perform well and even pass some of these tests, highlighting the insufficiency of such tests in assessing security. Consequently, the findings suggest that these tests can only provide a necessary, but not sufficient, condition for security. This work calls into question the reliability of various security analyses in related studies, and emphasizes the need to completely reevaluate methodologies for assessing the security of chaos-based encryption schemes.

Audio hiding in video is a process of embedding audio signals into video signals in such a way that the audio remains imperceptible to the human ear while watching the video, but can be extracted and decoded later. This technique is often used in applications such as digital watermarking, copyright protection, and audio data hiding for security purposes. Embedding audio signals into video can cause compression artifacts and reduce the overall video quality. Additionally, the embedded audio signal can also introduce noise and distortion to the original video signal, leading to degradation of the overall audio and video quality.

1.3 Issues

- The traditional way is followed to compare the original and encrypted image where the changing intensity value is found to be typically lower.
- Complexity is more.
- Distortion is high
- Only analysed the audio steganography

2 Methods

Audio encryption using XOR is a technique that can be used to protect audio data from unauthorized access. XOR, which stands for exclusive OR, is a binary operation that can be used to perform encryption. In this technique, a random key is chosen and XOR is performed between each bit of the audio data and the corresponding bit of the key. This process results in an encrypted version of the audio data. To generate audio data in XL form, the encrypted binary data can be saved as a plain text file with an .xl extension. This format can be useful for storing encrypted audio data in a way that can be easily read and processed by computer programs. It's important to note that XOR encryption is not considered to be a very strong form of encryption and can be easily cracked by an experienced attacker.

The technique involves encrypting the audio data using the XOR encryption technique and then converting it into binary format. The selected video frames are modified using the MPVD algorithm, which involves subtracting the pixel values of adjacent pixels to generate a difference value. The difference value is then used to modify the pixel value in the video frame. The encrypted audio data is then embedded in the least significant bits of the modified pixel values using the LSB algorithm.

2.1 Audio Encryption using XOR Method

Audio encryption using XOR is a simple technique that can be used to encrypt audio data. Here's how can do it:

2.1.1 Choose a key: The first step is to choose a key that will be used for encryption. The key should be a sequence of random bits that is at least as long as the audio data.

2.1.2 Convert audio data to binary: The audio data must be converted to binary before encryption can take place. This can be done using any suitable algorithm, such as PCM (Pulse Code Modulation) or WAV (Waveform Audio Format).

2.1.3 Encrypt using XOR: Once the audio data has been converted to binary, the encryption process can begin. This involves performing an XOR (exclusive OR) operation between each bit of the audio data and the corresponding bit of the key. This process should be repeated until all bits of the audio data have been encrypted.

2.1.4 Generate audio data in XL form: Once the audio data has been encrypted, it can be converted back to its original format (such as WAV or MP3). To generate the audio data in XL form, user can save the encrypted binary data as a plain text file with an .xl extension.

2.2 Encrypted Audio Data Hiding and Retrieval Process

2.2.1 Data hiding process:

Step 1: Choose a video file and an audio file that want to use for the hiding process.

Step 2: Encrypt the audio file using a XOR encryption algorithm.

Step 3: Convert the encrypted audio file into XL data.

Step 4: Divide the data of the encrypted audio file into smaller chunks that can fit into the LSB of the pixel values of the video file. The size of each chunk depends on the
number of LSBs ant to use for data hiding.

Step 5: Implement the modified pixel value differencing algorithm on the video file. This algorithm computes the difference between adjacent pixels in each frame of the video, and then modifies the LSB of the pixel value according to the binary data of the encrypted audio file chunks.

Step 6: Embed the binary data of the encrypted audio file into the LSB of the pixel values of the video frames.

Step 7: Save the modified video file with the hidden audio data.

2.2.2 Data retrieval process:

Step 1: Open the modified video file that contains the hidden audio data.

Step 2: Extract the LSBs of the pixel values of each frame of the video using the same algorithm that was used to embed the data.

Step 3: Reconstruct the binary data of the encrypted audio file by concatenating the LSBs of the pixel values.

Step 4: Divide the binary data of the encrypted audio file into chunks of the same size as those used during embedding.

Step 5: Decrypt each chunk of the binary data using the same encryption algorithm that was used during embedding.

Step 6: Reconstruct the decrypted audio data by concatenating the decrypted chunks.

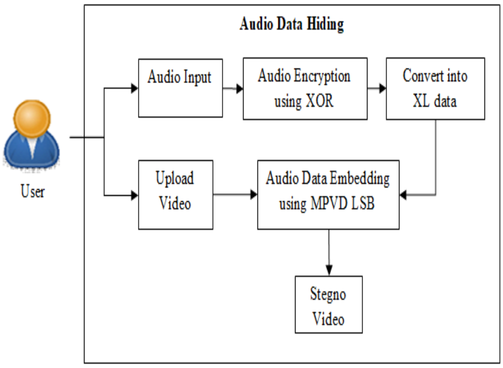


Fig. 1. Proposed System Architecture

3 Results and discussion

The original audio file is converted into encrypted audio file. The encrypted audio data has to be hidden within video file. The embedded data were extracted from stegno video and original audio file is recovered.

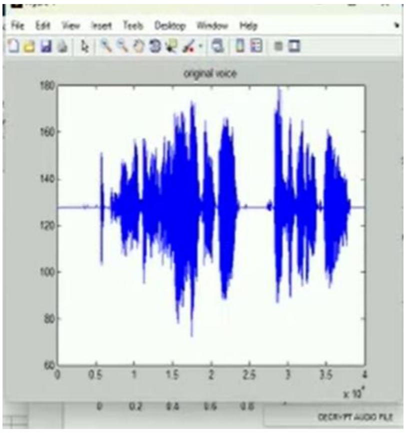


Fig. 2. Input Audio

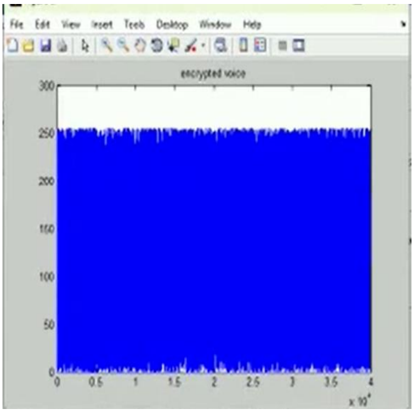
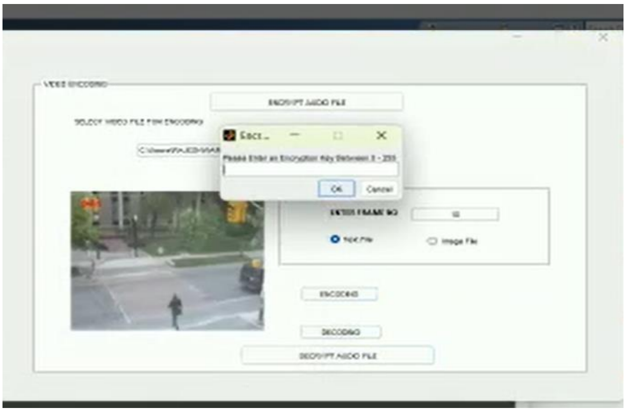


Fig. 3. Encrypted Audio



Please Enter an Encryption Key Between 1 - 255

Fig. 4. Encrypted Audio Hiding in Video

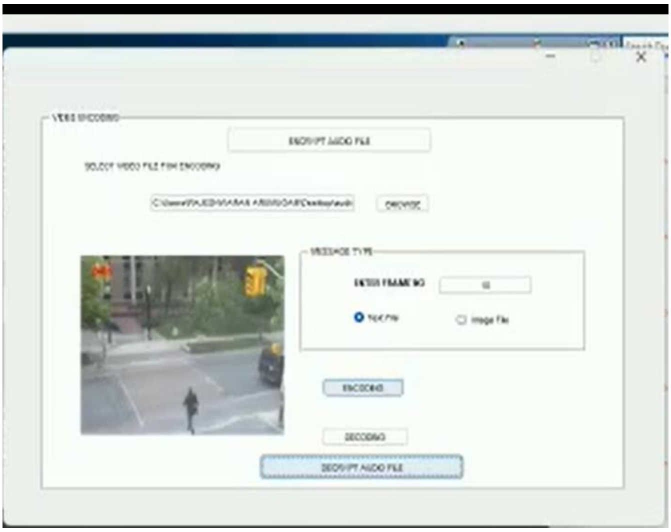


Fig. 5. Audio Extraction from Video

4 Conclusion

The following conclusions were made from this study:
XOR-based audio data hiding within video using modified pixel value differencing in LSB algorithm is a technique that can be used to embed encrypted audio data into a video file for the purpose of secure data transmission. The technique involves XORing the binary data of the encrypted audio file with the LSB of the pixel values of the video frames, rather than directly embedding the binary data as in the previous approach.
This increases the security of the data hiding process and makes it more resistant to detection and extraction by attackers. The data retrieval process involves extracting the XORed data from the LSB of the pixel values of each video frame, and then performing the XOR operation again with the same key used during embedding to obtain the original binary data of the encrypted audio file. This data is then decrypted using the same encryption algorithm that was used during embedding to retrieve the original audio data.

References

1. J. Hayes and G. Danezis, Advances in Neural Information Processing Systems, pp. 1954-1963. (2017)
2. D.P. Kingma and P. Dhariwal, Advances in Neural Information Processing Systems, pp. 10215-10224(2018)
3. D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, IEEE Access, **vol. 6**, pp. 38 303-38 314, (2018)
4. J. Zhu, R. Kaplan, J. Johnson, and L. Fei-Fei, European Conference on Computer Vision, pp. 657-672. (2018)
5. J. Shen, R. Pang, R. J. Weiss, M. Schuster, N. Jaitly, Z. Yang, Z. Chen, Y. Zhang, Y. Wang, R. Skerrv -Ryan et al., "Natural TTS synthesis by conditioning wavenet" International Conference on Acoustics, Speech and Signal Processing, pp. 4779-4783 (2018)
6. W. Ping, K. Peng, A. Gilinsky, S. O. Arik, A. Kannan, S. Narang , J. Raiman , and J. Miller, Proc. ICLR , pp. 214 -217, (2018)
7. K. Yang, K. Chen, W. Zhang, and N. Yu, International Work - shop on Digital Watermarking, pp. 55 -68.(2018)
8. Z. Zhang, J. Liu, Y. Ke, Y. Lei, J. Li , M. Zhang , and X. Yang , IEEE Access , vol. 7 , pp. 118 586 -118 597 ,(2019)
9. M. Yedroudj, F. Comby, and M. Chaumont, Journal of Visual Communication and Image Representation 1907.06956, (2019)
10. W. Ping, K. Peng, and J. Chen, "Clarinet: Parallel wave generation in end -to -end text to -speech" International Conference on Learning Representations, (2019)
11. Y. Masuyama, K. atabe, Y.Koizumi , Y. Oikawa and N. Harada , "Deep griffin -lim iteration" IEEE International Conference on Acoustics , Speech and Signal Processing , pp. 61 -65. (2019)
12. R. Prenger, R. Valle, and B. Catanzaro, "Wave glow: A flow - based generative network for speech synthesis, IEEE International Conference on Acoustics, Speech and Signal Processing, pp . 3617 -3621 (2019)
13. Y. Ren, Y. Ruan, X. Tan, T. Qin, S. Zhao, Z. Zhao, and T.-Y. Liu, Advances in Neural Information Processing Systems , pp. 3165 —3174. (2019)

14. Ramalingam, Mritha, Nor Ashidi Mat Isa, and Puviarasi. R "A secured data hiding using affine transformation in video steganography." Procedia Computer Science 171: 1147-1156. (2020)
15. N. Zhong, Z. Qian, Z. Wang, X. Zhang, and X. Li, IEEE Transactions on Circuits and Systems for Video Technology , (2020)